

**IMPLEMENTASI DIGITAL WATERMARKING MENGGUNAKAN  
ALGORITMA *MODIFIED LEAST SIGNIFICANT BIT* PADA GAMBAR  
MEDIA PROMOSI DI FAKULTAS TEKNOLOGI INDUSTRI UNISSULA**

**LAPORAN TUGAS AKHIR**

Laporan ini disusun guna memenuhi salah satu syarat untuk menyelesaikan  
program studi Teknik Informatika S-1 pada Fakultas Teknologi Industri  
Universitas Islam Sultan Agung



**Disusun Oleh:**

**AHMAD FARIKIN**

**NIM 32601500944**

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INDUSTRI  
UNIVERSITAS ISLAM SULTAN AGUNG  
SEMARANG**

**2022**

**FINAL PROJECT**

**IMPLEMENTATION OF DIGITAL WATERMARKING USING MODIFIED  
LEAST SIGNIFICANT BIT ALGORITHM ON PROMOTIONAL MEDIA  
IMAGES AT UNISSULA INDUSTRIAL TECHNOLOGY FACULTY**

*Proposed to complete the requirement to obtain a bachelor's degree (S-1) at  
Informatics Engineering Departement of Industrial Technology Faculty Sultan  
Agung Islamic University*



**Arranged By:**

**AHMAD FARIKIN  
NIM 32601500944**

**MAJORING OF INFORMATICS ENGINEERING  
INDUSTRIAL TECHNOLOGY FACULTY  
SULTAN AGUNG ISLAMIC UNIVERSITY  
SEMARANG  
2022**

## LEMBAR PENGESAHAN PEMBIMBING

Laporan Tugas Akhir dengan judul "Implementasi *Digital Watermarking* Menggunakan Algoritma *Modified Least Significant Bit* pada Gambar Media Promosi Di Fakultas Teknologi Industri Unissula", ini disetujui oleh :

Nama : Ahmad Farikin

NIM : 32601500944

Program Studi: Teknik Informatika

Telah disahkan oleh dosen pembimbing pada:

Hari : Senin

Tanggal : 24 Oktober 2022

Pembimbing I



Moch Taufik, ST, MIT  
NIDN.0622037502

Pembimbing II

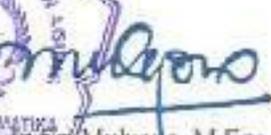


Basus Satrio W.P., S.Kom, M.Cs  
NIDN.1027118801

Mengetahui,

Ketua Program Studi Teknik Informatika  
Fakultas Teknologi Industri  
Universitas Islam Sultan Agung



  
H. Sri Mulyono, M.Eng.  
NIDN.0626066601

## LEMBAR PENGESAHAN PENGUJI

Laporan tugas akhir dengan judul "Implementasi Digital *Watermarking* Menggunakan Algoritma *Modified Least Significant Bit* pada Gambar Media Promosi Di Fakultas Teknologi Industri Unissula" ini telah dipertahankan di depan dosen penguji Tugas Akhir pada :

Hari : .....

Tanggal : .....

### TIM PENGUJI

Anggota I

  
Dedy Kurniadi, ST,M.Kom  
NIDN.0622058802

Anggota II

  
24-10-22  
Ghufron, ST,M.Kom  
NIDN.062079005

Ketua Penguji

  
24/10/2022  
Badie, ST,M.Kom  
NIDN.0619018701

## SURAT PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan dibawah ini :

Nama : Ahmad Farikin

NIM : 32601500944

Judul Tugas Akhir : Implementasi *Digital Watermarking* Menggunakan Algoritma *Modified Least Significant Bit* pada Gambar Media Promosi Di Fakultas Teknologi Industri Unissula.

Dengan bahwa ini saya menyatakan bahwa judul dan isi Tugas Akhir yang saya buat dalam rangka menyelesaikan Pendidikan Strata Satu (S1) Teknik Informatika tersebut adalah asli dan belum pernah diangkat, ditulis ataupun dipublikasikan oleh siapapun baik keseluruhan maupun sebagian, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka, dan apabila di kemudian hari ternyata terbukti bahwa judul Tugas Akhir tersebut pernah diangkat, ditulis ataupun dipublikasikan, maka saya bersedia dikenakan sanksi akademis. Demikian surat pernyataan ini saya buat dengan sadar dan penuh tanggung jawab.

Semarang, 24 oktober 2022

Yang Menyatakan,



Ahmad Farikin

## PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH

Saya yang bertanda tangan dibawah ini :

Nama : Ahmad Farikin

NIM : 32601500944

Program Studi : Teknik Informatika

Fakultas : Teknologi industri

Alamat Asal : Dsn.Ngrijo RT.01/09 Desa.jambon Kec.pulokulon Kab.Grobogan  
Jawa Tengah

Dengan ini menyatakan Karya Ilmiah berupa Tugas akhir dengan Judul :  
"Implementasi Digital Watermarking Menggunakan Algoritma Modified Least  
Significant pada Media Promosi Di Fakultas Teknologi Industri Unissula" Menyetujui  
menjadi hak milik Universitas Islam Sultan Agung serta memberikan Hak bebas  
Royalti Non-Eksklusif untuk disimpan, dialihmediakan, dikelola dan pangkalan data  
dan dipublikasikan diinternet dan media lain untuk kepentingan akademis selama tetap  
menyantumkan nama penulis sebagai pemilik hak cipta. Pernyataan ini saya buat  
dengan sungguh-sungguh. Apabila dikemudian hari terbukti ada pelanggaran Hak  
Cipta/Plagiarisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang  
timbul akan saya tanggung secara pribadi tanpa melibatkan Universitas Islam Sultan  
Agung.

Semarang, 24 oktober 2022

Yang menyatakan



Ahmad Farikin

## KATA PENGANTAR

Dengan mengucapkan puji dan syukur kehadiran Allah SWT yang telah melimpahkan rahmat dan karunianya kepada penulis, sehingga dapat menyelesaikan Tugas Akhir dengan judul “Implementasi Digital *Watermarking* menggunakan Algoritma *Modified Least Significant Bit* pada Media Promosi Di Fakultas Teknologi Industri Unissula” guna untuk memenuhi salah satu syarat menyelesaikan studi serta dalam rangka memperoleh gelar sarjana (S-1) pada Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Islam Sultan Agung Semarang.

Tugas akhir ini dibuat dan disusun dengan bantuan dari berbagai pihak, baik materi maupun teknis, oleh karena itu saya sebagai penulis mengucapkan terima kasih kepada :

1. Kedua orang tua saya, kakak dan juga adik tercinta yang selalu memberikan semangat, doa kelancaran dan keberhasilan dalam ujian ini.
2. Bapak Moch Taufik, ST, MIT selaku dosen pembimbing pertama yang telah memberikan waktu dan ilmu kepada penulis.
3. Bapak Bagus Satrio WP, S.Kom., M.Cs. selaku pembimbing kedua yang telah memberikan waktu dan ilmu kepada penulis.
4. Seluruh dosen FTI yang telah memberikan banyak ilmu selama masa perkuliahan
5. Seluruh teman seperjuangan yang telah memberikan semangat bantuan.

Dengan segala kerendahan hati, penulis menyadari masih banyak kekurangan dari segi kuantitas dan kualitas, maupun dari segi ilmu pengetahuan dalam proses penyusunan laporan. sehingga penulis mengharapkan adanya kritikan dan saran yang membangun demi kesempurnaan laporan ini dimasa mendatang.

Semarang 24 Oktober 2022

Penulis

Ahmad Farikin

## DAFTAR ISI

LEMBAR PENGESAHAN PEMBIMBING .....	iii
LEMBAR PENGESAHAN PENGUJI .....	iv
SURAT PERNYATAAN KEASLIAN TUGAS AKHIR.....	v
PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH.....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR .....	xi
DAFTAR TABEL.....	xii
ABSTRAK.....	xiii
BAB I.....	1
Pendahuluan .....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Masalah .....	2
1.4 Tujuan.....	2
1.5 Manfaat.....	3
1.6 Sistematika Penulisan .....	3
BAB II.....	4
Tinjauan Pustaka dan Dasar Teori .....	4
2.1 Tinjauan Pustaka.....	4
2.2 Dasar Teori .....	6
2.2.1 <i>Digital Watermarking</i> .....	6
2.2.2 <i>Least Significant Bit (LSB)</i> .....	7

2.2.3 <i>Modified least significant bit</i> .....	9
2.2.4 <i>Digital Image</i> .....	10
2.2.5 MSE Dan PSNR .....	11
2.2.6 Matlab .....	13
BAB III.....	14
Metode Penelitian.....	14
3.1 Metode Penelitian .....	14
3.3.1. Pengumpulan Data.....	14
3.3.2. Metode pengembangan sistem.....	14
3.2 Perancangan sistem secara umum .....	15
3.3 Analisa perangkat keras.....	15
3.4 Analisa perangkat lunak .....	15
3.5 Perancangan arsitektur sistem.....	15
3.5.1. Proses <i>encode</i> .....	16
3.5.2. Proses <i>decode</i> .....	17
3.6 Perancangan sistem.....	18
3.6.1 <i>Use case diagram</i> .....	18
3.6.2 <i>Activity diagram</i> .....	19
3.7 Metode <i>Modified Least Significant Bit (MLSB)</i> .....	20
3.8 Perancangan <i>user interface</i> .....	22
BAB IV .....	26
Hasil dan Analisis Penelitian .....	26
4.1. Implementasi Sistem.....	26
4.2. Pengujian dengan sistem <i>black box</i> .....	30
BAB V.....	34
Kesimpulan dan Saran.....	34

5.1. Kesimpulan.....	34
5.2. Saran .....	34
Daftar Pustaka.....	35



## DAFTAR GAMBAR

Gambar 2.1 Alur proses <i>watermark</i> .....	7
Gambar 2.2 <i>Pixel</i> citra <i>grayscale</i> 10 x 10 .....	8
Gambar 2.3 <i>Pixel</i> citra yang diambil.....	8
Gambar 2.4 Proses <i>mlsb</i> .....	10
Gambar 3.1 <i>Flow chart encode</i> .....	16
Gambar 3.2 <i>Flow chart decode</i> .....	17
Gambar 3.3 <i>Use case diagram</i> .....	18
Gambar 3.4 Diagram <i>activity encode</i> .....	19
Gambar 3.5 Diagram <i>activity decode</i> .....	20
Gambar 3.6 Hasil <i>rundom number</i> .....	21
Gambar 3.7 Gambar objek .....	21
Gambar 3.8 Menu utama.....	22
Gambar 3.9 Menu <i>encode</i> .....	23
Gambar 3.10 Tampilan hasil <i>watermarking</i> .....	23
Gambar 3.11 Menu <i>decode</i> .....	24
Gambar 3.12 Menu <i>about</i> .....	24
Gambar 3.13 Menu <i>help</i> .....	25
Gambar 4.1 Halaman utama.....	26
Gambar 4.2 Menu <i>encode watermark</i> .....	27
Gambar 4.3 Tampilan hasil <i>watermark</i> .....	28
Gambar 4.4 Menu <i>decode watermark</i> .....	28
Gambar 4.5 Menu <i>about</i> .....	29
Gambar 4.6 Menu <i>help</i> .....	30

## DAFTAR TABEL

Tabel 2.1 Perubahan nilai pixel citra.....	9
Tabel 3 1 Perubahan pixel citra.....	22
Tabel 4.1 Pengujian <i>encode watermark</i> berhasil .....	31
Tabel 4.2 Pengujian <i>decode watermark</i> berhasil .....	32
Tabel 4.3 Pengujian hasil perhitungan mse, psnr, dan waktu pemrosesan .....	32



## ABSTRAK

*Watermarking* merupakan salah satu cabang dari ilmu steganografi, dimana akan disisipkan pesan ke dalam sebuah gambar, video ataupun audio untuk melindungi objek tersebut dari penyalahgunaan. Pada penelitian ini akan dibangun sebuah sistem *digital watermarking* guna melindungi hak cipta gambar digital yang ada pada media promosi di Fakultas Teknologi Industri Unissula. Pada penulisan ilmiah ini akan dibuat suatu sistem menggunakan metode *modified least significant bit* (MLSB), adapun tahapan dalam pembuatan sistem ini adalah melakukan analisa kebutuhan, perancangan sistem menggunakan UML, serta dalam melakukan pengkodean menggunakan matlab 2016a. Pada metode *modified least significant bit* (MLSB) ini bit yang dipakai tidak hanya bit terakhir lsb tetapi juga bit-2 lsb. Pada tahap pengujian pada beberapa gambar hasilnya tidak adanya perubahan antara gambar asli dan gambar *watermark*.

Kata kunci : *digital watermarking*, gambar digital, *modified least significant bit* (MLSB)

## ABSTRACT

*Watermarking is a branch of steganography, where a message will be inserted into an image, video or audio to protect the object from misuse. In this study, a digital watermarking system will be built to protect the copyright of digital images in promotional media at the Unissula Industrial Technology Faculty. In scientific writing, a system will be made using the modified least significant bit (MLSB) method, while the stages in making this system are conducting requirements analysis, system design using UML, and coding using Matlab 2016a. In the modified least significant bit (MLSB) method, the bit used is not only the last bit of lsb but also bit-2 of lsb. At the testing stage on several images the result is no change between the original image and the watermark image.*

Keywords : *digital watermarking*, digital image, *modified least significant bit* (MLSB)

## **BAB I**

### **Pendahuluan**

#### **1.1 Latar Belakang**

Perkembangan media informasi pada era sekarang ini berkembang sangat pesat dan tidak dapat dibendung lagi, semua orang dapat memperoleh informasi apapun yang diinginkan melalui media internet. Salah satu informasi yang bisa didapat di internet adalah produk digital diantaranya gambar, video, dan audio. Semua itu dapat dengan mudah diambil tanpa kehilangan kualitas aslinya.

Kemudahan dalam penyebaran citra digital mempunyai dampak positif dan negatif bagi pemilik asli citra digital. Sisi positifnya adalah pemilik citra digital lebih mudah menyebar luaskan produk citra digital miliknya ke seluruh media yang ada. Kemudian sisi negatifnya adalah jika tidak ada hak cipta pada produk citra digital maka akan orang lain akan dengan mudah mengakui kepemilikan citra digital tersebut dan bisa menyalahgunakannya.

Di dalam Undang-Undang Hak Cipta (UUHC) Pasal 12 Ayat 1 menjelaskan bahwa Hak cipta memberi sejumlah hak eksklusif kepada pencipta gambar untuk melaksanakan perbanyakan, perubahan, dan melarang orang lain melaksanakan tindakan-tindakan tersebut tanpa seizinnya. Jadi, semua orang tidak boleh menggunakan gambar atau foto untuk menghiasi blog atau konten lainnya tanpa seizin pemilik aslinya. (Istikomah and TBSA, 2014)

Pada media promosi Fakultas Teknologi Industri Unissula terdapat gambar-gambar digital yang perlu diamankan dari tindakan pelanggaran hak cipta yang bisa dilakukan oleh orang yang tidak bertanggung jawab. Salah satu cara yang dapat digunakan untuk melindungi hak cipta ialah dengan menggunakan teknik *watermaking*. *Watermarking* merupakan suatu proses penyisipan kata atau pesan kedalam gambar atau media lain yang berguna untuk melindungi dari tindakan klaim atau dicuri oleh orang lain. Salah satu metode yang digunakan dalam teknik *watermarking* yaitu *modified least significant bit*, yang merupakan metode pengembangan dari metode *least*

*significant bit*. Pada metode *modified least significant bit*, bit-bit data rahasia tidak digunakan mengganti *pixel* yang berurutan, namun dipilih susunan *pixel* secara acak. Pada metode ukuran citra tidak merubah ukuran citra yang sudah disisipi pesan sehingga tidak mengakibatkan kecurigaan akan adanya pesan penanda didalam citra tersebut.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, adapun rumusan masalah dari tugas akhir ini adalah sebagai berikut:

1. Bagaimana cara menjaga hak intelektual dan hak cipta gambar *digital* di Fakultas Teknologi Industri Unissula dari tindakan klaim atau penyalahgunaan gambar digital?
2. Bagaimana cara menghasilkan citra *image* yang *terwatermark* menggunakan teknik Digital *Watermarking* Algoritma *Modified Least Significant Bit*?

## 1.3 Batasan Masalah

Adapun batasan masalah dalam merancang perangkat lunak ini yaitu sebagai berikut:

1. Media yang digunakan berupa gambar.
2. Data yang disisipkan berupa teks.
3. Sistem hanya dapat digunakan oleh satu pengguna.

## 1.4 Tujuan

Tujuan dari tugas akhir ini yaitu :

1. Dapat melakukan labeling pada gambar dan menjaga hak cipta dari gambar digital.
2. Dapat mengimplementasikan Algoritma *Modified least Significant Bit* untuk proses *Digital Watermarking*

## 1.5 Manfaat

Berdasarkan hasil dari penelitian ini penulis mengharapkan manfaat dapat menambah wawasan dan pengetahuan tentang *digital watermarking* yang dapat digunakan untuk melindungi hak cipta gambar *digital*.

## 1.6 Sistematika Penulisan

Sistematika penulisan dalam laporan ini adalah sebagai berikut :

### **BAB 1 Pendahuluan**

Pada bab pendahuluan ini akan disampaikan tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan.

### **BAB II Tinjauan Pustaka dan Dasar Teori**

Pada bab ini berisikan tentang penelitian terdahulu dan dasar teori yang digunakan sebagai acuan dasar dalam pembuatan dan pengembangan sistem.

### **BAB III Metode Penelitian**

Pada bab ini akan memaparkan tentang langkah-langkah metode yang akan ditempuh penulis, analisi perangkat lunak dan keras yang digunakan serta desain sistem yang akan dibuat.

### **BAB IV Hasil dan Analisis Penelitian**

Pada bab ini akan memuat hasil dan implementasi desain sistem, serta pengujian sistem yang telah dibuat.

### **BAB V Kesimpulan dan Saran**

Pada bab ini memuat kesimpulan dari bab sebelumnya dan juga saran yang bertujuan untuk pengembangan sistem selanjutnya.

## BAB II

### Tinjauan Pustaka dan Dasar Teori

#### 2.1 Tinjauan Pustaka

Tinjauan pustaka pertama yaitu penelitian menggunakan metode *modified least significant bit* dan *linier congruential generator* sebagai metode pengacakan *seed*, pada penelitian ini menggunakan media gambar sebagai media penampung dan teks sebagai pesan yang disisipkan. Penelitian ini juga menggunakan pembangkitan bilangan acak atau disebut *pseudo random number* menggunakan metode *linier congruential generator*, yang digunakan sebagai acuan penyisipan pesan secara acak. Pada penelitian ini menghasilkan sebuah gambar *watermark* yang bagus namun kualitas gambar sedikit menurun karena format gambar yang disimpan berubah. (Sulistiyanto dan Luhur, 2017)

Penelitian selanjutnya menggunakan metode *modified least significant bit* (mlsb). Media yang digunakan pada penelitian ini yaitu gambar dan media yang disisipkan sebagai *watermark* juga sebuah gambar. Penelitian ini bit pesan tidak hanya disisipkan pada bit terakhir lsb, namun juga *byte* ke-1,2 dan 3 bit lsb. pada penelitian gambar cover harus 16 kali ukuran gambar gambar pesan untuk meningkatkan tingkat perlindungan. Pada penelitian ini menghasilkan gambar yang tersisipi pesan dengan baik dan ukuran gambar yang sedikit berbeda. (Odat dan Otair, 2016)

Penelitian selanjutnya menggunakan metode *modified least significant bit* (mlsb) yang dikombinasikan dengan lsb+1, dimana pada penelitian ini akan mengubah bit penyisipan menjadi nilai ASCII kemudian bit penyisipan ASCII akan bergabung dengan simbol kontrol ASCII, setelah proses tersebut algoritma akan melakukan proses pengurangan dengan nilai bit terendah. Proses penyisipan pesan ini dilakukan secara acak, dengan menggunakan *pseudo random number* yang akan dipilih untuk tempat penyisipan pesan. Penelitian ini menghasilkan masing-masing kekuatan dan kelebihan masing-masing algoritma yang tentunya mempengaruhi hasil *watermark*. (Lubis *et al.*, 2019)

Selanjutnya menggunakan teknik *watermarking* dan metode LSB berbasis java. Media yang digunakan dalam penelitian ini adalah teks dan juga gambar *digital* yang disisipkan kedalam video. Pada penelitian ini menghasilkan sebuah aplikasi penyisipan teks dan gambar kedalam video. Dimana video yang sudah disisipi *watermark* tidak mengalami perubahan pada tampilan video.(Aini, 2016)

Penelitian selanjutnya menggunakan teknik *watermarking* untuk mengamankan audio digital menggunakan metode *phase coding*. Yaitu metode dimana pergantian fase sinyal audio original dengan satu dari dua fase referensi masing-masing mengkodekan informasi. *Watermark* pada penelitian ini digambarkan menggunakan pergeseran fase yang ada didalam fase tersebut. Penelitian ini menghasilkan sebuah *audio watermark* akan sangat sulit dimanipulasi karena setiap *file* yang *copy* maka *file watermark* akan tetap berada di audio yang telah digandakan.(Fitri, 2015)

Kemudian penelitian menggunakan menggunakan teknik *watermarking* dan *steganografi*, peneliti mengimplimentasikan teknik *visibel watermarking* yaitu sebuah teknik *watermarking* yang dapat dilihat oleh panca indera manusia. Teknik ini dapat bersifat valid dan juga transparan. Kemudian untuk penyisipan *watermark* peneliti menggunakan metode *least significant bit* (LSB) kedalam gambar digital. Dalam penelitian ini dapat disimpulkan bahwa teknik *watermarking* dan *steganografi* dapat digunakan untuk mengamankan sebuah informasi dari pemalsuan dan juga penggandaan yang bersifat ilegal. Dengan menggabungkan kedua teknik ini dapat menghasilkan tingkat keamanan yang tinggi dan lebih sulit untuk dimanipulasi.(Wahyuningsih,dkk 2016)

Selanjutnya peneliti menggunakan *watermarking* sebagai acuan validasi keabsahan sebuah *file* multimedia dengan menggunakan skema *blind watermark*. Kemudahan proses penyisipan menggunakan metode LSB yang mana panjang bit LSB sebanyak 2-bit LSB. penelitian menggunakan dua gambar yaitu gambar warna dan *grayscale*. Teknik ini menjadi alternatif penyisipan *invisible watermarking* dengan mempertimbangkan beberapa koefisien sebagaimana yang telah dipaparkan. Namun pada penelitian

menghasilkan kualitas gambar yang mengalami penurunan kualitas gambar yang signifikan yang dapat dilihat dari hasil perhitungan MSE dan PSNR yang relatif rendah. Kemudian keberhasilan ekstraksi gambar *terwatermark* memudahkan otentifikasi dan validasi kepemilikan gambar digital yang dapat dilihat dari key yang berupa *password* dan id yang merupakan nomor yang unik pemilik gambar. (Suheryadi, 2017)

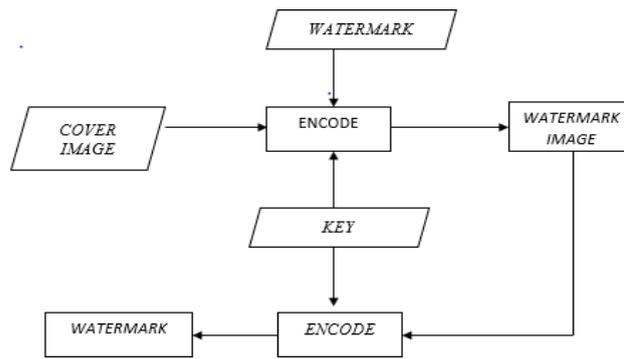
Penelitian selanjutnya menggunakan pengembangan dari metode LSB yaitu *hybird least signifikan bit*. Teknik ini mampu menyisipkan *watermark* dengan baik. Pada teknik *hybird* LSB ini ditambahkan *enkripsi hamming code* dan *repetition code* yang dapat memperbaiki hasil dari *ekstraksi watermark* dibandingkan dengan LSB murni atau klasik. Dengan LSB penyisipan level 1 dan 2 masuk mencolok *watermark*-nya, dan berangsur tak terlihat di level 3 sampai dengan 8. Pada keadaan ini telah memenuhi syarat *watermarking* yaitu tersembunyi atau tak terlihat keberadaannya. (Kurniawan, dkk 2016)

## 2.2 Dasar Teori

### 2.2.1 Digital Watermarking

*Watermarking* sebuah ilmu berakar dari konsep ilmu *steganography*. *Steganography* sendiri merupakan suatu ilmu dan seni yang digunakan untuk menyembunyikan suatu pesan sehingga orang lain tidak dapat melihat atau mendeteksinya.

*Watermarking* merupakan suatu ilmu atau teknik yang digunakan untuk menyembunyikan informasi atau pesan kedalam suatu elemen multimedia seperti citra, video, atau audio. Pada teknik ini informasi yang disisipkan harus dapat diekstrak kembali untuk mendapatkan informasi yang sebelumnya telah disisipkan. Dari pengertian tersebut terdapat 2 tahap dalam proses ini yaitu proses *encode* atau penyisipan dan juga *decode* atau ekstraksi. Proses *watermarking* dapat dilihat pada gambar dibawah ini :



Gambar 2.1 Alur proses watermark

Pada gambar 2.1 diatas dapat dilihat gambar asli akan di-*encode* (disisipi) pesan atau informasi rahasia dan juga kunci tertentu. Dan jika akan memeriksa keasliannya akan dilakukan proses *decode* (ekstraksi) dengan memasukan *key* (kunci) yang sama seperti waktu proses *encode*.(Solichin, 2010)

### 2.2.2 Least Significant Bit (LSB)

*Least significant bit* merupakan salah satu metode yang digunakan untuk menyembunyikan informasi atau pesan rahasia kedalam media digital dengan cara menyisipkan pesan pada bit paling kanan ke *pixel file* obyek. Untuk menyisipkan pesan ke dalam media digital dengan menggunakan metode *LSB modified*. Misalkan untuk menyisipkan suatu segmen pesan hasil dan modulasi sebesar 4 *byte* dengan modifikasi satu bit LSB dibutuhkan 32 data citra digital untuk menampungnya. Dari segmen pesan '1010' dengan 4 *byte* data citra digital sebagai berikut : '01101110 00100011 01000010 01101101'.

Dengan operasi atau prose penggantian bit terakhir dengan 4 bit pesan dengan berurutan menjadi sebagai berikut:

'01101110001000110100001001101101'

Pesan:

1010

Hasil:

'01101111001000100100001101101100'

Dengan adanya sedikit modifikasi ini, maka perubahan yang terjadi pada gambar digital akibat perubahan pada bit tidak terlalu berpengaruh pada kualitas gambar. Berikut merupakan contoh penyisipan karakter A ke dalam sebuah gambar *grayscale* 8 bit dengan ukuran 10x10.

1	6	5	3	7	4	7	4	1	0
3	5	3	5	5	5	5	7	7	0
0	0	0	2	2	6	6	6	6	6
5	5	4	4	4	4	4	4	7	3
2	2	0	0	0	0	1	1	1	1
7	5	5	5	7	7	7	6	3	3
3	3	3	3	3	3	3	3	7	5
5	5	5	5	5	5	5	5	2	3
0	0	0	0	0	0	4	4	4	4
3	3	3	3	3	1	1	1	6	2

• Gambar 2.2 Pixel citra *grayscale* 10 x 10

Langkah pertama yaitu merubah huruf dan juga citra ke dalam bentuk biner, nilai biner dari karakter A yaitu 01000001. Jumlah digit biner dari A hanya 8 digit maka jumlah piksel yang dibutuhkan untuk disisipkan hanya 8 piksel saja. Perhatikan gambar dibawah ini :

8 piksel pertama diambil

1	6	5	3	7	4	7	4	1	0
3	5	3	5	5	5	5	7	7	0
0	0	0	2	2	6	6	6	6	6
5	5	4	4	4	4	4	4	7	3
2	2	0	0	0	0	1	1	1	1
7	5	5	5	7	7	7	6	3	3
3	3	3	3	3	3	3	3	7	5
5	5	5	5	5	5	5	5	2	3
0	0	0	0	0	0	4	4	4	4
3	3	3	3	3	1	1	1	6	2

Gambar 2.3 Pixel citra yang diambil

Langkah berikutnya yaitu bit yang sudah dipilih dengan bit-bit biner dari huruf A seperti tabel dibawah ini :

Tabel 2.1 Perubahan nilai *pixel* citra

Piksel citra yang diambil				
Piksel citra		A	Piksel citra yang berubah	
Desimal	Biner		Desimal	Biner
1	00000001	0	0	00000000
6	00000110	1	7	00000111
5	00000101	0	4	00000100
3	00000011	0	2	00000010
7	00000111	0	6	00000110
4	00000100	0	4	00000100
7	00000111	0	6	00000110
4	00000100	1	5	00000101

Untuk menampung 1 bit data pesan maka diperlukan 1 piksel citra media penampung 8 bit karena 8 bit piksel citra hanya bisa menyembunyikan satu di LSB-nya. Ukuran data maksimum yang bisa disembunyikan dengan menggunakan metode lsb ini adalah seperti contoh berikut:

$$\begin{aligned} \text{media penampung} &: \text{citra } \textit{grayscale} \text{ 8bit berukuran } 64 \times 32 \text{ piksel} \\ \text{ukuran media penampung} &= 64 \times 32 \times 8 \text{ bit} \\ &= 16384 \text{ bit} \end{aligned}$$

1 piksel media penampung = 8 bit.

Oleh karena itu, citra ini hanya bisa menampung maksimum besar pesan  $16384/8 = 2048$  bit dikurangi panjang nama filenya karena dalam penyembunyian data rahasia hanya akan menyembunyikan isi data termasuk nama filenya. Semakin besar ukuran data yang akan disembunyikan, maka semakin besar pula kemungkinan citra penampung rusak akibat manipulasi yang dilakukan. (Sari dkk, 2017)

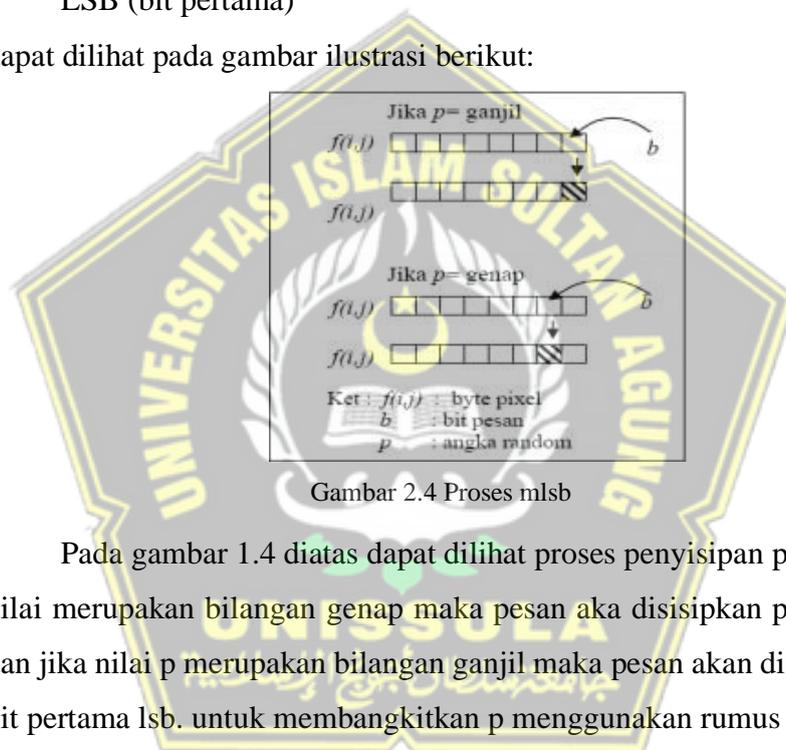
### 2.2.3 *Modified least significant bit*

Metode *modified least significant bit* merupakan sebuah metode pengembangan dari metode lsb murni/klasik, dimana pada metode ini pesan akan disipkan dimedia secara runder atau acak. Bit yang aka dipakai untuk

menyembukan pesan tidak bit pertama melainkan juga bit yang kedua. Pada metode ini akan dilakukan pembangkitan angka random dari sebuah fungsi random generator yang akan dibuat sebagai acuan untuk penyisipan pesan. Proses metode ini dapat dilihat pada gambar berikut:

- a) Bangkitkan *pseudo random number* ( $p$ )
- b) Proses penyembunyian bit pesan dengan aturan sebagai berikut :
  - Jika nilai  $p$  merupakan bilangan genap, sisipkan pesan bit LSB (bit kedua)
  - Jika nilai  $p$  merupakan bilangan ganjil, maka sisipkan pesan pada bit LSB (bit pertama)

dapat dilihat pada gambar ilustrasi berikut:



Gambar 2.4 Proses mlsb

Pada gambar 1.4 diatas dapat dilihat proses penyisipan pesan yaitu jika nilai merupakan bilangan genap maka pesan akan disisipkan pada bit kedua, dan jika nilai  $p$  merupakan bilangan ganjil maka pesan akan disisipkan pada bit pertama lsb. untuk membangkitkan  $p$  menggunakan rumus :

$$X_n = (7X_{n-1} + 11) \text{ Mod } 17 \quad (1)$$

$X_n$  = bilangan acak ke- $n$  dari deretannya                       $a$  = faktor pengali

$X_{n-1}$  = bilangan acak sebelumnya                                       $b$  = *increment*

$m$  = *modulus*

Pembangkitan bilangan acak ini disebut dengan LCG (*linier congruential generator*) (Laksito, 2008)

#### 2.2.4 Digital Image

*Digital image* adalah sebuah *image*  $f(x,y)$  yang sudah dibuat pada koordinat spasial menggunakan tingkat intensitas cahaya tertentu. *Digital*

*image* bisa ditampilkan sebagai matriks dua dimensi menggunakan baris dan juga kolom (x,y) *image*, sementara elemennya akan menyakan nilai warna dalam posisi tertentu sesuai cara penyimpanannya. Format *image* dibagi menjadi dua bagian yaitu *format raster* (bitmap) dan juga format vektor. Format raster akan menyimpan seluruh *image* secara apa adanya, sesuai apa yang ditampilkan pada layar bitmap itu sendiri, sebagai sebuah array yang berisi titik-titik kecil dan juga persegi.

Adapun tipe-tipe *file* untuk menyimpan *image bitmap* dapat berupa seperti berikut:

- a) *Bitmapped file* (\*.BMP)
- b) *Graphics Image Format* (\*.GIF)
- c) *Image* (\*.IMG)
- d) *PC Paint Brush Format* (\*.pcx)
- e) *Tagged Image File Format* (\*.TIFF)
- f) *Joint Photographic Expert Group* (\*.JPEG)(Tullah *et al.*, 2014)

#### 2.2.5 MSE Dan PSNR

Pengolahan citra mempunyai standar pengukuran kualitas citra yaitu MSE dan PSNR. *Peak signal to Noise Ratio* digunakan untuk mengukur tingkat performa dan keberhasilan dari sebuah metode *filtering* pada sebuah citra. Tingkat pengukuran setiap orang berbeda-beda. Jadi akan lebih baik jika menggunakan MSE dan PSNR untuk pengukuran performa yang lebih baik.

PSNR (*Peak signal to Noise Ratio*) merupakan sebuah perhitungan untuk menentukan sebuah nilai pada citra. Besar kecilnya nilai MSE yang terjadi pada citra akan mempengaruhi nilai PSNR. PSNR akan dinyatakan dalam skala *decibel* (dB) dalam bentuk logaritma. Semakin kecil nilai PSNR, hasil yang akan didapatkan semakin kurang baik. Sebaliknya jika nilai PSNR besar, hasil yang akan didapatkan juga akan semakin baik. Jadi antara MSE dan PSNR mempunyai hubungan nilai yang semakin kecil.

MSE (*Mean Square error*) merupakan sebuah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi. Nilai MSE dapat diperoleh dengan cara membandingkan nilai citra hasil pada posisi *pixel* yang sama dengan selisih pixel citra asal. Misal  $s_{xy}$  merupakan citra masukan  $C_{xy}$

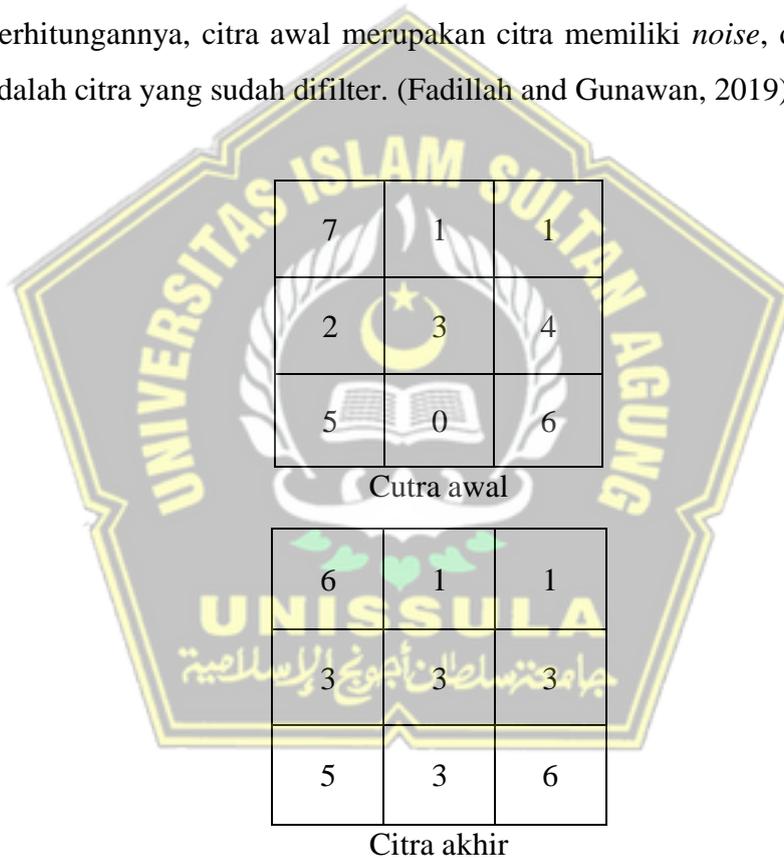
adalah citra keluaran, citra tersebut mempunyai M baris dan N kolom, maka dapat didefinisikan seperti berikut:

$$MSE = \frac{1}{MN} \sum_{x=1}^m \sum_{y=1}^n (S_{xy} - C_{xy})^2 \quad (2)$$

Rumus menghitung PSNR yaitu :

$$PSNR = 20 \cdot \log_{10} (MAX_1) - 10 \log_{10} (MSE) \quad (3)$$

Nilai PSNR dibawan 30dB akan mengindikasikan kualitas yang relatif rendah, dimana distorsi yang dikarenakan penyisipan akan terlihat dengan jelas. Akan tetapi kualitas *stego-image* dengan nilai 40dB atau di atasnya mempunyai nilai yang tinggi. Dibawah ini merupakan contoh perhitungannya, citra awal merupakan citra memiliki *noise*, dan citra akhir adalah citra yang sudah difilter. (Fadillah and Gunawan, 2019)



$$MSE = \frac{(7-6)^2 + (1-1)^2 + (1-1)^2 + (2-3)^2 + (3-3)^2 + (4-3)^2 + (5-5)^2 + (0-3)^2 + (6-6)^2}{3 \times 3}$$

$$MSE = \frac{1+0+0+1+0+1+0+9+0}{9} = 1,33$$

$$PSNR = 10 \log_{10} \left( \frac{7}{\sqrt{1,33}} \right) = 8,25925$$

### 2.2.6 Matlab

Matlab merupakan kependekan *matrix laboratory* karena setiap data yang terdapat matlab menggunakan dasar *matriks*. Matlab dikembangkan oleh MathWorks. Salah satu kelebihan yang ada pada matlab yaitu kemampuan dalam grafik dengan kustomisasi terbaik saat ini.

Didalam matlab terdapat banyak *tools* yang dapat membantu berbagai disiplin ilmu. Selain itu, matlab juga memiliki *library* yang sangat membantu dalam penyelesaian berbagai masalah matematis seperti pembuatan simulasi fungsi, perancangan GUI dan pemodelan matematika. Berikut merupakan bagian utama dari matlab yaitu :

- 1 *Development environment*, yaitu kumpulan perangkat dan fasilitas yang dapat membantu untuk menggunakan fungsi-fungsi dan *file-file* yang ada pada matlab.
- 2 *Matlab mathematical function library*, yaitu kumpulan algoritma komputasi mulai fungsi-fungsi dasar seperti : *sin*, *cos*, sampai dengan fungsi yang lebih kompleks lagi seperti *matrix inverse*.
- 3 *Matlab language*, yaitu suatu *high level matrix/array* dengan *control flow* statement dan lainnya.

*Matlab application program interface*, yaitu suatu *library* yang dapat memungkinkan program yang telah kita buat dalam bahasa C berinteraksi dengan matlab. (ikhsanparinduri, 2018).

## BAB III

### Metode Penelitian

#### 3.1 Metode Penelitian

Metode penelitian yang akan digunakan dalam pembuatan tugas akhir ini adalah sebagai berikut :

##### 3.3.1. Pengumpulan Data

Langkah yang digunakan untuk pengumpulan data untuk penelitian ini adalah sebagai berikut :

- a. Data yang digunakan dalam penelitian berasal dari tim promosi melalui link [s.id/videoFTI](http://s.id/videoFTI) dan media sosial Fakultas Teknologi Industri Unissula
- b. Studi literatur dalam penelitian dilakukan dengan mencari dan mempelajari tentang ilmu *watermarking* dan metode *modified least significant bit* (MLSB) dari internet, buku, jurnal dan materi-materi lainnya yang berkaitan dengan penelitian ini.

##### 3.3.2. Metode pengembangan sistem

Metode pengembangan sistem yang digunakan dalam penelitian ini yaitu metode pengembangan *prototyping*. Metode *prototyping* ini merupakan suatu metode pengembangan perangkat lunak melalui pendekatan yang bertujuan untuk membuat rancangan perangkat lunak dengan cepat dan bertahap sehingga dapat segera dievaluasi. Pada metode ini pengembang akan melakukan penyesuaian-penyesuaian untuk menghasilkan sebuah sistem yang lebih baik. Adapun tahapan metode *prototype* adalah sebagai berikut :

###### a) Identifikasi kebutuhan

Pada tahapan ini dilakukan identifikasi kebutuhan dan pengumpulan data yang nantinya akan digunakan sebagai acuan dalam pengembangan sistem

###### b) Membangun dan memperbaiki *Prototype*

Setelah proses identifikasi dan pengumpulan data selesai dilakukan, selanjutnya akan dilakukan proses perancangan *prototype*, seperti proses *input* dan *output*, perancangan UML (*Unified modelling language*) dan *user interface* (UI). Setelah semua proses dilakukan, akan dilakukan evaluasi dan perbaikan sistem sesuai kebutuhan.

### c) Pengujian *Prototype*

pada tahap ini akan dilakukan proses pengujian dan evaluasi *prototype* apakah sudah sesuai dengan yang diharapkan. Apabila pada proses pengujian ini belum memenuhi kebutuhan akan dilakukan evaluasi dan perbaikan kembali *prototype* sampai menjadi sebuah sistem sesuai kebutuhan.

## 3.2 Perancangan sistem secara umum

Sistem yang akan dikembangkan oleh penulis merupakan sebuah sistem *encode* dan *decode watermark* ke dalam sebuah gambar digital menggunakan algoritma *modified least significant bit (mlsb)*. Dimana setelah proses *encode* atau proses penyisipan *watermark* berhasil dilakukan, maka akan dilakukan proses *decode watermark* (ekstraksi pesan) dengan memasukan gambar *watermark* dan *password* sesuai pada saat awal proses penyisipan pesan, sehingga *watermark* atau pesan rahasia dapat kembali diekstrak.

## 3.3 Analisa perangkat keras

1. TOSHIBA ASPIRE E1-410
2. Prosesor intel celeron N2820
3. RAM 4GB
4. 320 GB HDD

## 3.4 Analisa perangkat lunak

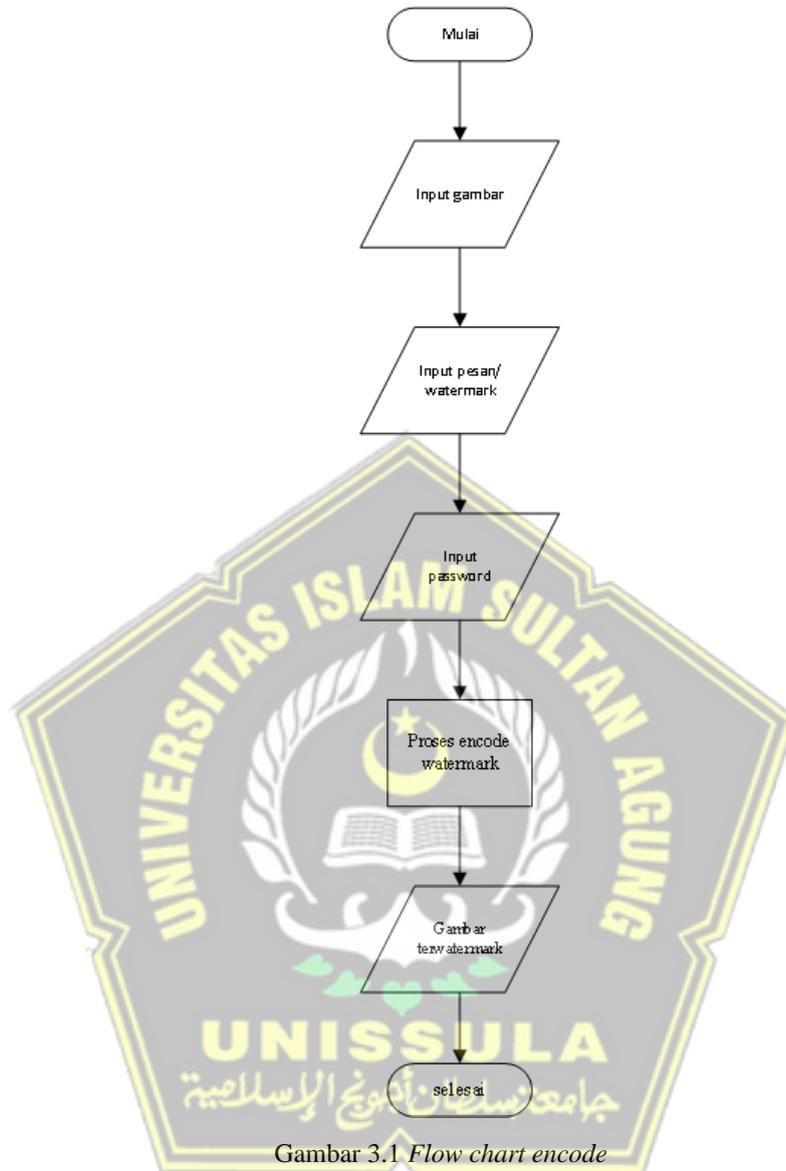
Perangkat lunak yang digunakan dalam penelitian ini menggunakan matlab 2016a, dimana matlab versi ini sudah mumpuni untuk digunakan dan cukup ringan untuk digunakan sesuai dengan spek perangkat keras yang digunakan.

## 3.5 Perancangan arsitektur sistem

Berikut ini merupakan *flow chart* proses *encode* dan *decode watermark* pada sistem yang akan dibuat :

### 3.5.1. Proses *encode*

*Flow chart* proses *encode watermark* adalah sebagai berikut :



Gambar 3.1 *Flow chart encode*

Penjelasan dari proses *encode* pada gambar diatas adalah sebagai berikut :

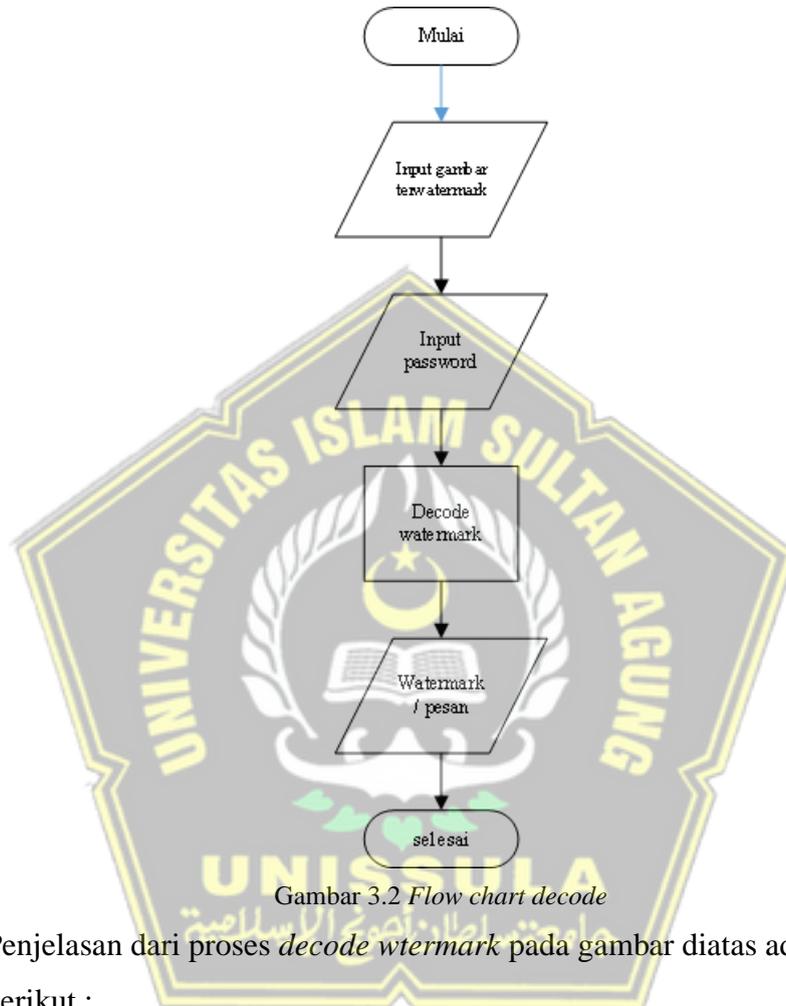
- Memulai program.
- Memasukan gambar yang akan disisipi oleh *watermark*.
- Kemudian memasukan *watermark* yang berupa teks yang akan disisipkan ke dalam gambar digital.
- Kemudian memasukan *password* yang merupakan *key* untuk nantinya digunakan untuk mengekstrak *watermark* kembali.
- Selanjutnya yaitu proses *encode watermark* yaitu proses penyisipan *watermark* ke dalam gambar digital menggunakan metode *mlsb*.

f. Setelah semua proses selesai akan dihasilkan sebuah gambar yang sudah tersisipi *watermark*.

g. Selesai.

### 3.5.2. Proses *decode*

*Flow chart* proses *decode watermark* adalah sebagai berikut :



Gambar 3.2 *Flow chart decode*

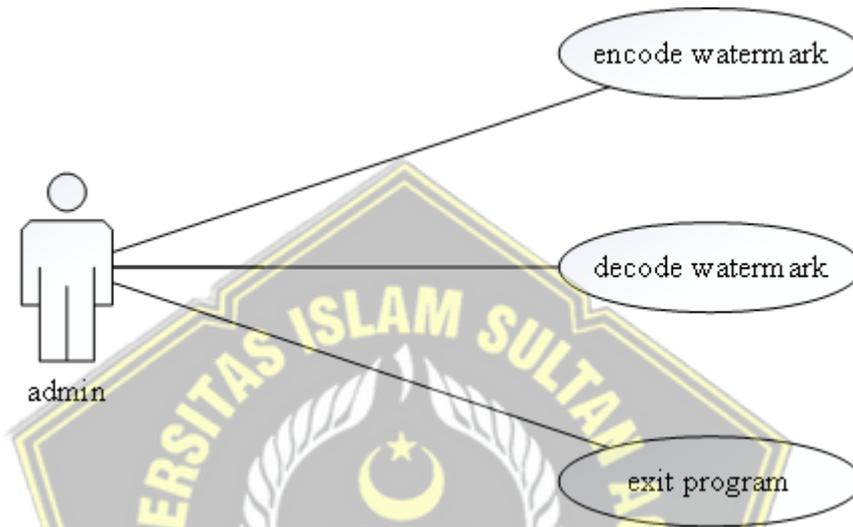
Penjelasan dari proses *decode watermark* pada gambar diatas adalah sebagai berikut :

- Memulai program
- Memasukan gambar yang sudah disisipi *watermark* atau pesan tersembunyi
- Memasukan *password* sesuai dengan saat proses penyisipan *watermark*.
- Kemudian sistem akan melakukan proses *decode watermark* yaitu proses ekstraksi pesan rahasia yang sudah disisipkan ke dalam gambar digital.
- Setelah proses ekstraksi atau *decode* maka *watermark* atau pesan rahasia akan tampil layar sistem
- Selesai.

### 3.6 Perancangan sistem

#### 3.6.1 Use case diagram

*Use case* diagram merupakan salah satu dari berbagai jenis diagram dari UML (*Unified Modelling Language*) yang merupakan gambaran interaksi dari *user* dengan sistem. Berikut merupakan *use case* diagram dari penelitian ini :

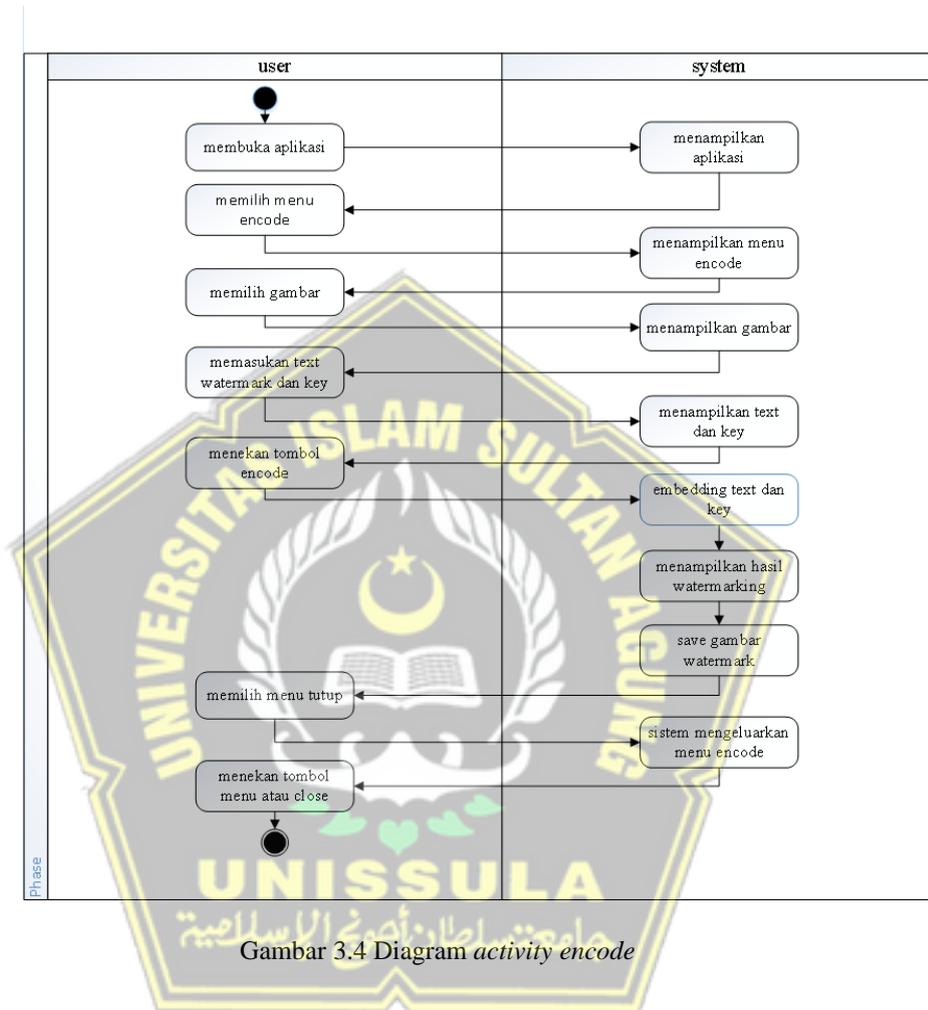


Gambar 3.3 Use case diagram

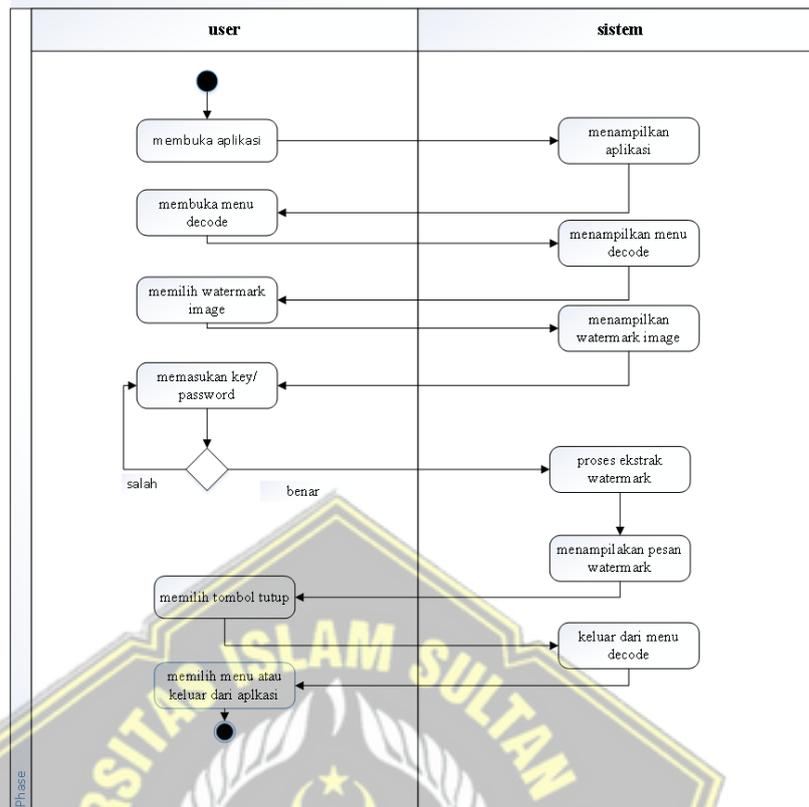
Gambar diatas merupakan *use case* diagram sistem dimana pada diagram tersebut terdapat satu aktor yaitu admin sebagai pengguna. Adapun aktifitas yang dapat dilakukan admin adalah pertama *encode watermark*, yaitu proses penyisipan pesan *watermark* ke dalam sebuah gambar *digital*. Kemudian aktifitas selanjutnya adalah *decode watermark* yaitu proses ekstraksi *watermark* yang telah disisipkan pada gambar digital sebelumnya. Dan aktifitas terakhir yaitu keluar dari program atau sistem yang berarti mengakhiri proses yang telah dilakukan.

### 3.6.2 Activity diagram

Activity diagram merupakan diagram yang menunjukkan proses-proses yang terjadi pada sebuah sistem. Activity diagram merujuk pada diagram *use case* sebelumnya yaitu proses *encode watermark* dan *encode watermark*. Berikut merupakan diagram *activity* pada sistem yang telah dibuat :



Gambar 3.4 Diagram activity encode



Gambar 3.5 Diagram *activity decode*

### 3.7 Metode *Modified Least Significant Bit (MLSB)*

Berikut merupakan Langkah metode *modified least significant bit (MLSB)* yaitu pertama membangkitkan nilai *pseudo random number generator*, disini menggunakan *password (seed)* dengan nilai 1 dan dihitung menggunakan rumus  $X_n = (7 X_{n-1} + 11) \bmod 17$  akan dihasilkan *random number* sebagai berikut :

n	Xn	ket
1	9	ganjil
2	6	genap
3	8	genap
4	16	genap
5	4	genap
6	5	ganjil
7	12	genap
8	10	genap
9	13	ganjil

Gambar 3.6 Hasil *random number*

Setelah *pseudo random number* dibangkitkan, selanjutnya akan dilakukan proses *watermarking* kedalam sebuah gambar. Disini akan menggunakan gambar *grayscale* dengan ukuran  $720 \times 479$  *pixel* sehingga akan dihasilkan matrik  $720 \times 479$ .



Gambar 3.7 Gambar objek

130 128 122 122 126 118 128 138 142 140  
128 122 112 112 118 116 128 142 148 148  
126 124 120 114 112 116 124 136 144 146  
126 128 126 124 122 120 126 134 140 140  
134 136 134 132 130 126 126 128 126 122  
138 140 138 138 136 128 124 120 114 106

disini akan disisipkan huruf A, kemudian akan dikonversikan kedalam bentuk biner yaitu

$$A = 01000001,$$

setelah itu pesan (*watermark*) akan disisipkan dengan pola jika nilai  $p$  (*random number*) bernilai ganjil *bit* pesan akan disisipkan ke *bit* lsb pertama dan jika nilai  $p$  bernilai genap *bit* pesan akan disisipkan ke *bit* ke-2 lsb, dapat dilihat seperti dibawah ini :

Tabel 3 1 Perubahan pixel citra

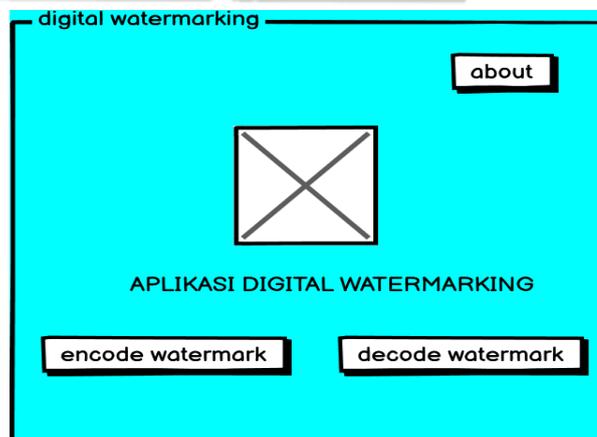
Prng	10	12	5	4	16	8	6	9
Biner citra	100000 0	100000 0	0111101 0	011110 0	011111 0	011101 0	100000 0	1000101 0
	128	130	122	120	124	116	128	139

Pada setiap *bit* pertama dan kedua lsb digantikan dengan *bit* pesan yang telah disisipkan. Pergantian ini tidak terlihat kasat mata karena perubahan nilai sangat kecil. Sehingga jika dikembalikan ke bentuk citra asli akan nampak seperti semula tanpa ada perubahan pada citra yang sudah disisipi *watermark*. Perubahan nilai matrik *citra* dapat dilihat dibawah ini :

128 130 122 120 124 116 128 139 142 140  
 128 122 112 112 118 116 128 142 148 148  
 126 124 120 114 112 116 124 136 144 146  
 126 128 126 124 122 120 126 134 140 140  
 134 136 134 132 130 126 126 128 126 122  
 138 140 138 138 136 128 124 120 114 106

### 3.8 Perancangan user interface

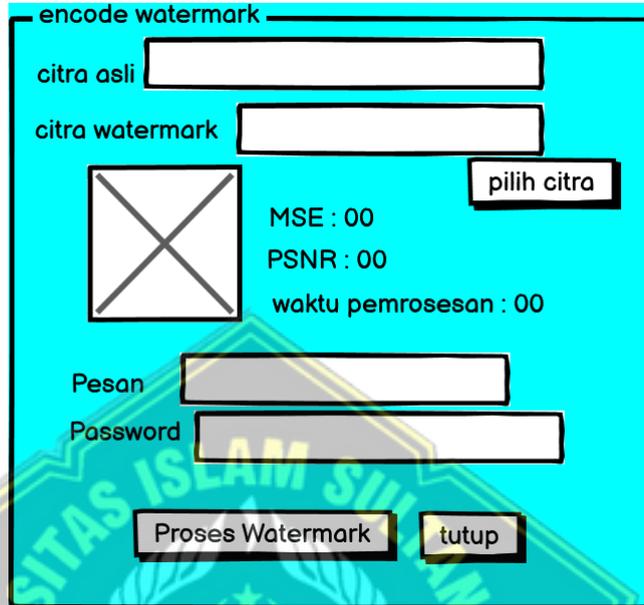
#### 1. Halaman utama



Gambar 3.8 Menu utama

Pada gambar 3.6 merupakan halaman utama pada saat sistem dimulai, pada halaman utama berisikan menu-menu antara lain menu *encode watermark*, *decode watermark*, dan *about*.

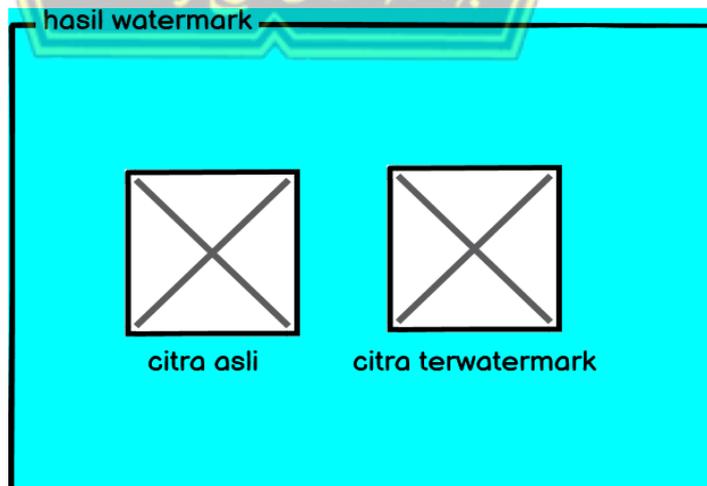
## 2. halaman encode



Gambar 3.9 Menu *encode*

Pada gambar 3.7 merupakan tampilan halaman menu *encode watermark* pada halaman ini proses penyisipan *watermark*. pada menu ini terdapat menu pilih cita, *form* nama cita *watermark* yang akan disimpan, nilai mse, psnr dan waktu pemrosesan, *form* pesan *watermark*, *form* password, *button* proses *watermark* dan tutup.

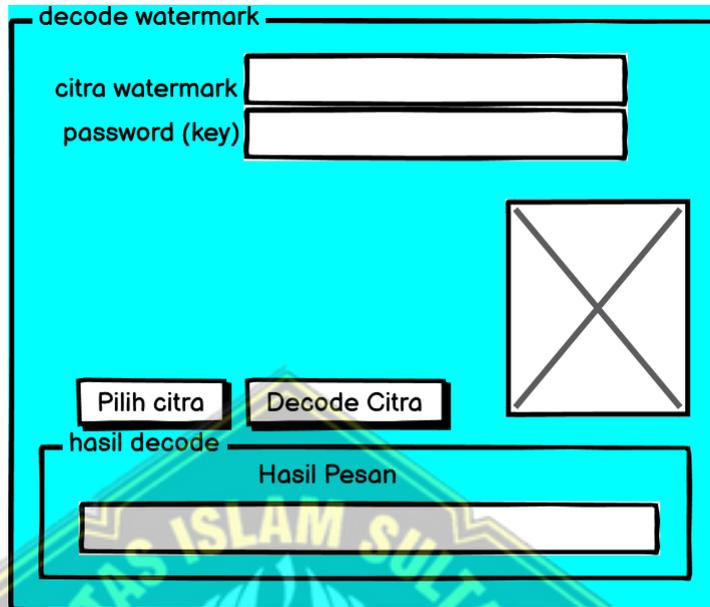
## 3. Tampilan hasil *encode watermark*



Gambar 3.10 Tampilan hasil *watermarking*

Pada gambar 3.8 merupakan tampilan setelah proses *watermarking* berhasil dilakukan dimana akan ditampilkan antara citra asli dan citra *watermark*

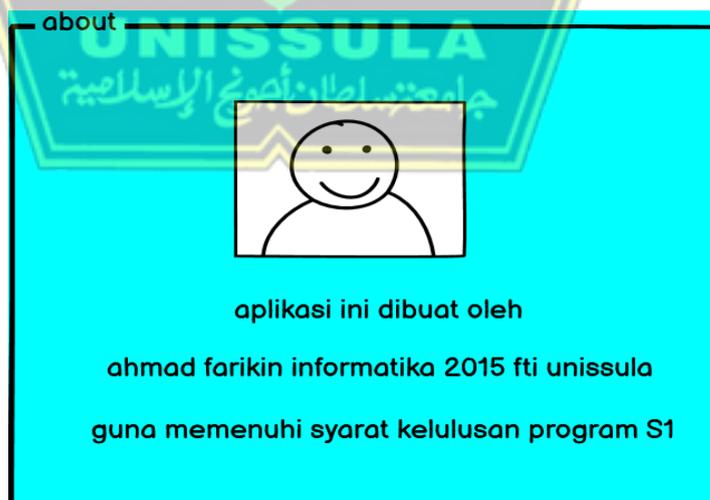
#### 4. Tampilan menu *encode watermark*



Gambar 3.11 Menu *decode*

Pada gambar 3.9 merupakan tampilan dari menu *decode watermark*, pada menu ini pesan *watermark* yang sudah disisipkan pada citra akan diekstrak kembali menggunakan *password* pada saat awal proses penyisipan dilakukan.

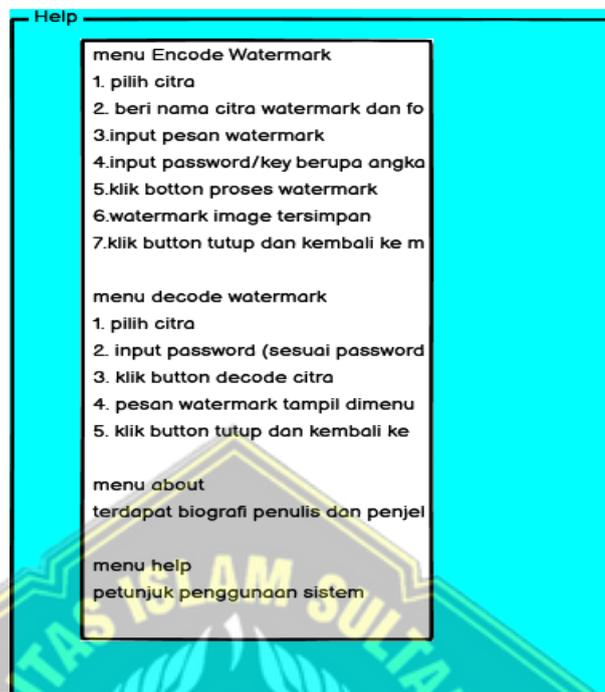
#### 5. Tampilan menu *about*



Gambar 3.12 Menu *about*

Pada gambar 3.10 merupakan desain menu *about*, akan ditampilkan profil dari penulis dan penjelasan singkat mengenai sistem yang akan dibuat.

6. menu help



Gambar 3.13 Menu *help*

Pada gambar 3.11 merupakan menu *help* berisi tentang petunjuk singkat cara penggunaan sistem.

## BAB IV

### Hasil dan Analisis Penelitian

#### 4.1. Implementasi Sistem

Implementasi merupakan tahapan lanjutan dari penerapan rancangan desain sistem sebelumnya. Pada tahap ini rancangan desain selanjutnya akan diubah ke dalam bentuk yang bisa dipahami oleh mesin melalui proses coding. Berikut merupakan beberapa implementasi sistem yang sudah dibuat

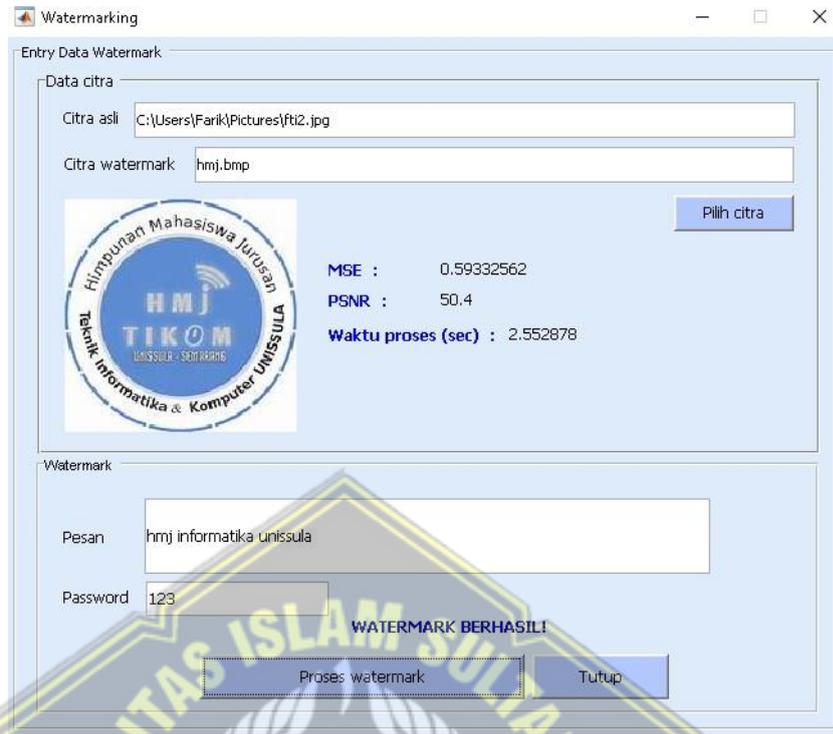
##### 1. Halaman Utama



Gambar 4.1 Halaman utama

Gambar 4.1 merupakan tampilan dari halaman awal sistem aplikasi *digital watermarking*. Pada menu ini terdapat empat menu utama yaitu menu *encode watermark*, *decode watermark*, *about*, dan *help*.

## 2. Halaman *encode watermark*



Gambar 4.2 Menu *encode watermark*

Gambar 4.2 merupakan halaman *encode watermark*, dimana pada menu ini penyisipan pesan *watermark* akan dilakukan. Pada tahap *encode* ini yang pertama dilakukan oleh *user* yaitu memilih citra yang akan di *watermarking*, setelah itu memberi dan *format citra watermark* yang nantinya akan disimpan, kemudian *user* harus menulis pesan *watermark* pada *form* pesan, dilanjutkan menambahkan *password*, kemudian mengklik tombol proses *watermark* hingga muncul tulisan *watermark* berhasil. Pada menu ini juga akan menampilkan perhitungan MSE, PSNR, dan juga lama waktu pemrosesan *encode watermark* dalam satuan *second*.

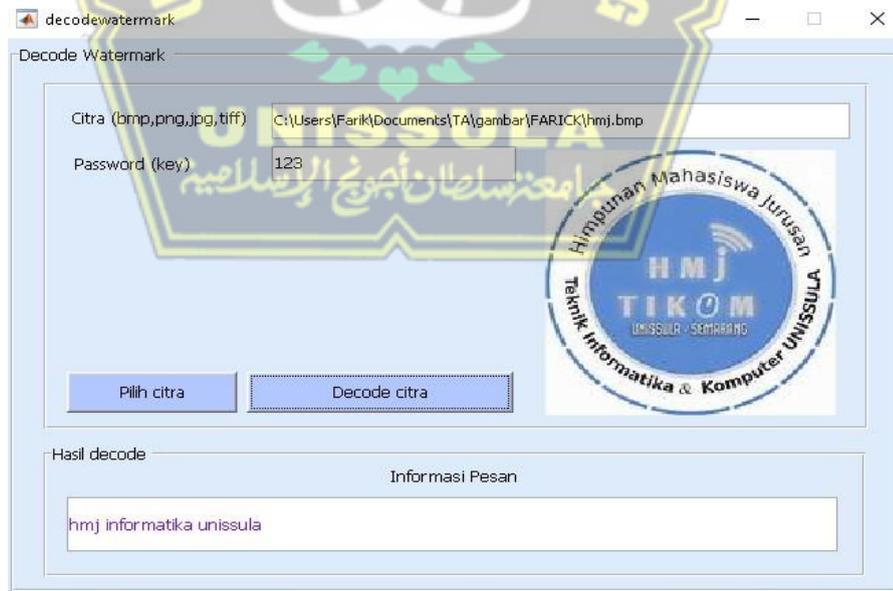
### 3. tampilan hasil



Gambar 4.3 Tampilan hasil *watermark*

Gambar 4.3 merupakan tampilan hasil dari *encode watermark*, dimana akan ditampilkan citra asli dan citra setelah diberi *watermark*.

### 4. Menu *decode watermark*

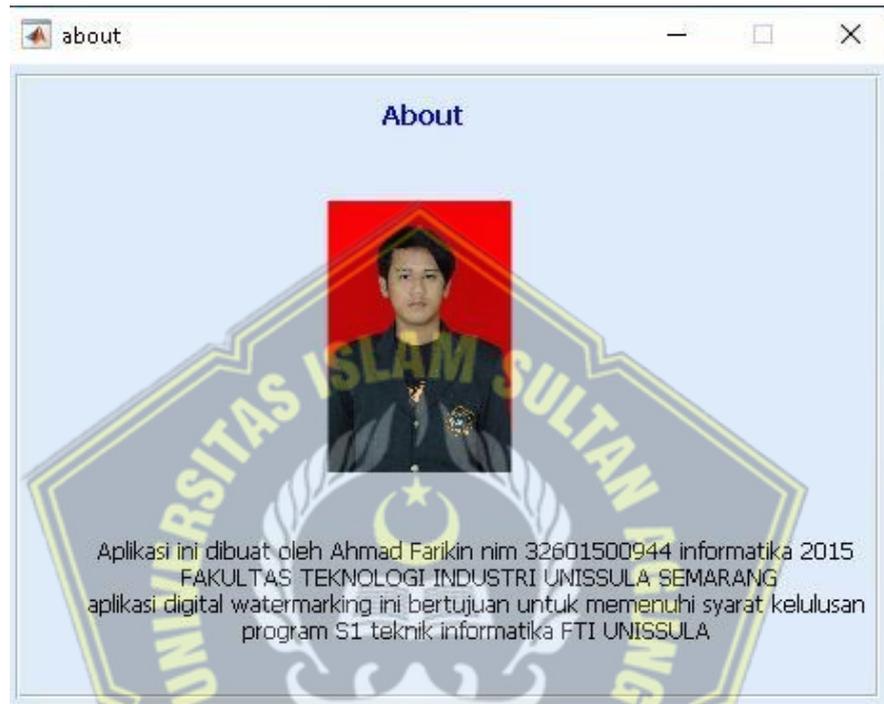


Gambar 4.4 Menu *decode watermark*

Gambar 4.4 merupakan tampilan dari menu *decode watermark*, pada menu ini proses *decode* atau *ekstrak* dari *watermark* yang sudah disisipkan

sebelumnya akan dilakukan. Langkah pertama dalam proses ini yaitu memilih *citra watermark* kemudian memasukkan *password* yang sama pada saat proses awal penyisipan. Setelah semua sudah dilakukan kemudian *user* mengklik *button decode watermark*, kemudian jika proses berhasil pesan *watermark* akan muncul pada *form* informasi pesan.

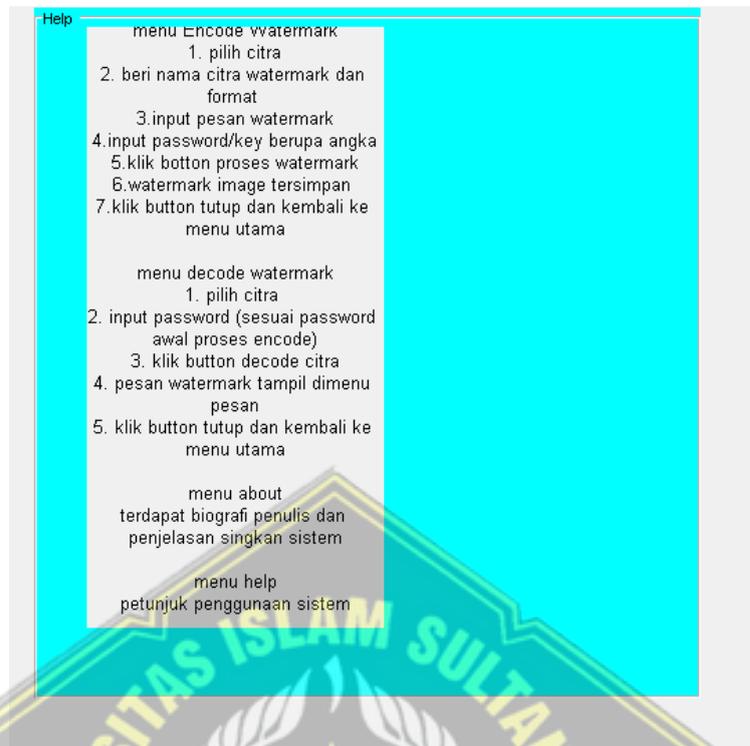
#### 5. Menu *about*



Gambar 4.5 Menu *about*

Gambar 4.5 merupakan tampilan dari menu *about* dimana didalamnya berisikan ulasan singkat dari penulis.

## 6. Menu help



Gambar 4.6 Menu *help*

Gambar 4.6 merupakan tampilan dari menu *help* , pada menu ini berisikan penjelasan singkat tentang tata petunjuk penggunaan sistem

### 4.2. Pengujian dengan sistem *black box*

Pengujian *black box* merupakan sebuah metode pengujian sistem perangkat lunak yang hanya berfokus pada fungsionalitas sebuah aplikasi tanpa melihat struktur kerja internal yang ada didalam sistem. Berikut merupakan hasil dari pengujian *black box testing*:

Tabel 4.1 Pengujian *encode watermark* berhasil

Citra asli		Pesan <i>watermark</i>	<i>password</i>	status
Nama	size	Isi pesan		
 Fti.png	256 kb (4252x3507 Pixel)	Logo fakultas teknologi industri unissula	123456	Watermark Berhasil
 Budai.png	289 kb (1863x1863 Pixel)	Logo budai	123456	Watermark berhasil
 IMG_6994.png	16,2 MB (5485x5472 pixel)	Foto promosi fti	123456	Watermark berhasil
 mrt.jpg	194 kb (1152x864 pixel)	Tim mobil listrik fti	123456	Watermark berhasil
 Hmj.tif	7,16 kb (160x162 pixel)	Logo hmj tif	123456	Watermark berhasil

Tabel 4.2 Pengujian *decode watermark* berhasil

Citra watermark	Password	Isi watermark	Hasil
 Fti.bmp	123456	logo fakultas teknologi industri unissula	Berhasil
 Budai.bmp	123456	logo budai	Berhasil
 Img_6994.bmg	123456	foto promosi fti	Berhasil
 mrt.bmp	123456	Tim mobil listrik fti	Berhasil
 Hmj.tif	123456	logo hmj tif	Berhasil

Tabel 4.3 Pengujian hasil perhitungan mse, psnr, dan waktu pemrosesan

citra asli		Pesan watermark	MSE	PSNR	Waktu pemrosesan (second)
Nama	Size				
 Fti.png	256 kb (4252x3507 Pixel)	logo fakultas teknologi industri unissula	0.39713048	52,2	548,669661

citra asli		Pesan watermark	MSE	PSNR	Waktu pemrosesan (second)
Nama	Size				
 Budai.png	289 kb (1863x1863 Pixel)	logo budai	0,43950385	51,7	119,335465
 Img_6994.png	16,2 MB (5485x5472 pixel)	foto promosi fti	0.13440545	56,9	1159413066
 mrt.jpg	194 kb (1152x864 pixel)	tim mobil listrik	0,53924569	50,8	40.062843
 Hmj.tif	7,16 kb (160x162 pixel)	logo hmj tif	0,59367284	50,4	1.750038

## BAB V

### Kesimpulan dan Saran

#### 5.1. Kesimpulan

Dari hasil penulisan dan uji coba diatas dapat diberi kesimpulan bahwa *digital watermarking* menggunakan metode *modified least significant bit* (MLSB) dapat dengan mudah digunakan untuk melindungi hak karya cipta dari pemalsuan. Metode ini menghasilkan perubahan warna yang tidak signifikan, sehingga tidak terlihat oleh mata namun bisa dideteksi melalui perhitungan. Pada tahapan uji coba *watermark* yang berupa teks dapat disisipkan dengan baik ke dalam gambar digital. Namun metode ini masih perlu dikembangkan lagi karena untuk memproses gambar yang berukuran besar dan pesan yang panjang masih membutuhkan waktu proses yang lumayan lama, sehingga itu menyebabkan kurangnya efisiensi waktu. Metode ini akan lebih baik jika digabungkan dengan teknik-teknik steganografi lainnya, untuk memperkuat ketahanan *watermark* dari tindakan pemalsuan.

#### 5.2. Saran

Adapun saran penulis dalam melanjutkan pengembangan sistem yaitu perlu melakukan pengembangan lebih lanjut mengenai metode ini, khususnya pada tahapan pengacakan bit sehingga pesan yang telah disisipkan akan lebih sulit untuk dideteksi. Kemudian dapat juga dikombinasikan dengan teknik-teknik steganografi lainnya untuk memperkuat ketahanan citra *watermark* dari tindakan pemalsuan citra.

## Daftar Pustaka

- Aini, N. (2016) 'Aplikasi Penanda Digital ( Watermarking ) File Video Dengan Metode Least Significant Bit ( Lsb ) Implementasi : Java Programming',
- Fadillah, N. And Gunawan, C. R. (2019) 'Mendeteksi Keakuratan Metode Noise Salt And Pepper Dengan Median Filter', *Jurnal Informatika*, 6(1), Pp. 91–95. Doi: 10.31311/Ji.V6i1.5439.
- Fitri, Z. (2015) 'Audio Digital Watermarking Untuk Melindungi Data Multimedia', *Techsi*, 6(1), Pp. 190208. Available at <http://Ejournal.Tif.Unimal.Ac.Id/Index.Php/Ejournal/Article/View/86>.
- Ikhsan Parinduri (2018) 'Perangkaian Gerbang Logika Dengan Menggunakan Matlab ( Simulink )', V(1).
- Istikomah And TBSA (2014) 'Perlindungan Hukum Terhadap Hak Cipta Menurut Pasal 12 Undang-Undang Nomor 28 Tahun 2014 Tentang Hak Cipta Di Indonesia', 12(2007), Pp. 703712. Available at: <https://Hsgm.Saglik.Gov.Tr/Depo/Birimler/Saglikli-Beslenme-Hareketli-Hayat-Db/Yayinlar/Kitaplar/Diger-Kitaplar/TBSA-Beslenme-Yayini.Pdf>.
- Kurniawan, K., Siradjuddin, I. A. And Muntasa, A. (2016) 'Keamanan Citra Dengan Watermarking Menggunakan Pengembangan Algoritma Least Significant Bit', *Jurnal Informatika*, 13(1), Pp. 9–14. Doi: 10.9744/Informatika.13.1.9-14.
- Laksito, W. (2008) 'Modifikasi Least Significant Bit Dalam Steganografi', *Jurnal Ilmiah SINUS*, 6, Pp. 1–8.
- Lubis, R. R. A. *Et Al.* (2019) 'Analysis On Combination Of Watermarking Algorithm: Modified Least Significant Bit Algorithm With Least Significant Bit+1', *Journal Of Physics: Conference Series*, 1235(1), Pp. 0–6. Doi: 10.1088/1742-6596/1235/1/012081.
- Odat, A. M. And Otair, M. A. (2016) 'Image Steganography Using Modified Least Significant Bit', *Indian Journal Of Science And Technology*, 9(39). Doi: 10.17485/Ijst/2016/V9i39/86878.
- Sari, J. I., Sulindawaty And Sihotang, H. T. (2017) 'Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma HILL Cipher Dan Metode Least Significant BIT (LSB)', *Jurnal*

*MantikPenusa*,1(2),Pp.1Availableat:Http://Ejurnal.Pelitanusantara.Ac.Id/Index.Php/Mantik/Article/View/253/

- Solichin, A. (2010) 'Digital Watermarking Untuk Melindungi Informasi Multimedia', *Budi Luhur Information Technology (BIT)*, 7(1), Pp. 1–08.
- Suheryadi, A. (2017) 'Penerapan Digital Watermark Sebagai Validasi Keabsahan Gambar Digital Dengan Skema Blind Watermark', *JTT (Jurnal Teknologi Terapan)*, 3(2), Pp. 1–6. Doi: 10.31884/Jtt.V3i2.54.
- Sulistyanto, A. And Luhur, U. B. (2017) 'Digital Watermarking Pada Citra Menggunakan Metode Modified Least Significant Bit ( MLSB ) Dengan Penyebaran Pesan Secara Acak Menggunakan Metode Linear Congruential Generator ( LCG ): Studi Laboratorium ICT Terpadu Universitas BUDI LUHUR Agung Sulistyant', (August). Doi: 10.13140/RG.2.2.14857.13926.
- Tullah, R. *Et Al.* (2014) 'Perancangan Steganografi Dengan Media Gambar Pada Aplikasi Berbasis Android', *Jurnal Sisfotek Global*, 1(1), Pp. 1–7.
- Wahyuningsih, S., Pandex, T. V. D. And Stefanny, V. (2016) 'Implementasi Visible Watermarking Dan Steganografi Least Significant Bitpada Ffile Citra Digital', 8(2), Pp. 140–145.

