IMPLEMENTASI ALGORITMA XOR PADA CITRA SEBAGAI PENGAMANAN PENGAJUAN HAK MEREK

LAPORAN TUGAS AKHIR

Laporan ini Disusun Guna Memenuhi Salah Satu Syarat Memenuhi Gelar Sarjana Strata (S1) pada Program Studi Teknik Informatika Fakultas Teknologi Industri Universitas Islam Sultan Agung Semarang

DISUSUN OLEH

MOHAMMAD FARID GUNAWAN

NIM 32601800017

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM SULTAN AGUNG

SEMARANG

2022

FINAL PROJECT

XOR ALGORITHM IMPLEMENTATION ON IMAGE AS A SECURITY FOR MARK RIGHTS FILING

Proposed to complete the requirement to obtain a bachelor's degree (S1) at Informatics Engineering Departement of Industrial Technology Faculty Sultan Agung Islamic University

Arranged By :

MOHAMMAD FARID GUNAWAN

NIM 32601800017

MAJORING OF INFORMATICS ENGINEERING

INDUSTRIAL TECHNOLOGY FACULTY

SULTAN AGUNG ISLAMIC UNIVERSITY

SEMARANG

2022

LEMBAR PENGESAHAN PEMBIMBING

Laporan Tugas Akhir dengan judul "IMPLEMENTASI ALGORITMA XOR PADA CITRA SEBAGAI PENGAMAN PENGAJUAN HAK MEREK " ini disusun oleh :

Nama : Mohammad Farid Gunawan

NIM : 32601800017

Program Studi : Teknik Informatika

Telah disetujui oleh Dosen Pembimbing pada :

Hari : Sabtu

Tanggal : 31 Desember 2022

Mengesahkan,

Pembimbing I	Pembimbing II
Bagus Satrio Waluyo Poetro, S.Kom, M.Cs	Badie'ah, ST. M.Kom
NIDN. 1027118801	NIDN. 0619018701

Mengetahui,

Ketua Program Studi Teknik Informatika

Fakultas Teknologi Industri

Universitas Islam Sultan Agung

Ir. Sri Mulyono, M. Eng

NIDN. 0626066601

LEMBAR PENGESAHAN PENGUJI

Laporan tugas akhir dengan judul " IMPLEMENTASI ALGORITMA XOR PADA CITRA SEBAGAI PENGAMANAN PENGAJUAN HAK MEREK " ini telah dipertahankan di depan tim penguji proposal Tugas Akhir pada :

Hari : .....

Tanggal : .....

TIM PENGUJI

Penguji I	Penguji II
Andi Riansyah, ST.M.Kom	Ghufron, ST. M. Kom
NIDN. 0609108802	NIDN. 0602079005

SURAT PERNYATAAN KEASLIAN TUGAS AKHIR

Yang bertanda tangan dibawah ini :

Nama	: Mohammad Farid Gunawan
Nim	: 32601800017
Prodi	: Teknik Infomatika
Judul Tugas Akhir	: IMPLEMENTASI ALGORITMA XOR PADA CITRA SEBAGAI PENGAMANAN PENGAJUAN HAK MEREK

Dengan bahwa ini saya menyatakan bahwajudul 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 dikemudian hari tenyata terbukti bahwa judul Tugas Akhir yang saya buat pernah diangkat, ditulis, ataupun dipublikasikan, maka saya bersedia dikenakan sanksi akademis. Demikian surat pernyataan ini saya buat dengan sadar dan penuh tanggung jawab.

Semarang, 20 Februari 2023

Yang Menyatakan

Mohammad Farid Gunawan

PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH

Saya yang bertanda tangan dibawah ini:

Nama	: Mohammad Farid Gunawan
NIM	: 32601800017
Program Studi	: Teknik Informatika
Fakultas	: Teknologi Industri
Alamat	: Ds. Mantingan RT 02 RW 01 Kec. Jaken Kab. Pati

Dengan ini saya menyatakan Karya IImiah Tugas Akhir dengan Judul: Implementasi Algoritma XOR Pada Citra Sebagai Pengamanan Pengajuan Hak Merek Menyetujui menjadi hak milik Universitas Islam Sultan Agung serta memiliki Hak bebas Royalti Non-Ekslusif untuk disimpan, dialihmediakan, dikelola dan pangkalan data dan dipublikasikan diintermet dan media lain untuk kepentingan akademi selama tetap mencantumkan nama penulis sebagai pemilik hak cipta. Permyataan ini sya buat dengan sungguh-sungguh. Apabila dikemudian hari terbukti ada pelaggaran hak Cipta/Plagiatisme dalam karya ilmiah ini, maka segala bentuk tuntutan hukum yang timbul akan saya tanggung secara pribadi tanpa melibatkan Universitas Islam Sultan Agung.

Semarang, 28 Februari 2023

Yang Menyatakan

Mohammad Farid Gunawan

KATA PENGANTAR

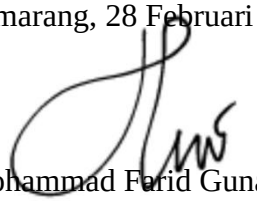
Dengan mengucap syukur alhamdulillah atas kehadirat Allah SWT yang telah memberikan rahmat dan karunianya kepada penulis, sehingga dapat menyelesaikan Tugas Akhir dengan judul "Implementasi Algoritma XOR Pada Citra Sebagai Pengamanan Pengajuan Hak Merek" ini untuk memenuhi salah satu syarat menyelesaikan 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 disusun dan dibuat dengan adanya bantuan dari berbagai pihak, materi maupun teknis, oleh karena itu saya selaku penulis mengucapkan terima kasih kepada:

1. Rektor UNISSULA Bapak Prof. Dr. H. Gunarto, SH., M.Hum yang mengijinkan penulis menimba ilmu di kampus ini.
2. Dekan Fakultas Teknologi Industri Ibu Dr. Novi Marlyana, ST., MT.
3. Dosen pembimbing I penulis Bagus Satrio Waluyo Poetro, S.Kom, M.Cs yang telah meluangkan waktu dan memberi ilmu.
4. Dosen pembimbing II penulis Badie'ah, ST. M.Kom yang telah memberikan banyak nasehat dan saran.
5. Orang tua penulis yang telah mengijinkan untuk menyelesaikan laporan ini.
6. Dan kepada semua pihak yang tidak dapat saya satu persatu.

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

Semarang, 28 Februari 2023



Mohammad Farid Gunawan

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Pendaftaran merek pada Hak Kekayaan Intelektual atau HKI merupakan hal penting yang harus dilakukan dalam bisnis khususnya pelaku usaha dan bisnis rintisan berbasis digital atau *startup*. Hal ini karena pendaftaran tersebut memberikan jaminan hukum bagi pemilik bisnis sehingga merek mereka tidak dapat digunakan oleh organisasi lain. Selain itu, tujuan dari pendaftaran merek adalah untuk memastikan bahwa pemilik merek menerima perlindungan hukum dari negara. Di HKI memliki banyak sekali data pengajuan merek yang sangat penting dan harus dijaga dari pihak yang tidak bertanggung jawab yang dapat di salah gunakan. Maka dari itu, diperlukannya teknik yang dapat mengamankan data dari pihak-pihak yang ingin menyalahgunakan data tersebut. Satu diantaranya teknik yang dapat mengamankan dan melindungi sebuah data atau informasi adalah enkripsi. Penelitian ini sendiri bermaksud membangun sebuah sistem keamanan gambar pengajuan logo merek yang menggunakan metode algoritma XOR. Pada pengujian tersebut telah dilakukan beberapa skenario uji dan input test case dengan menggunakan data valid dan data invalid, fungsi sendiri berjalan dengan baik dan sudah seperti yang diharapkan. Hasil dari penelitian ini dapat menerapkan metode algoritma XOR digunakan untuk enkripsi dan dekripsi memberikan hasil yang sesuai dengan yang direncanakan dan hasil yang di berikan cukup memuaskan untuk digunakan enkripsi gambar. Dan hasil dari dekripsi sesuai dengan gambar aslinya.

Kata Kinci : Algoritma XOR, Enkripsi, Hak Merek

ABSTRACT

Registering a trademark on Intellectual Property Rights or IPR is an important thing that must be done in business, especially digital-based business actors and startups. This is because the registration provides a legal guarantee for business owners so that their mark cannot be used by other organizations. In addition, the purpose of trademark registration is to ensure that the trademark owner receives legal protection from the state. HKI has a lot of data on trademark submissions which are very important and must be guarded against irresponsible parties which can be misused. Therefore, techniques are needed that can secure data from parties who want to misuse the data. One of the techniques that can secure and protect data or information is encryption. This research itself intends to build a security system for submitting brand logo images using the XOR algorithm method. In this test several test scenarios and input test cases have been carried out using valid data and invalid data, the function itself runs well and is as expected. The results of this study can apply the XOR algorithm method used for encryption and decryption to provide results that are in accordance with what was planned and the results given are satisfactory enough to use image encryption. And the results of the decryption match the original image.

Key Words : *XOR Algorithm, Encryption, Brand Rights*

BAB I
PENDAHULUAN

1.1 Latar Belakang

Pendaftaran merek pada Hak Kekayaan Intelektual atau HKI merupakan hal penting yang harus dilakukan dalam bisnis khususnya pelaku usaha dan bisnis rintisan berbasis digital atau *startup*. Hal ini karena pendaftaran tersebut memberikan jaminan hukum bagi pemilik bisnis sehingga merek mereka tidak dapat digunakan oleh organisasi lain. Selain itu, tujuan dari pendaftaran merek adalah untuk memastikan bahwa pemilik merek menerima perlindungan hukum dari negara. Namun, jika suatu saat terjadi peniruan atau penggunaan merek tanpa persetujuan pemiliknya, maka tanda terima pendaftaran merek dapat dijadikan bukti dalam sengketa merek.

Di HKI memliki banyak sekali data pengajuan merek yang sangat penting dan harus dijaga dari pihak yang tidak bertanggung jawab yang dapat di salah gunakan. Maka dari itu, diperlukannya teknik yang dapat mengamankan data dari pihak-pihak yang ingin menyalahgunakan data tersebut. Satu diantaranya teknik yang dapat mengamankan dan melindungi sebuah data atau informasi adalah enkripsi.

Enkripsi merupakan sebuah teknik yang dapat mentransformasikan informasi atau teks ke bentuk kode-kode rahasia yang bertujuan untuk menyamarkan data yang diterima, disimpan, dan dikirim. Proses untuk mengolah data ini memerlukan algoritma yang akan direapkan kembali dengan menggunakan kunci dekripsi oleh penerima *plaintext* (teks polos) digunakan untuk merujuk pada dokumen yang belum dienkripsi, sedangkan *chipertext* (teks yang tersandi). Satu diantaranya sebuah metode yang dapat melakukan sebuah enkripsi data yaitu algoritma XOR.

Algoritma XOR sendiri merupakan satu diantara banyak algoritma kriptografi yang cepat dan akurat ketika melakukan proses enkripsi dan dekripsi. Cara kerja algoritma XOR adalah dengan menggunakan setiap bit dari kunci yang dibuat untuk melakukan operasi XOR pada setiap bit dari *plaintext*. Algoritma XOR sendiri memiliki keunggulan utama yaitu dalam hal kecepatan, karena algoritma ini

melakukan operasi enkripsi dan dekripsi dengan kecepatan yang jauh lebih cepat daripada algoritma kriptografi lainnya. Keamanan dalam algoritma XOR ini bisa dinaikkan menggunakan cara menambahkan jumlah kunci keamanan yang dibuat kemudian kunci tersebut diacak dengan jumlah yang telah ditentukan, sehingga peluang penyerang untuk dapat mengetahui kunci yang telah dibuat hampir tidak bisa. Algoritma XOR sendiri merupakan algoritma simetris yang dapat digunakan dalam mode operasi *block cipher*, di mana panjang *plaintext* akan dikantongi dan dikirim dengan panjang yang berbeda dalam bentuk pesan blok-blok. Jika enkripsi ingin lebih aman maka blok yang digunakan harus semakin panjang(Sidik dkk., 2019).

Pada Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) UNISSULA bidang Hak Kekayaan Intelektual (HKI) memiliki banyak sekali dokumen sangat penting, dimana keamanan dokumen tersebut memerlukan proteksi dalam menjaga kemanan oleh pihak yang tidak bertanggung jawab yang dapat disalah gunakan untuk kepentingan tertentu. Pasalnya saat ini LPPM belum menggunakan keamanan dokumen enkripsi ataupun dekripsi dalam pengamanan dokumen. Oleh karena itu dibutuhkan sistem untuk mengamankan dokumen LPPM menggunakan kemanan enkripsi dan dekripsi.

Berdasarkan paparan di atas penulis mengusulkan sebuah judul "Implementasi Algoritma XOR Pada Citra Sebagai Pengamanan Pengajuan Hak Merek" menggunakan data yang diperoleh dari Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) UNISSULA khususnya di bidang Hak Kekayaan Intelektual (HKI). Penelitian ini sendiri bermaksud membangun sebuah sistem keamanan gambar pengajuan logo merek yang menggunakan metode algoritma XOR.

1.2 Perumusan Masalah

Bagaimana cara mengamankan gambar logo pengajuan merek LPPM UNISSULA menggunakan metode algoritma XOR.

1.3 Pembatasan Masalah

Batasan masalah di dalam penelitian ini sendiri adalah sebagai berikut :

1. Dalam penelitian ini data yang digunakan merupakan data pengajuan gambar logo merek dari LPPM UNISSULA bidang HKI.
2. Aplikasi masih bersifat prototype dengan beberapa data sebagai bahan pengujian.

1.4 Tujuan

Tujuan dari tugas akhir ini sendiri yaitu membuat sebuah prototype sistem keamanan gambar pengajuan logo merek menggunakan algoritma XOR di LPPM UNISSULA bidang HKI .

1.5 Manfaat

Manfaat penelitian ini, sistem ini diharapkan dapat mengamankan semua data gambar pengajuan logo merek di LPPM UNISSULA

1.6 Sistematika Penulisan

Sistematika penulisan yang akan digunakan oleh penulis dalam sebuah pembuatan laporan tugas akhir adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab pertama, penulis membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan, metodologi, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA DAN DASAR TEORI

Pada bab kedua, berisi rangkuman artiker dari penelitian sebelumnya dan dasar teori yang berguna untuk membantu penulis memahami cara kerja aplikasi berbasis web untuk sistem keamanan gambar dengan menggunakan bahasa pemograman dan metode yang ada.

BAB III METODE PENELITIAN

Pada bab ketiga, menjelaskan bagaimana proses melakukan penelitian mendalam yang terdiri dari analisis sistem, alur sistem, desain web, dan pengkodean web.

BAB IV HASIL PENELITIAN

Pada bab keempat, penulis menjelaskan hasil dari penelitian yang telah dilakukan yaitu hasil dari pengujian dan analisa sistem.

BAB V KESIMPULAN DAN SARAN

Pada bab kelima, penulis menjelaskan kesimpulan dari proses penelitian yang telah dilakukan secara keseluruhan dan saran untuk pengembangan sistem pada penelitian selanjutnya.

BAB II
TINJAUAN PUSTAKA DAN DASAR TEORI

2.1 Tinjauan Pustaka

Adapun beberapa penelitian terdahulu yang menjadi dasar bahan acuan yang berhubungan dengan judul penelitian ini. Dalam melaksanakan penelitian tinjauan pustakan yang dimaksudbakan dapat digunakan sebagai acuan.

Penelitian tentang pembuatan sistem informasi pengaman dokumen menggunakan metode algoritma XOR dan Algoritma AES berbasis Web menyatakan bahwa dengan adanya algoritma kriptografi, keamanan filr data atau dokumen menjadi lebih aman dari modifikasi dan pencurian karena penggunaan proses algoritma XOR dan AES, naik sebelum sampai tujuan atau sebelemu dikirimkan. Sedangkan proses dekripsi sendiri akan mengubah file yang telah ditulis dengan kunci menjadi file baru yang identik dengan aslinya tanpa ada perubahan yang mencolok.oleh karena itu, hal ini akan memudahkan pengguna untuk menggunakan sistem saat mengamankan file dan mengembalikan file seperti semula(Junianto dkk., 2020).

Penelitian tentang pembuatan aplikasi pengaman data menggunakan algoritma XOR menyatakan bahwa berdasarkan temuan dari penelitian ini menyatakan bahwa, dimungkinkan untuk menggunakan aplikasi data yang menerapkan algoritma XOR untuk memudahkan user dalam pengolahan data guru untuk mengenkripsi data sehingga hanya orang tertentu yang dapat membaca data yang telah dienkripsi.selain itu, aplikasi ini juga dapat mendekripsi data itu kembali sehingga pengguna dapat mengaksesnya(Andryanto & Dasril, 2017).

Penelitian tentang membuat sebuah aplikasi pengirim dokumen yang menggunakan algoritma XOR dan algoritma RSA menyatakan bahwa hasil dari proyek pengujian yang dilakukan meliputi catatan tiga kali pengujian sistem yang saat ini dilakukan. Terdapat keterbatasan pada optimasi waktu proses yang dibutuhkan untuk membuat kunci pada pengujian 1 selama optimasi waktu proses. Hal ini disebabkan oleh fakta bahwa ketika ukuran bit meningkat, ukuran bilangan prima yang harus dibangkitkan juga meningkat. Terdapat kolerasi antara

pembahasan pengujian ke 2 tentang bagaimana ukuran file memengaruhi seberapa cepat enkripsi atau dekripsi diselesaikan, dengan ukuran file yang lebih besar maka membutuhkan waktu pemrosesan yang lebih lama daripada file yang lebih kecil, yang membutuhkan waktu ekripsi dan dekripsi yang lebih cepat. Format file apapun dengan sendirinya tidak mengganggu kecepatan enkripsi atau dekripsi. Jika kekuatan bit strenght lebih besar maka kecepatan dalam proses enkripsi akan lebih cepat dalam pengujian ke 3. Hal ini disebabkan oleh fakta bahwa kekuatan bit itu sendiri pengaruh besar dalam melakukan proses enkripsi. Ketika semakin meningkat nilai bit maka jumlah perulangan yang dilakukan selama proses enkripsi semakin sedikit(Refialy, 2022).

Penelitian yang berjudul Peningkatan Keamanan Teks Menggunakan Kriptografi Dan Steganografi menyatakan bahwa penelitian saat ini menggabungkan teknik steganografi dan kriptografi dengan algoritma RSA dan XOR untuk menyediakan steganografi yang aman yang dapat dievaluasi kualitasnya. MSE dan PSNR mengevaluasi kualitas data steganografi dari hasilpenelitian. MSE melampaui rata-rata 0,8768, sedangkan PSNR melampaui 50,1588. Tidak ada perbedaan antara gambar asli dan gambar steganografi yang dibuat oleh visualisasi manusia. Hasil analisis menunjukkan bahwa metode yang direkomendasikan dapat menghasilkan steganografi yang aman(Agustini & Kurniawan, 2019).

Penelitian tentang pembuatan aplikasi pengaman teks berbasis mobile menggunakan algoritma XOR dan algoritma AES menyatakan bahwa implementasi algoritma kriptografi, yang menggabungkan antara algoritma AES dan XOR untuk penyandian teks yang berhasil diselesaikan pada platform android. Aplikasi yang dikembangkan bekerja sesuai dengan algoritma yang digunakan. Dengan membiarkan keaslian pesan yang dikirim, plainteks yang telah diacak bisa dikembalikan menjadi seperti semula. Selain itu, waktu yang dibutuhkan untuk menyelesaikan proses enkripsidengan menggunakan algoritma XOR dan AES secara bersamaan menghasilkan waktu lebih sedikit dibandingkan dengan waktu yang dibutuhkan untuk menyelesaikan proses tersebut dengan hanya menggunakan

satu algoritma saja. Proses enkripsi yang telah dilakukan memilikiselisish waktu 3,12 detik(Amalia & Rosyani, 2018).

Perbandingan lama waktu enkripsi algoritma XOR dan algoritma AES lebih efisien algoritma XOR dengan selisih 0,01 detik. Selain itu, panjang plainteks berbanding lurus dengan lama waktu proses enkripsi. Ketika plainteks lebih kompleks, semakin banyak waktu yang dibutuhkan untuk menyelesaikan proses enkripsi, seperti yang terlihat pada Tabel 2.1.

Tabel 2.1 Tabel perbandingan Algorima XOR dan Algoritma AES(Amalia & Rosyani, 2018).

No.	Panjang Plaintext	Algoritma XOR	Algoritma AES
1.	100	1,3 detik	1,3 detik
2.	120	1,3 detik	1,3 detik
3.	130	1,3 detik	1,4 detik
4.	140	1,4 detik	1,4 detik
Total		**4,13** detik	**4,14** detik

Algoritma XOR sendiri memiliki keunggulan utama dalam hal kecepatan, karena algoritma ini melakukan enkripsi dan dekripsi dengan kecepatan yang jauh lebih cepat daripada algoritma kriptografi lainnya. Dengan membuat kunci dan membuat pengacakan kunci seacak mungkin, kekuatan algoritma XOR dapat ditingkatkan, sehingga probabilitas penyerangan menebak kunci yang digunakan semakin susah.

Algoritma kriptografi yang paling sederhana namun efektif dalam melakukan enkripsi atau dekripsi adalah algoritma XOR. Algoritma XOR dalam melakukan operasi yaitu dengan cara meng-XOR-kan bit dan kunci. Keunggulan utama dari algoritma XOR adalah kecepatan dalam melakukan enkripsi dan dekripsi dibandingkan dengan algoritma lainnya. Proses enkripsi dan dekripsi sangat mudah dan cepat, tetapi juga cukup akurat. (Sidik dkk., 2019).

2.2 Dasar Teori

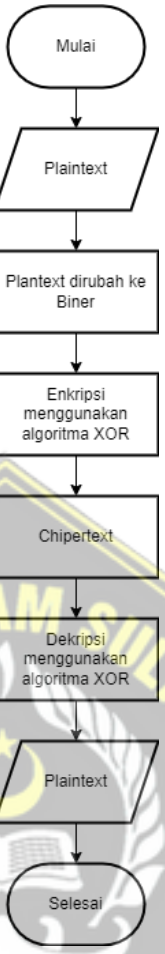
2.2.1 Kriptografi

Kriptografi adalah cabang pengetahuan yang menggabungkan pengetahuan seni dan ilmu untuk menganalisis informasiatau data tertentu dengan aman(Poetro & Wardoyo, 2017). Banyak implementasi kriptografi yang dibuat, khususnya di bidang teknologi untuk kemanan dan perlindungan. Hampir setiap kali seseorang mengakses internet, merek menggunakan kriptografi tanpa sepengetahuan telah digunakan. Sebagai contoh, untuk berkomunikasi atau menerima informasi, informasi akan dienkripsi sebelum dibagikan dan didekripsi lagi sebelum diketahiu oleh penerima. Sebagai contoh, untuk masuk ke email, anda hanya memerlukan fungsi hash untuk menentukan apakah kata sandi anda kuat atau lemah. Mekanisme hashing yang digunakan dalam kriptografi untuk menjaga kerahasiaan menggunakan fungsi hash dan menghasilkan nilai hash.

Kinerja algoritma kriptografi tergantung pada jenis teks atau kalimat, seperti *plaintext*, sandienkripsi dan dekripsi, dan panjang kunci. Jika algoritma menggunakan panjang kunci lebih dari itu, makaakan lebih aman ada dua cara dalam kriptografi. Metode utama adalah menggunakan kunci yang identik untuk proses enkripsi dan dekripsi, yang diknal sebagia kriptografi kunci simetris. Lainnya menggunakan asimetris kunci kriptografi untuk dekripsi dan kunci yang berbeda satu untuk enkripsi(Santoso dkk., 2019).

2.2.2 Algoritma XOR

Algoritma kriptografi yang paling umum saat ini yaitu yang dikenal dengan algoritma XOR, dengan menerapkan algoritma XOR pada plainteks dengan kunci untuk menghasilkan chiperteks. Prosedur untuk menjadikan plainteks kembali adalah dengan menerapkan algoritma XOR dengan chiperteks dan kunci untuk menghasilkan plainteks. Algoritma ini mudah untuk dioperasikan tidak perlalu membebani komputer(Amalia & Rosyani, 2018). Berikut adalah flowchart dari algoritma XOR.



Gambar 2. 1 *Flowchart* algoritma XOR

Pada gambar 2.1 merupakan *flowchart* dari algoritma XOR. Yang pertama yaitu terdapat sebuah plaintext. kemudian dirubah menjadi biner. Biner akan dienkripsi menggunakan algoritma XOR kemudian akan menjadi ciphertext. Selanjutnya akan didekripsi menggunakan algoritma XOR akan menjadi plaintext.

Berikut tabel operasi algoritma XOR dan contoh proses enkripsi dan dekripsi menggunakan algoritma XOR :

Tabel 2. 2 Tabel operasi algoritma XOR

C	D	C⊕ D
0	0	0
1	0	1

0	1	1
1	1	0

Algoritma enkripsi menggunakan XOR adalah dengan meng-XOR-kan *plaintext* (P) dengan kunci (K) menghasilkan *ciphertext* (C):

Keterangan :

⊕: XOR

P : *Plaintext*

C : *Ciphertext*

K : Kunci

$$C = P \oplus K \qquad (1)$$

Algoritma dekripsi menggunakan XOR adalah dengan meng-XOR-kan *ciphertext* (C) dengan kunci (K) menghasilkan *plaintext* (P):

$$P = C \oplus K \qquad (2)$$

Contoh enkripsi dan dekripsi teks (*plaintext*) “OKE” dengan kunci “@”, tahapan penghitungan manualnya adalah sebagai berikut :

1. Buka tabel ASCII, kemudian cari nilai “OKE” dan “@”, sehingga kita temukan nilai O = 79, K=75, O=69, dan <=3C
2. Ubah angka 79, 75, 69, dan 48 kedalam bilangan biner, sehingga kita dapatkan nilai 79=01001111, 75=01001011, 69=01000101, 3C=00111100
3. Lakukan proses enkripsi dengan metode XOR (C = P Å K) seperti berikut :

plainteks 01001111 (karakter ‘O’)

kunci 00111100 ⊕ (karakter ‘<’)

cipherteks 01110011 (karakter ‘s’)

plainteks 01001011 (karakter ‘K’)

kunci 00111100 ⊕ (karakter ‘<’)

cipherteks 01110111 (karakter ‘w’)

plainteks 01000101 (karakter ‘E’)

kunci 00111100 ⊕ (karakter ‘@’)

cipherteks 01111001 (karakter ‘y’)

4. Cipherteks dari teks “OKE” dengan kunci “<” adalah “swy”. Karakter “swy” didapatkan dari nilai :
   01110011(biner)= 73(decimal)=karakter “s” (tabel ASCII)
   01110111(biner)=117(decimal)=karakter “w” (tabel ASCII)
   01111001(biner)=121(decimal)=karakter “y” (tabel ASCII)
5. Untuk melakukan proses dekripsi dengan metode XOR (P = C Å K) seperti berikut :
   cipherteks 01110011 (karakter ‘s’)
   kunci 00111100 ⊕ (karakter ‘<’)
   plainteks 01001111 (karakter ‘O’)

   cipherteks 01110111 (karakter ‘w’)
   kunci 00111100 ⊕ (karakter ‘<’)
   plainteks 01001011 (karakter ‘K’)

   cipherteks 01111001 (karakter ‘y’)
   kunci 00111100 ⊕ (karakter ‘@’)
   plainteks 01000101 (karakter ‘E’)
6. Plainteks dari pesan “yaw” dengan kunci “8” adalah “AYO”. Karakter

"AYO" didapatkan dari nilai seperti yang telah dijelaskan pada poin 1 dan 2 diatas.

01001111 (biner)= 4F(decimal)=karakter "O" (tabel ASCII)

01001011 (biner)=4B(decimal)=karakter "K" (tabel ASCII)

01000101 (biner)=45(decimal)=karakter "E" (tabel ASCII)

2.2.3 Lembaga penelitian dan pengabdian masyarakat (LPPM) UNISSULA

Lembaga penelitian dan pengabdian masyarakat (LPPM) merupakan lembaga yang dibawah naungan Universitas Islam Sultan Agung Semarang yang diberikan tanggung jawab untuk penyelenggaraan dan pelaksanaan penelitian dan pengabdian kepada masyarakat. Di dalam LPPM sendiri terdapat beberapa bidang salah satunya yaitu bidang Hak Kekayaan Intelektual (HKI). HKI sendiri terdiri dari dua yaitu hak cipta dan hak kekayaan industri. Menurut ketentuan yang berlaku dalam peraturan perundang-undangan yang relevan, hak cipta adalah hak eksklusif dari pemegang hak untuk memulai, mempertahankan, atau meningkatkan ciptaannya, atau memberi izin untuk itu. Sedangkan kekayaan industri terdiri dari 6 hak yaitu :

- Paten
- Desain industri
- Varietas tanaman
- Merek
- Desain tata letak sirkuit terpadu
- Rahasia dagang

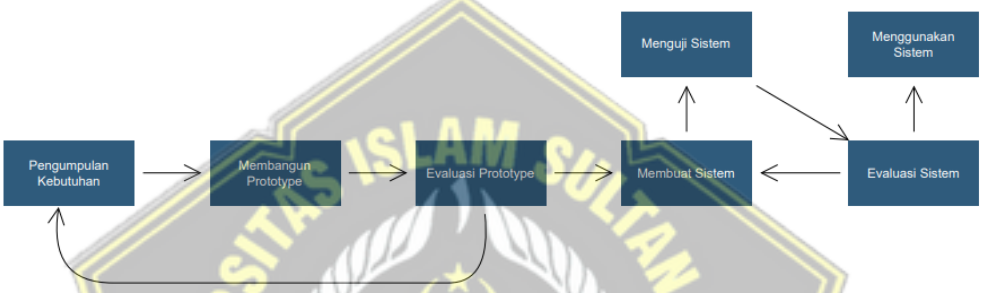
Di indonesia sendiri masih kurangnya apresiasi terhadap hak kekayaan intelektual itu sendiri khususnya di hak merek, maka dari itu adanya penelitian ini diharapkan mampu mengamankan gambar logo pengajuan merek yang ada pada LPPM itu sendiri.

2.2.4 Metode *Prototype*

Metode *prototype* proses berulang untuk mengembangkan perangkat lunak di mana kebutuhan diterjemahkan ke dalam sistem kerja yang terus meningkat melalui kolaborasi antara pengguna dan analis. Dengan *prototype* yang berfungsi, model

sistem atau bagiannya dikembangkan dengan cepat dan mendapatkan daya tarik dalam diskusi berulang dengan pengguna.

Dengan memanfaatkan metodologi *prototype*, pengembangan sistem dapat mencakup sejumah evaluasi dan penyesuaian desain yang berpusat pada pengguna, serta menyediakan alat yang diperlukan bagi pengembang sistem untuk membuat sistem yang memenuhi kebutuhan mereka. Menggunakan masukkan dari pengguna selama proses mengembangan sehingga komunikasi dengan pegguna selalu berlangsung. Bebrikut alur dari metode *prototype* yang dijelaskan pada gambar 2.2.



Gambar 2.2 Alur proses metode Prototype(Makiolor dkk., 2017)

Dalam porses pengembangan sistem ini terdapat beberapa tahapahan yang perlu dilakukan, antara lain sebagai berikut:

1. Pengumpulan Kebutuhan

Dalam tahap ini, pengembangan aplikasi dan komunikasi pengguna mendefinisikan secara detail sistem yang akan dikembangkan, spesifikasi yang diperlukan, dan mengidentifikasi msalah yang mungkin timbul.

2. Membangun *Prototype*

Setelah berkomunikasi dengan pengguna, kreator memulai langkah berikutnya, yang memerlukan pembuatan *prototype* dan dengan cepat merancang sistem yang sesuai dengan analisis pengguna.

3. Evaluasi *Prototype*

Pada langkah ini, pengguna memutuskan apakah *prototype* yang dibuat sudah memenuhi kebutuhan dan keinginan mereka atau belum. Jika belum, *prototype* akan direvisi dengan menghapus bahsa sebelumnya jika perlu. Namun, jika langkah selanjutnya akan dilakukan jika semuanya sudah beres.

4. Membuat Sistem

Dalam hal ini pengembang sistem membuat sistem dengan menggunakan bahasa yang sesuai untuk *prototype* yang telah diterima oleh pengguna.

5. Menguji Sistem

Setelah sistem dibangun, langkah selanjutnya adalah mementukan apakah sistem tersebut befungsi dengan harapan pencipta dan pengguna ata tidak.

6. Evaluasi Sistem

Pada titik ini, sistem sedang dievaluasi. Jika diperlukan koreksi atau masukan lebih lanjut dari pengguna, tugas itu akan dilakukanoleh pengembang. Namun, jika sistem ditemukan sesuai persyaratan, tugas itu akan selesai. Pada langkah berikutnya, pengguna akan menentukan maksud mereka sebelum menggunakan sistem yang sering mereka gunakan.

7. Menggunakan Sistem

Pada tahap ini merupakan tahapan akhir proses pengembangan sistem dengan menggunakan metode *prototype*. Sistem telah memungkinkan pengujian, sesuai dengan harapan pengguna, dan siap digunakan(Makiolor dkk., 2017).

2.2.5 PHP

Gambar 2.3 Logo PHP

Hypertext Preprpcess adalah bahasa pemograman utama yang berjalan pada server web dan berfungsi sebagai server data adalah pemograman. Data pengguna akan disimpan di server web database, di mana data tersebut dapat ditampilkan jika akses diberikan. Untuk menjalankan kode PHP file terlebih dahulu diunggah ke dalam server tersebut. Setelah itu user melakukan proses transfer file dari komputer ke dalam server web yang mana hal tersebut dikenal dengan istilah uploading.

Sebuah perangat lunak yang dapat mentransfer data dari komputer user ke web server sehingga dapat dengan mudah dan aman ditampilkan di browser diperlukan umtukmembuat situs web yang mudah dijalankan setiap saat di browser. PHP merupakan satu diantara aplikasi mampu diluncurkan dalam server dan sangat user-friendly.

PHP berjalan di dalam dokumen yang ditulis dalam HTML *(Hypertext Markup Language)* digunakan untuk mengirimkan permintaan dari sebuah halaman web. Dengan PHP, anda dapat mengubah situs web menjadi aplikasi web yang dapat disesuaikan(Mubarak, 2019).

2.2.6 HTML

Hypertext Markup Language (HTML) adalah bahasa standar yang digunakan untuk menampilkan konten web. HTML sendiri tidak didsarkan pada kode atau simbol tertentu yang digunakan dalam file atau dokumen tertentu, sehingga memungkinkan untuk menampilkan di layar komputer dan dapat dimengerti oleh orang lain. HTML sendiri dipandang sebagai metode untuk mentransfer konten dari situs web ke situs web liannya. HTML mampu menampilkan hal-hal berikut :

a. Mengubah teks dari header dan isi situs web.
b. Membuat tabel di dalam halaman web.
c. Publikasi online konten situs web.
d. Membuat formulir yang dapat digunakan untuk memfasilitasi pendaftaran dan transaksi online.

HTML merupakan yang paling umum digunakan untuk membuat sebuah dokumen yang dapat dibaca di web. Selain itu, HTML merupakan bhasa yang dignakan untuk pemograman web yang cepat dan fleksibel(Butsianto, 2020).

2.2.7 XAMPP

Gambar 2.4 Logo XAMPP

XAMPP adalah perangkat lunak dasar yang mendukung sejumlah sistem operasi dan digunakan untuk mengkompilasi sejumlah program. Berfungsi sebagai server mandiri *(localhost)*, menampung server web Apache, basis data MySQL, dan aplikasi pembelajaran bahasa yang ditulis dalam bahasa pemograman PHP dan Perl.

Berdasarkan definisi tersebut, dapat disimpulkan XAMPP sendiri merupakan sejenis perangkat lunak yang dapat digunakan meluncurkan situs web lokal yang didukung oleh PHP dan MySQL. XAMPP dapat disebut sebagai server Cpanel virtual yang memungkinkan pratinjau sehingga situs web dapat dimodifikasi tanpa online atau terhubung ke internet(Siregar & Sari, 2018).

2.2.8 Mysql

Gambar 2.5 Logo MySQL

Pada awalnya, MySQL kadang-kadang disebut sebagai *Structured Query Language* (SQL) adalah bagian dari bahasa tersebut. Bahasa SQL secara khusus dirancang untuk digunakan untuk membuat database. American National Standards Institute (ANSI) mendefinisikan SQL untuk pertama kalinya pada tahun 1986. MySQ adalah sistem manajemen basis data sumber terbuka yang kuat untuk data terpisah.

Sistem untuk mengelola data dasar adalah MySQL atau sistem konvensional. Dengan demikian, data yang diambil dari sebuah basis data kemudian dimasukkan ke dalam beberapa tabel yang diputar untuk mempermudah manipulasi data. MySQL dapat digunakan untuk membuat database dengan berbagai ukuran, dari yang kecil sampai yang besar tergantung kebutuhan (Novendri, 2019).

2.2.9 Black Box Testing

Gambar 2.6 Proses *Black Box Testing*

Black Box Testing merupakan evaluasi sistem yang berkonsentrasi pada kemampuan fungsional sistem. *Black box testing* memeriksa fungsi-fungsi yang tidak jelas atau tidak ada kesalahan antar muka, kesalahan pada struktu dan akses data, kesalahan tentang kinerja, pertanyaan tentang asumsi dan kesimpulan, dan sebagainya. Sebelum melakukan *black box testing*, perlu disusun daftar persyaratan fungsional dan non-fungsional untuk memahami jenis fitur yang akan datang.

Pengujian sistem dilakukan dengan menggunakan *black box testing* untuk dapat menemukan kesalahan di beberapa jenis kategori, diantaranya ialah menemukan kesalahan dalam struktur data atau akses database eksternal, kemudian kesalahan dalam kinerja(Achmad & Yulfitri, 2020).

BAB III
METODE PENELITIAN

3.1 Pengumpulan Data

Berikut ini adalah tahapan dari pengumpulan data untuk menamatkan penelitian ini sebagai berikut :

1. Studi Literatur

Dalam studi literatur ini penulis mempelajari beberapa hal yang berhubungan dengan PHP, Mysql, XAMPP, Algoritma XOR dari berbagai sumber seperti artiker, jurnal, youtube, dan situs website.

2. Observasi

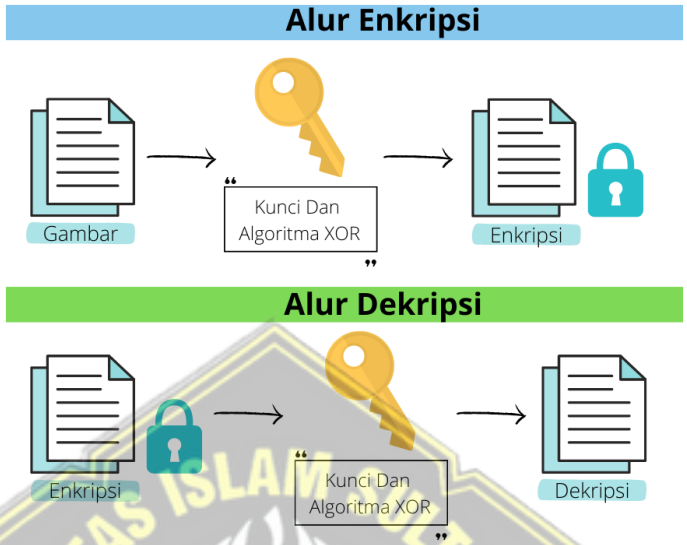
Dalam Observasi ini penulis melakukan observasi untuk mendapatkan data sesuai yang diperlukan dan melakukan pengamatan untuk mengetahui cara mengimplementasikan program. Data yang digunakan merupakan data gambar logo pengajuan hak paten merek LPPM UNISSULA bidang HKI.

3.2 Perancangan Sistem

3.2.1 Desain Sistem

Pada penelitian ini menjelaskan bagaimana membuat sebuah sistem keamanan gambar logo pada pengajuan merek LPPM UNISSULA bidang HKI menggunakan metode algoritma XOR. Tujuan dari penelitian ini adalah menjaga keamanan dan kerahasiaan gambar logo pengajuan merek. Pada tahap awal user mengupload gambar logo kedalam sistem. Lalu sistem akan melakukan proses enkripsi menggunakan algoritma XOR, kemudian gambar asli dan hasil enkripsi akan ditampikan didalam teks area yang ditampilkan didalam sistem dan sistem juga menyediakan dowload untuk file enkripsinya. Kemudian pada proses dekripsinya user harus mengupload file enkripsi kemudian akan di dekripsi menggunakan XOR oleh sistem menjadi dekripsi kemudian dokumen enkripsi dan gambar dekripsi akan ditampilkan didalam sistem dan sistem juga menyediakan download untuk file dekripsinya. Adapun alur enkripsi dan dekripsi ditunjukkan

pada gambar dibawah.



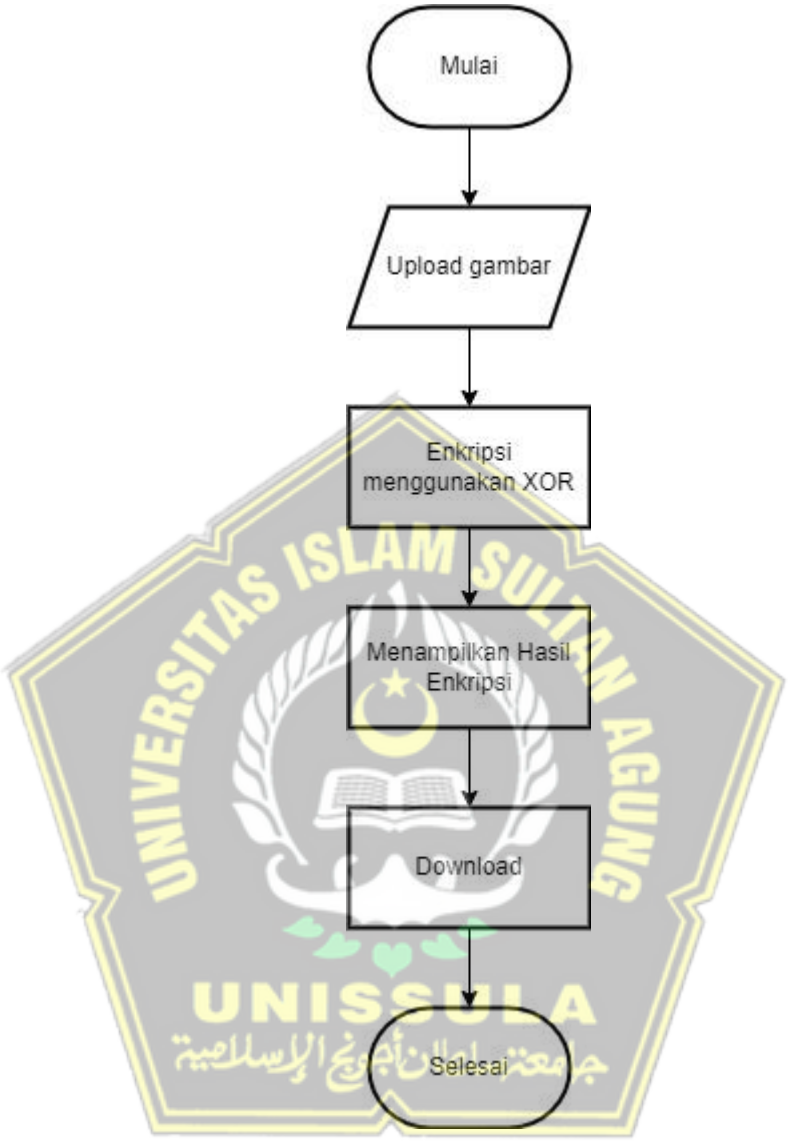
Gambar 3.1 Alur Enkripsi Dan Dekripsi

Pada gambar 3.1 menggambarkan alur proses dari enkripsi dan dekripsi oleh sistem. Tahap enkripsi gambar akan di enkripsi menggunakan kunci dan algoritma XOR kemudian akan menghasilkan dokumen yang telah terenkripsi. Kemudian pada tahap dekripsi dokumen hasil enkripsi akan di dekripsi mengguakan kunci dan algoritma XOR kemudian akan menghasilkan gambar yang telah terdekripsi yang sama seperti gambar asli.

3.2.2 Flowchart Sistem

Pada flowchart sistem terdapat dua bagian flowchart yaitu flowchart enkripsi dan flowchart dekripsi, berikut tampilan dari flowchart sistem enkripsi dan flowchart sistem dekripsi.

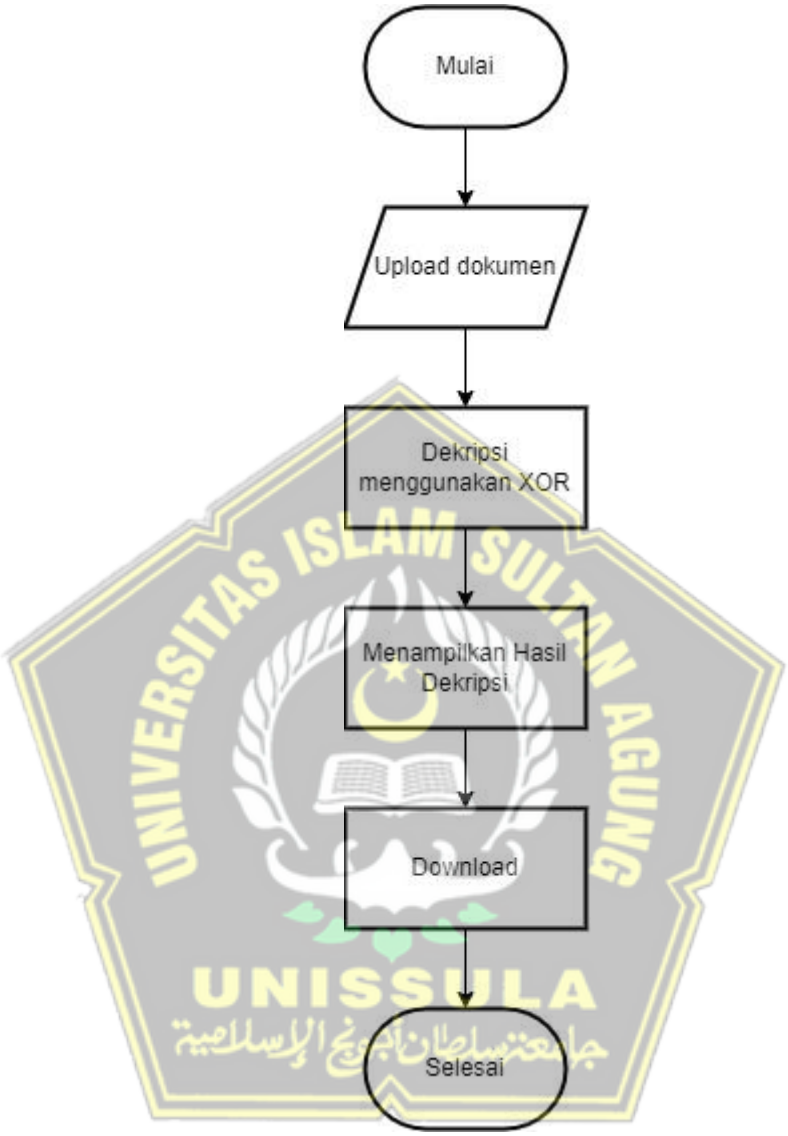
1. Flowchart Sistem Enkripsi



Gambar 3.2 *Flowchart* Sistem Enkripsi

Pada gambar 3.2 merupakan langkah-langkah dan proses sistem enkripsi, pada tahap pertama yaitu user mengupload gambar yang mau dienkripsi kemudian gambar akan ditampilkan didalam sistem dan akan diproses enkripsi menggunakan algoritma XOR oleh sistem lalu hasil dari enkripsi gambar dengan format txt akan ditampilkan oleh sistem, jika user ingin mendownload dokumen user tinggal mengklik tombol download.

2. Flowchart Sistem Dekripsi



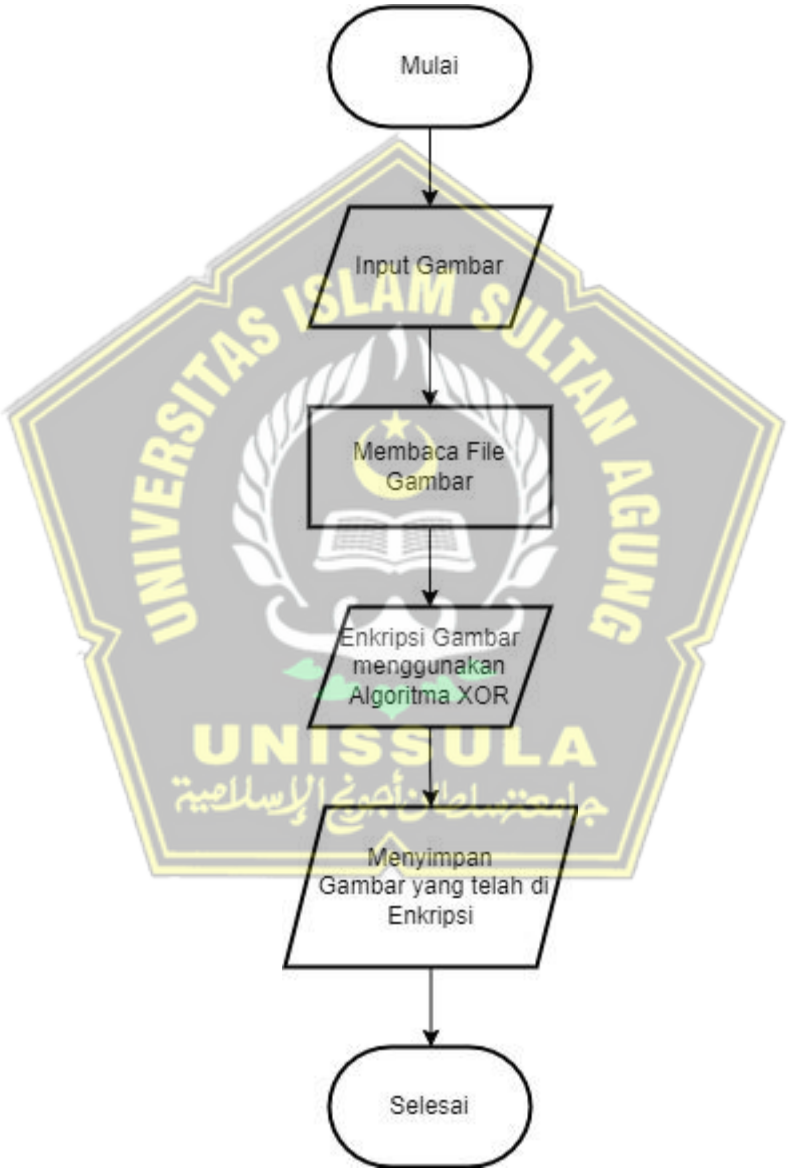
Gambar 3.3 *Flowchart* Sistem Dekripsi

Pada gambar 3.3 merupakan langkah-langkah dan proses sistem dekripsi, pada tahap pertama yaitu mengupload dokumen enkripsi kedalam sistem kemudian sistem menampilkan dokumen didalam sistem dan sistem akan mendekripsi dokumen tersebut menggunakan algoritma XOR lalu setelah didekripsi sistem akan menampilkan gambar hasil dari dekripsi, jika user ingin mendownload gambar user tinggal mengkilk tombol download.

3.2.3 *Flowchart* Enkripsi dan Dekripsi

Pada proses enkripsi terdapat dua bagian Flowchart enkripsi dan flowchart dekripsi, berikut tampilan dari flowchart enkripsi dan dekripsi pada gambar berikut ini :

1. *Flowchart* Enkripsi Gambar



Gambar 3.4 *Flowchart* Enkripsi Gambar

Pada gambar 3.4 dijelaskan langkah-langkah dan proses enkripsi, pada tahap pertama yaitu user melakukan upload gambar kemudian sistem mebaca file gambar,

setelah sistem membaca gambar akan dilakukan proses enkripsi gambar menggunakan algoritma XOR, hasil dari enkripsi gambar akan disimpan dan akan ditampilan didalam sistem.

2. Flowchart Dekripsi Gambar

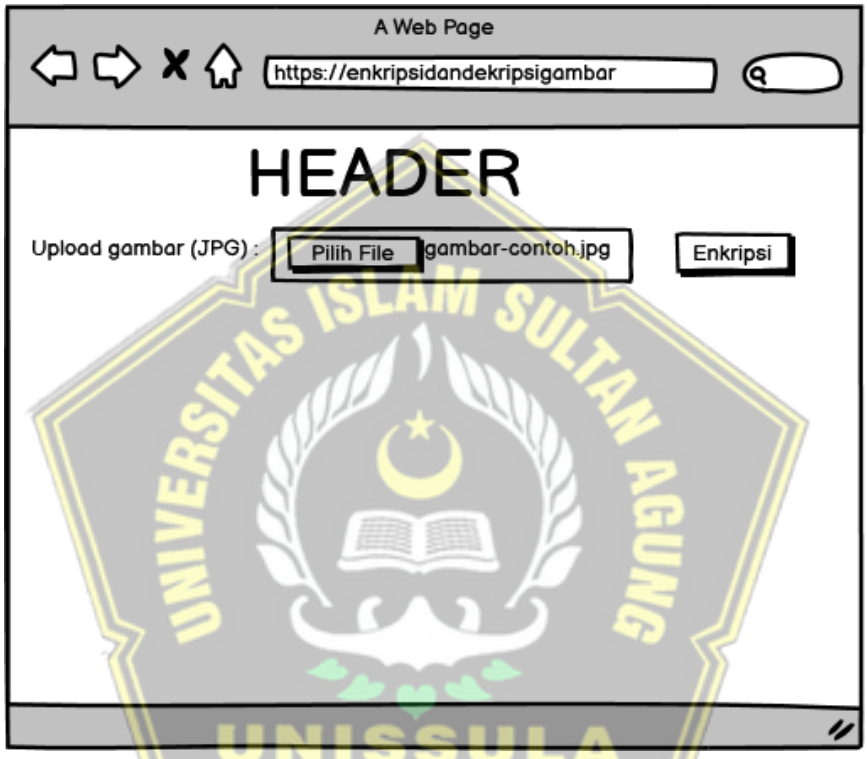
Gambar 3.5 *Flowchart* Dekripsi Gambar

Pada gambar 3.5 dijelaskan langkah-langkah dan proses dekripsi gambar, pada tahap pertama yaitu upload image_encrypted.txt, kemudian membaca file hasil enkripsi setelah itu dilakukan proses dekripsi menggunakan algoritma XOR, kemudian akan disimpan ditampilkan didalam sistem hasil dekripsi.

3.2.4 *User Interface* (UI)

User Interface isi dari rancangan desain aplikasi yang dibutuhkan sebagai panduan sebelum dilakukannya pembuatan aplikasi secara langsung. Berikut adalah rancangan User Interface.

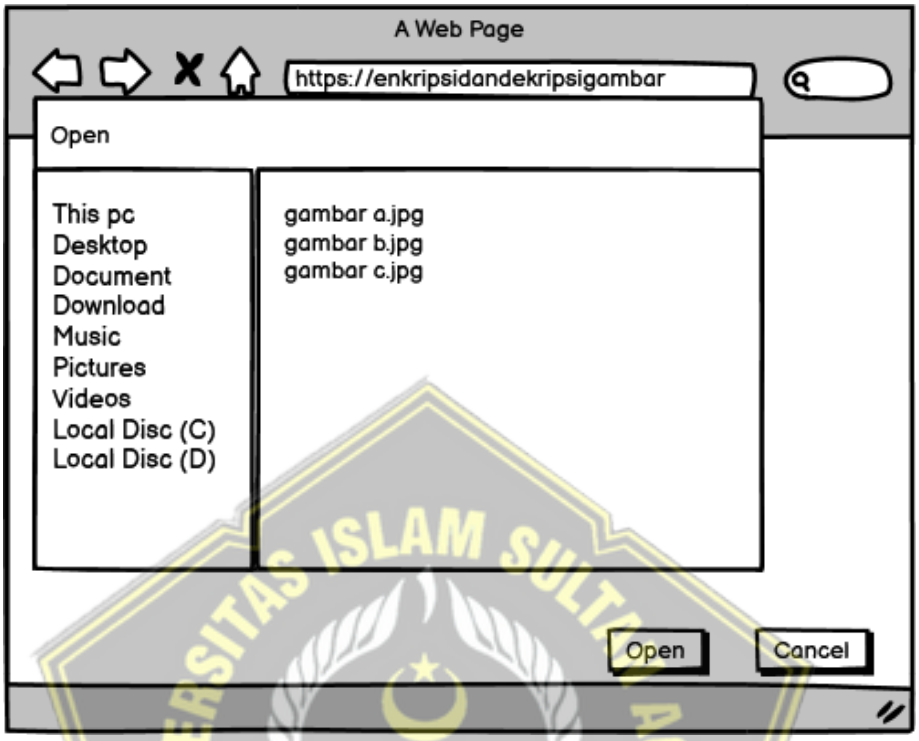
1. Desain tampilan awal enkripsi



Gambar 3.6 Desain Tampilan Awal Enkripsi

Pada gambar 3.6 merupakan desain tampilan dari menu enkripsi. Pada tampilan ini terdapat tombol pilih file dan enkripsi, jika user mengklik tombol pilih file maka akan ditampilkan tab pilih file.

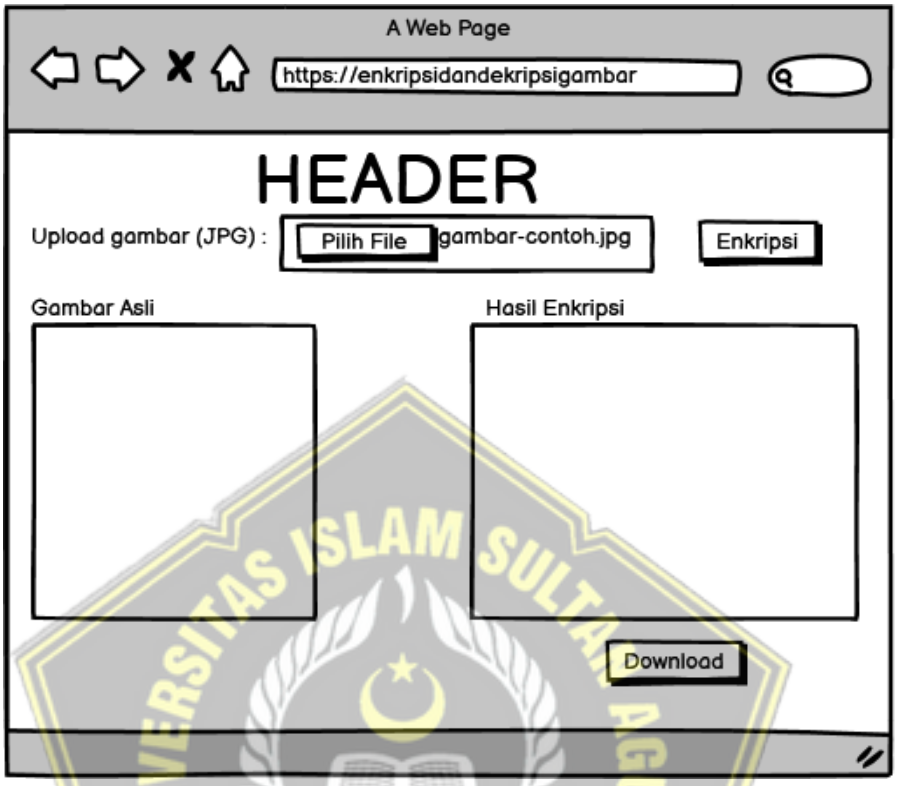
2. Desain tampilan tab pilih file



Gambar 3.7 Desain Tampilan Tab Pilih File

Pada gambar 3.7 merupakan desain dari tampilan tab pilih file. Pada tampilan terdapat daftar file, tombol open dan cancel.

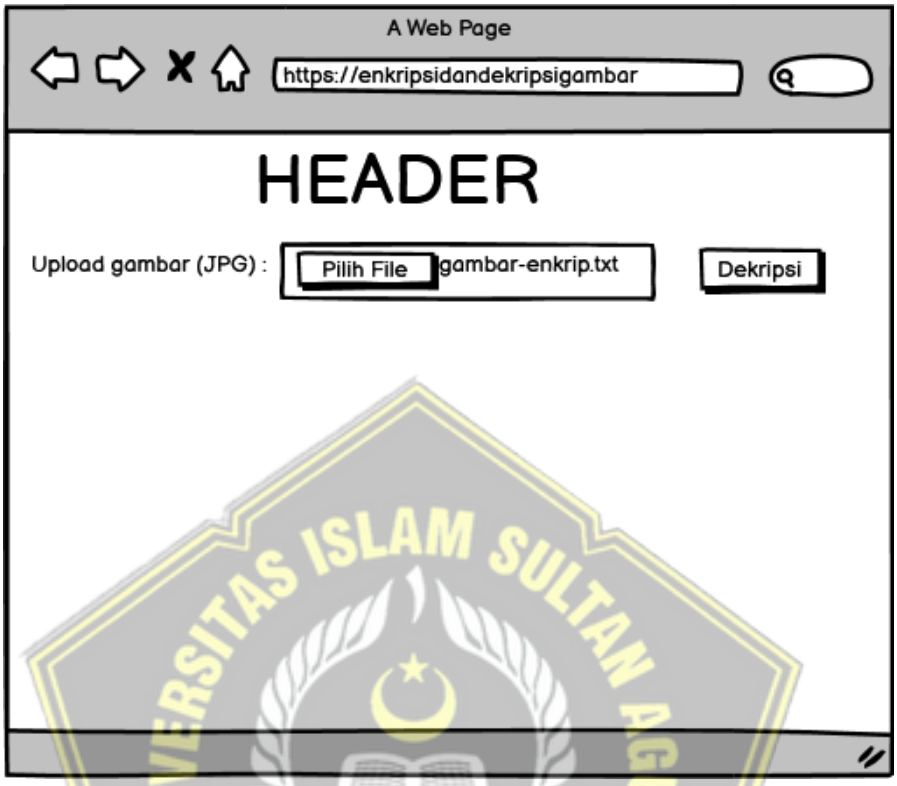
3. Desain tampilan menu enkripsi



Gambar 3.8 Desain Tampilan Menu Enkripsi

Pada gambar 3.8 diatas merupakan tampilan desain dari menu hasil proses enkrisi. Pada tampilan ini terdapat tombol (pilih file, enkripsi dan download) tampilan gambar asli dan tampilan hasil enkripsi.

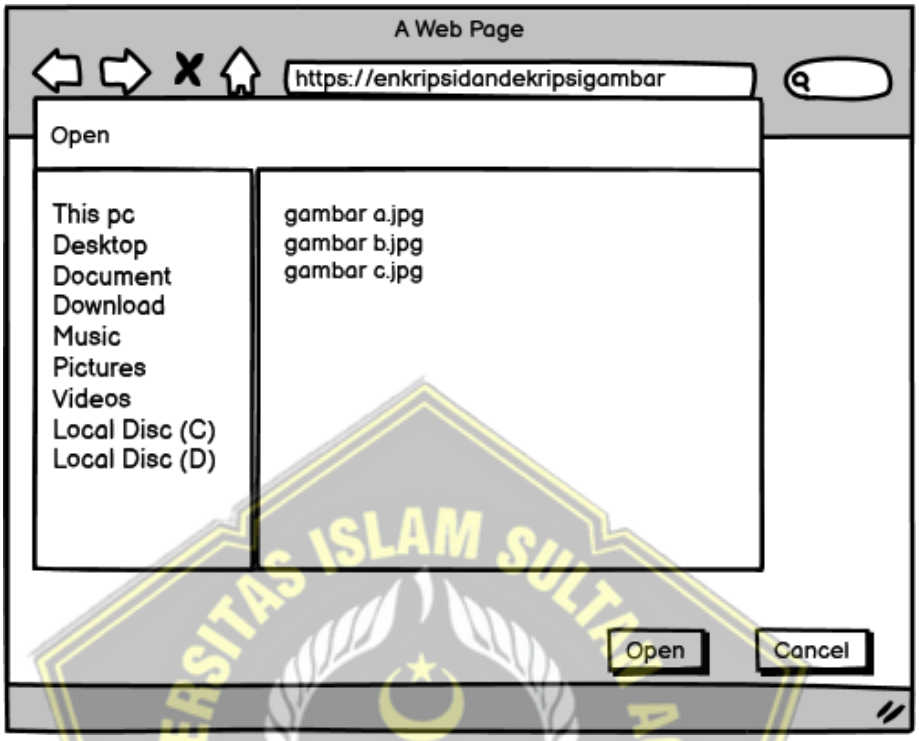
4. Desain tampilan awal dekripsi



Gambar 3.9 Desain Tampilan Awal Dekripsi

Pada gambar 3.9 merupakan desain tampilan dari menu dekripsi. Pada tampilan ini terdapat tombol pilih file dan dekripsi, jika user mengklik tombol pilih file maka akan ditampilkan tab pilih file.

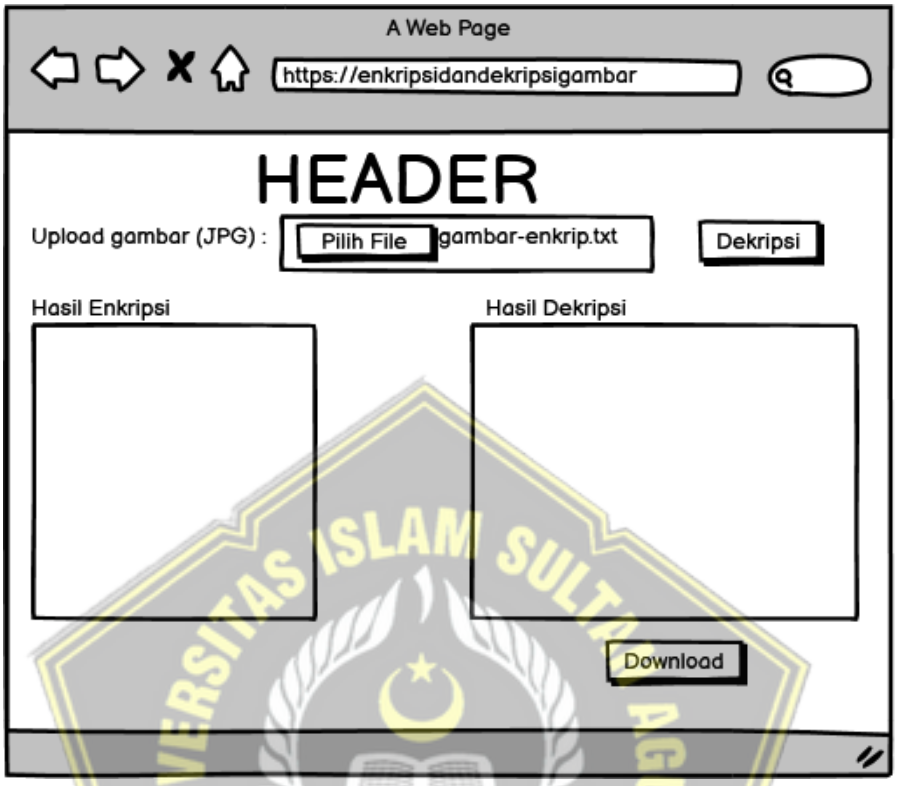
5. Desain tampilan tab pilih file



Gambar 3.10 Desain Tampilan Tab Pilih File

Pada gambar 3.10 merupakan desain dari tampilan tab pilih file. Pada tampilan terdapat daftar file, tombol open dan cancel.

6. Desain tampilan menu dekripsi



Gambar 3. 11 Desain Tampilan Menu Dekripsi

Pada gambar 3.11 diatas merupakan tampilan desain dari menu hasil proses dekripsi. Pada tampilan ini terdapat tombol (pilih file, enkripsi dan download) tampilan gambar asli dan tampilan hasil dekripsi.

BAB IV
HASIL DAN ANALISIS PENELITIAN

4.1 Implementasi *User Interface* (UI)

Implementasi *User Interface* (UI) merupakan tahap penerapan rancangan yang telah dibuat sebelumnya.

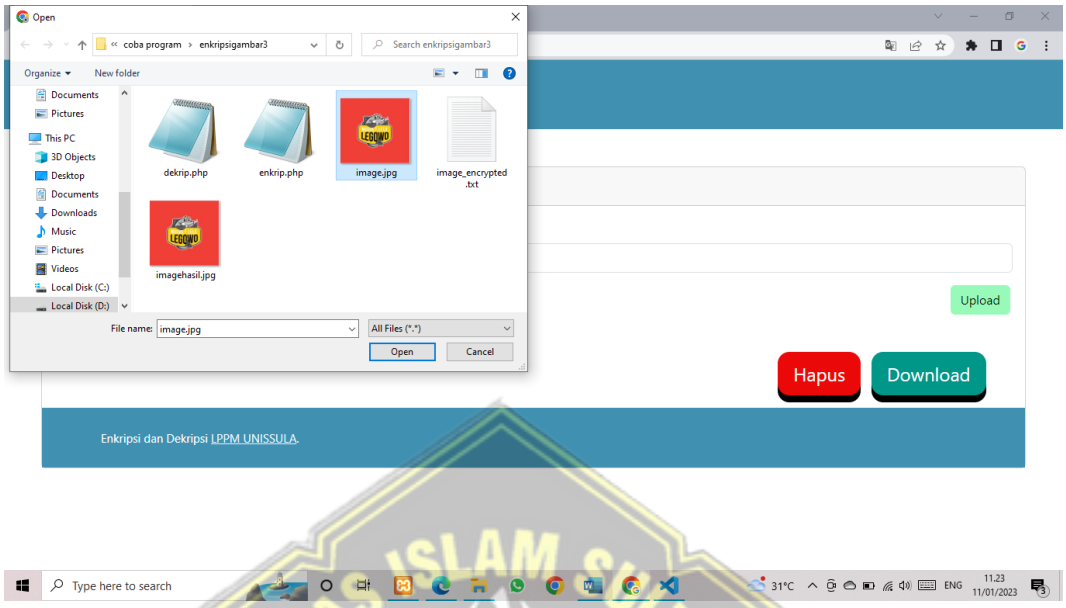
4.1.1 Tampilan *User Interface* (UI) Enkrispi

1. Tampilan Enkripsi

Gambar 4.1 Tampilan Menu Enkripsi

Pada gambar 4.1 merupakan tampilan dari menu enkripsi, dimana dalam tampilan tersebut terdapat menu upload gambar yang akan dienkripsi, tampilan gambar asli, tampilan hasil enkripsi. kemudian ada beberapa tombol seperti pilih file, enkripsi dan download. Langkah pertama dalam proses enkripsi yaitu dengan cara memilih file gambar yang akan di Enkripsi lalu klik tombol enkripsi kemudian sistem akan memproses enkripsi menggunakan algoritma XOR dan kemudian sistem akan menampilkan gambar asli dan hasil enkripsi. Jika ingin mendownload hasil dokumen yang terenkripsi maka tinggal mengkilk tombol download yang ada pada sistem.

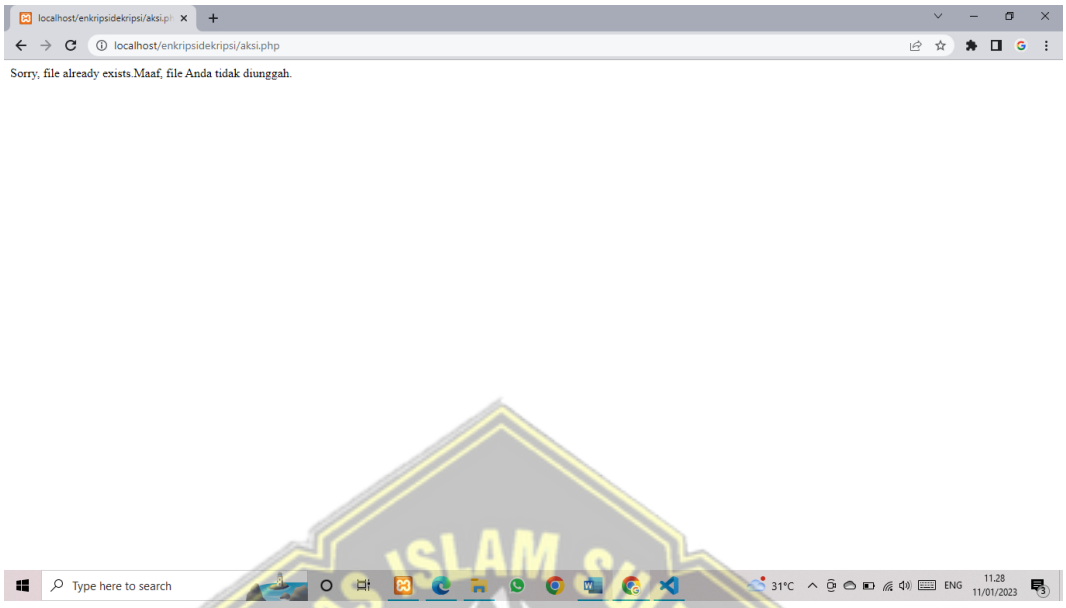
2. Tapilan upload gambar yang akan di Enkripsi



Gambar 4.2 Tampilan Upload Gambar

Pada gambar 4.2 merupakan tampilan proses upload gambar asli yang akan dienkripsi. Langkah pertama yaitu user mengklik tombol pilih file kemudian akan muncul tab baru lalu user memilih file yang akan di proses enkripsi lalu klik open kemudian jika sudah klik tombol upload yang ada di tampilan sistem, setelah itu sistem akan mengenkripsi dokumen yang telah diupload.

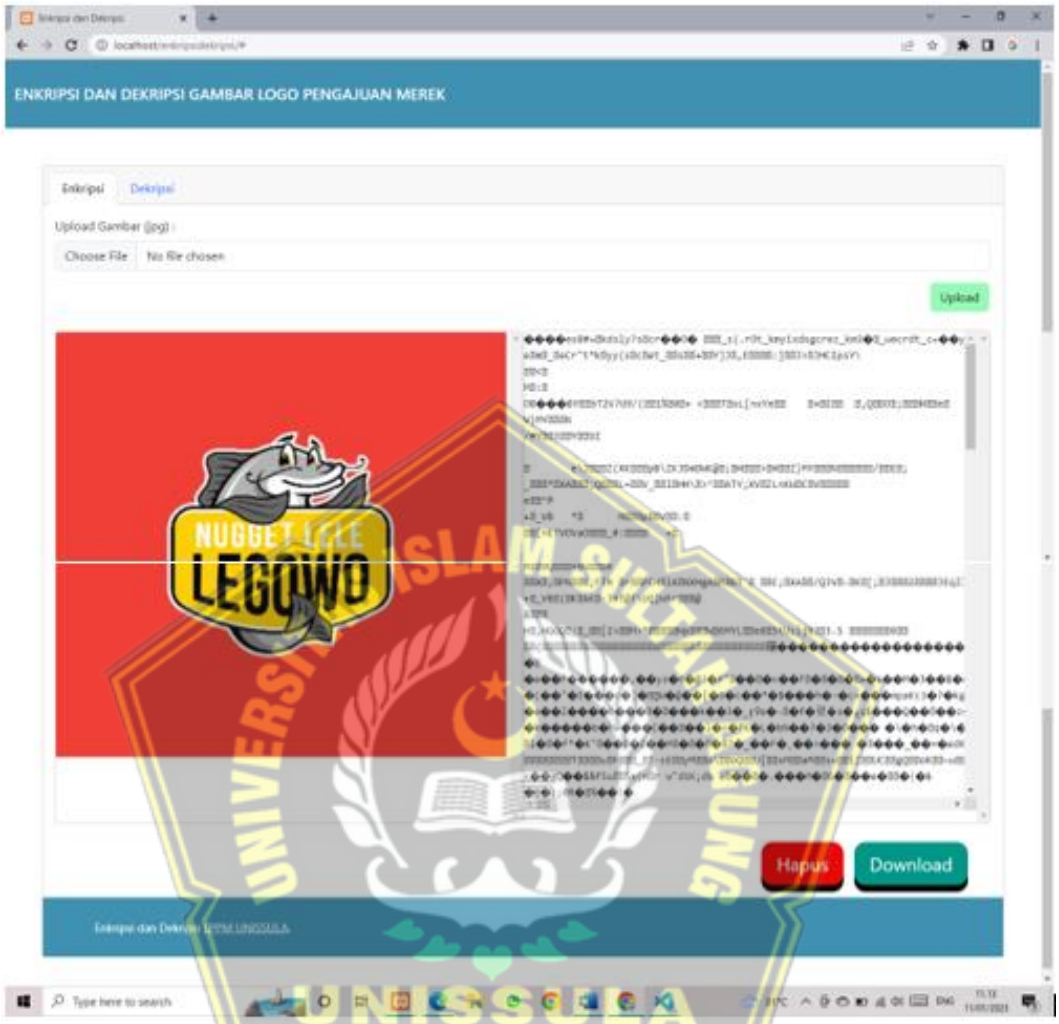
3. Tampilan ketika upload dokumen selain format JPG.



Gambar 4.3 Tampilan upload dokumen selain format JPG

Pada gambar 4.3 merupakan tampilan ketika user mengupload gambar dengan format selain jpg akan menampilkan seperti gambar diatas dan file akan gagal di upload.

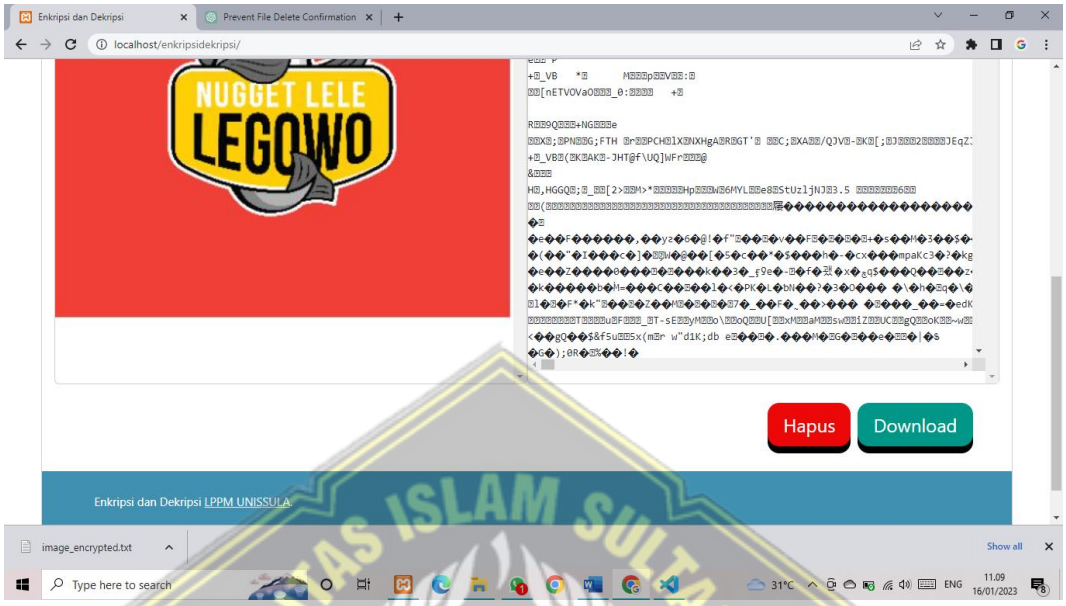
4. Tampilan setelah proses Enkripsi



Gambar 4.4 Tampilan Setelah Proses Enkripsi

Pada gambar 4.4 merupakan tampilan dari hasil setelah proses Enkripsi dimana didalam tampilan tersebut terdapat tampilan gambar asli yang diupload oleh user dan tampilan hasil Enkripsi. Terdapat juga tombol hapus dan download, dimana fungsi dari tombol hapus yaitu menghapus file yang diupload dan file hasil enkripsi didalam sistem sedangkan tombol download berfungsi untuk mendownload file hasil dari proses enkripsi.

5. Tampilan download dokumen enkripsi



Gambar 4. 5 Tampilan Download Dokumen Enkripsi

Pada gambar 4.5 merupakan tampilan ketika user telah mendownload dokumen yang telah dienkripsi dimana user telah mengklik tombol download dokumen akan terunduh ke dalam folder download di dalam perangkat yang digunakan oleh user.

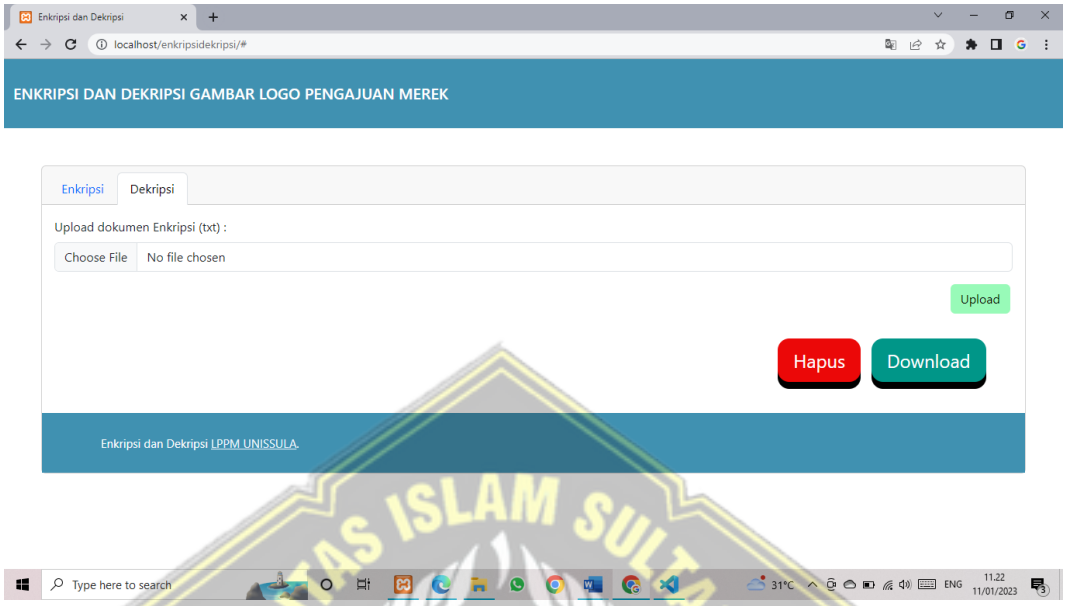
6. Tampilan dokumen hasil Enkripsi

Gambar 4.6 Tampilan Dokumen Hasil Enkripsi

Pada gambar 4.6 merupakan tampilan hasil dari Enkripsi gambar dengan format TXT.

4.1.2 Tampilan *User Interface* (UI) Dekrispi

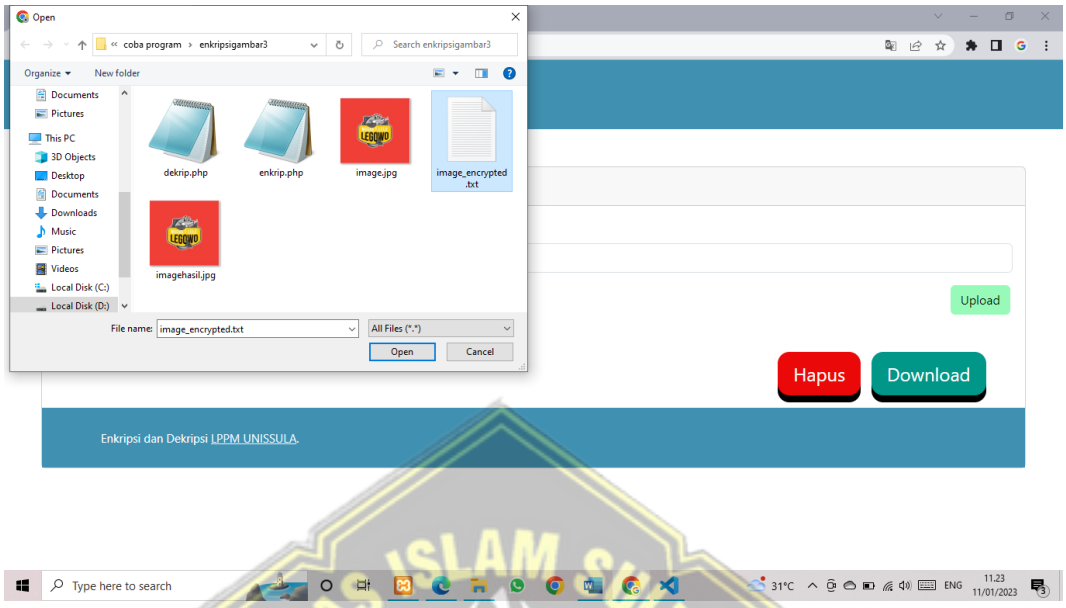
1. Tampilan Dekripsi



Gambar 4. 7 Tampilan Menu Dekripsi

Pada gambar 4.7 merupakan tampilan dari sistem Dekripsi, dimana didalam sistem tersebut terdapat beberapa menu antara lain yaitu menu upload hasil enkripsi, tampilan hasil enkripsi yang telah di upload, tampilan hasil dekripsi. Kemudian ada beberapa tombol seperti pilih file, dekripsi, dan download. Langkah pertama dalam proses Dekripsi yaitu upload dokumen hasil Enkripsi lalu sistem akan memproses Dekripsi menggunakan algoritma XOR kemudian setelah proses selesai sistem akan menampilkan dokumen yang diupload dan gambar hasil Dekripsi.

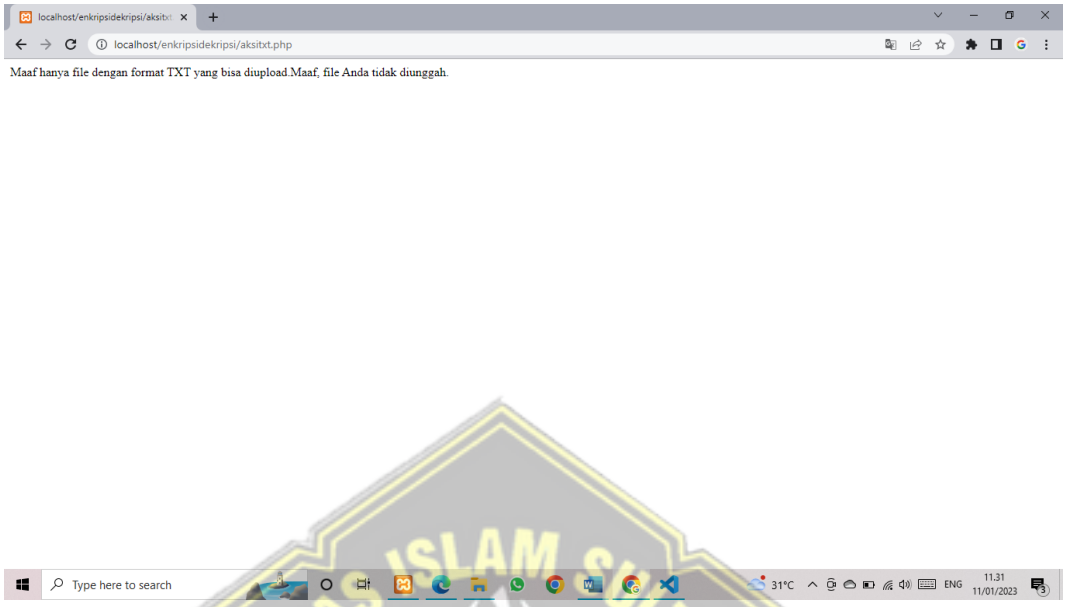
2. Tampilan upload dokumen yang akan di Dekripsi



Gambar 4.8 Tampilan Upload Dokumen Enkripsi

Pada gambar 4.8 merupakan tampilan proses upload file hasil enkripsi yang akan didekripsi. Langkah pertama yaitu user mengklik tombol pilih file kemudian akan muncul tab baru lalu user memilih file yang akan di proses dekripsi lalu klik open selanjutnya jika sudah klik tombol upload yang ada pada di tampilan sistem, setelah itu sistem akan dekripsi dokumen yang telah diupload.

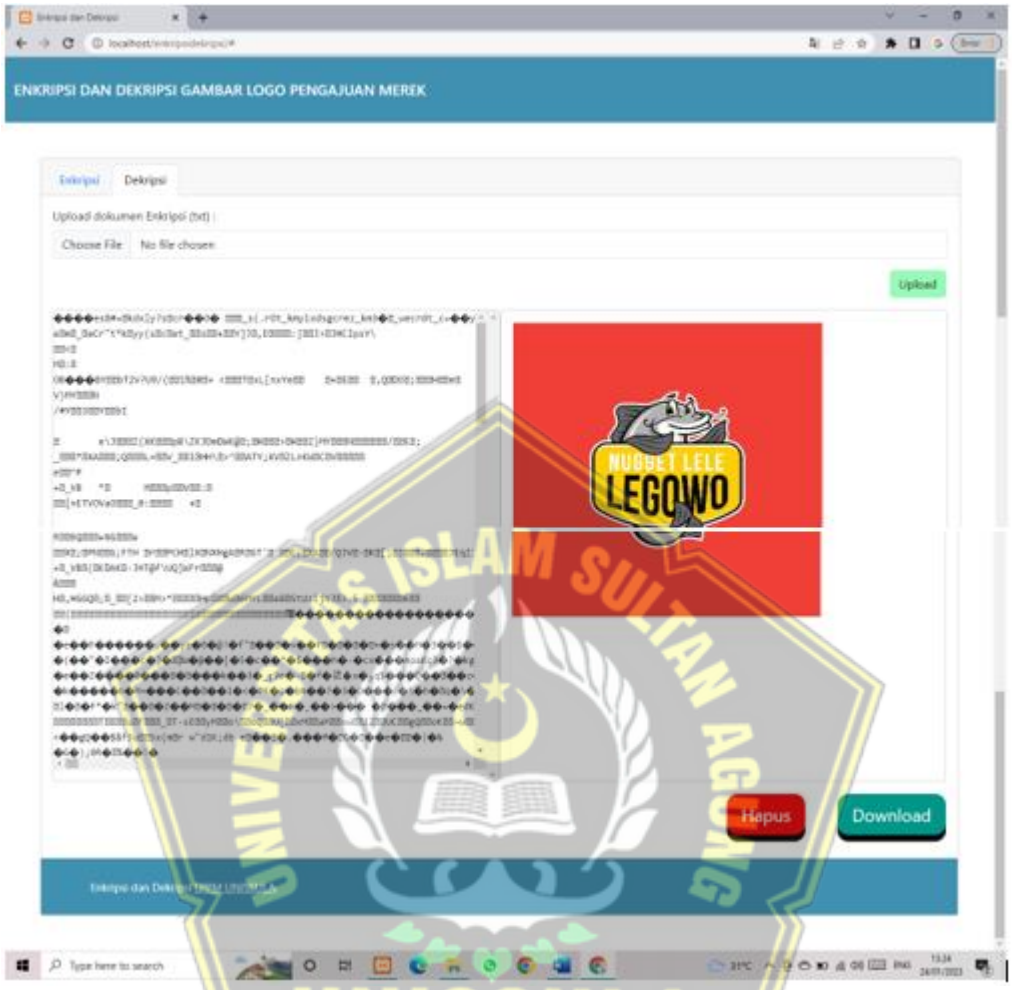
3. Tampilan ketika upload dokumen selain format TXT.



Gambar 4.9 Tampilan upload dokumen selain format TXT

Pada gambar 4.9 merupakan tampilan ketika user mengupload file dengan format selain txt akan menampilkan seperti gambar diatas dan file akan gagal di upload.

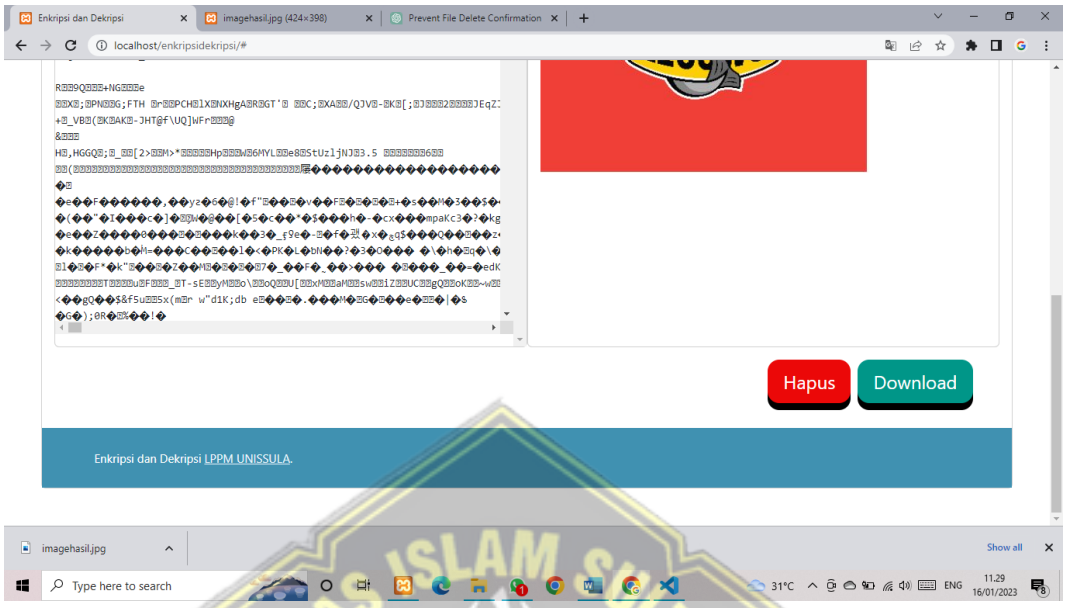
4. Tampilan hasil proses Dekripsi



Gambar 4. 10 Tampilan Menu Setelah Proses Dekripsi

Pada gambar 4.10 merupakan tampilan hasil setelah proses Dekripsi dimana didalam tampilan tersebut terdapat tampilan file enkripsi yang diupload oleh user dan tampilan gambar hasil Dekripsi. Terdapat juga tombol hapus dan download, dimana fungsi dari tombol hapus yaitu menghapus file yang diupload dan file hasil enkripsi didalam sistem sedangkan tombol download berfungsi untuk mendownload gambar hasil dari proses Dekripsi.

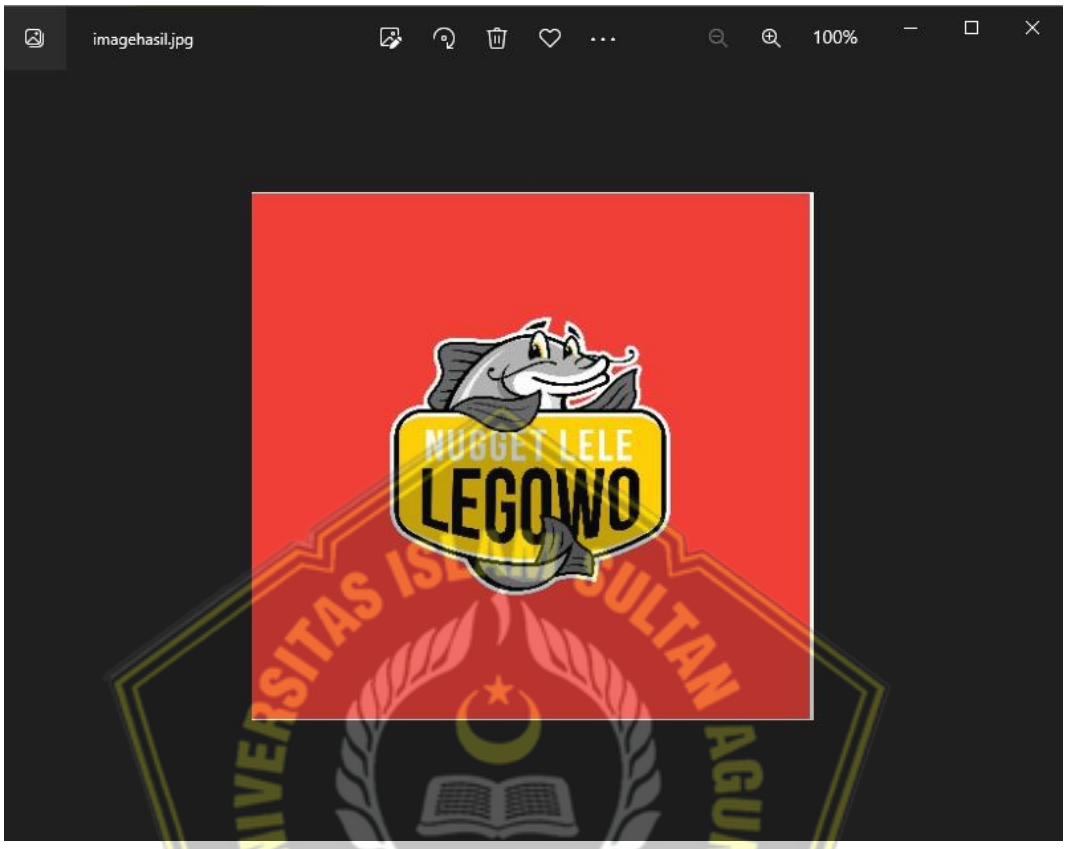
5. Tampilan download gambar hasil dekripsi



Gambar 4.11 Tampilan Download Gambar Hasil Dekripsi

Pada gambar 4.11 merupakan tampilan ketika user telah mendownload dokumen yang telah didekripsi dimana user telah mengklik tombol download dokumen akan terunduh ke dalam folder download di dalam perangkat yang digunakan oleh user.

6. Tampilan gambar hasil dekripsi



Gambar 4. 12 Tampilan Gambar Hasil Dekripsi

Pada gambar 4.12 merupakan tampilan hasil gambar yang sudah didekripsi, dimana gambar hasil dekripsi berhasil kembali seperti gambar asli.

4.2 Pengujian Sistem

Black Box Testing merupakan satu diantara metode yang dapat digunakan untuk proses pengujian sistem ini. Black Box Testing digunakan karena untuk memastikan bahwa setiap komponen bekerja sesuai dengan parameter proses yang sudah didefinisikan dalam kaitannya dengan input yang didefinisikan. Black Box Testing dengan demikian harus memastikan bahwa pengguna memasukkan data yang akurat dan sistem menampilkan hasil yang sesuai dengan fungsionalitas setiap komponen sistem. Pada tahap pengujian yang dilakukan kali ini menggunakan jenis fungction testing yang akan dilakukan proses pengujian dari setiap fungsi yang ada pada sistem.

4.2.1 Pengujian Enkripsi Gambar

Tabel 4. 1 Pengujian *Enkripsi* gambar

Hasil dari uji coba (Menggunakan Data *Valid*)				
Pengujian Gambar	**Kasus Uji**	**Hasil Uji Coba Yang Diharapkan**	**Hasil Uji Coba**	**Keterangan**
Enkripsi Gambar.jpg 	Upload Gambar	Bisa Enkripsi gambar	Sesuai	Sukses
Hasil dari uji coba (Menggunakan Data *Invalid*)				
Pengujian Gambar	**Kasus Uji**	**Hasil Uji Coba Yang Diharapkan**	**Hasil Uji Coba**	**Keterangan**
Enkripsi Gambar dengan format PNG 	Upload gambar	Gagal melakukan Enkripsi	Sesuia	Sukses

Enkripsi Gambar dengan format PDF 	Upload gambar	Gagal melakukan Enkripsi	Sesuai	Sukses

4.2.2 Pengujian Dekripsi *gambar*

Tabel 4. 2 Pengujian dekripsi gambar

Hasil dari uji coba (Menggunakan Data *Valid*)				
Pengujian Dokumen	**Kasus Uji**	**Hasil Uji Coba Yang Diharapkan**	**Hasil Uji Coba**	**Keterangan**
Dekripsi gambar format TXT 	Import enkripteks.txt	Bisa melakukan Dekripsi	Sesuai	Sukses
Hasil dari uji coba (Menggunakan Data *Invalid*)				
Pengujian Dokumen	**Kasus Uji**	**Hasil Yang Diharapkan**	**Hasil**	**Keterangan**
Dekripsi gambar dengan format PDF 	Import enkripteks.pdf	Gagal melakukan dekripsi	Sesuai	Sukses

4.3 Hasil dan Analisa

Hasil dari penelitian ini dapat menerapkan metode algoritma XOR digunakan untuk enkripsi dan dekripsi memberikan hasil yang sesuai dengan yang direncanakan dan hasil yang di berikan cukup memuaskan untuk digunakan enkripsi gambar. Dan hasil dari dekripsi sesuai dengan gambar aslinya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari hasil proses penelitian yang sudah dilakukan oleh penulis, dapat menyimpulkan bahwa dari hasil proses pengujian yang sudah dilakukan memperoleh hasil berikut ini :

1. Algoritma XOR dapat diimplementasikan buat melakukan proses enkripsi dan dekripsi gambar.
2. Hasil yang diperoleh dari enkripsi gambar memiliki ekstensi (nama_file).txt

5.2 Saran

Dari proses penelitian yang sudah dilakukan, peneliti memiliki sejumlah saran untuk mengembangkan sistem ini kedepannya menjadi sistem yang lebih lengkap diantaranya sebagai berikut:

1. Diperlukan tambahan algoritman AES bertujuan untuk lebih meningkatkan keamanan pada gambar.
2. Untuk desainnya disempurnakan lagi agar lebih mempermudah user yang memakainya.
3. Program dapat melakukan enkripsi format gambar pdf, png.

DAFTAR PUSTAKA

A, Andryanto, D. (2017). Perancangan Aplikasi Pengamanan Data Menggunakan Algoritma XOR. *Jurnal Teknik Informatika Unika St. Thomas (JTIUST), Volume 02 Nomor 02, Desember 2017*, *8*(1), 61–69.

Achmad, Y. F., & Yulfitri, A. (2020). Pengujian Sistem Pendukung Keputusan Menggunakan Black Box Testing Studi Kasus E-Wisudawan Di Institut Sains Dan Teknologi Al-Kamal. *Jurnal Ilmu Komputer*, *5*, 42.

Agustini, S., & Kurniawan, M. (2019). Peningkatan Keamanan Teks Menggunakan Kriptografi Dan Steganografi. *SCAN - Jurnal Teknologi Informasi Dan Komunikasi*, *14*(3), 33–38. https://doi.org/10.33005/scan.v14i3.1685

Amalia, R., & Rosyani, P. (2018). Implementasi Algoritma AES dan Algoritma XOR pada Aplikasi Enkripsi dan Dekripsi Teks Berbasis Android. *Faktor Exacta*, *11*(4), 370. https://doi.org/10.30998/faktorexacta.v11i4.2878

Aripin, S., & Somantri, S. (2021). Implementasi Progressive Web Apps (PWA) pada Repository E-Portofolio Mahasiswa. *Jurnal Eksplora Informatika*, *10*(2), 148–158. https://doi.org/10.30864/eksplora.v10i2.486

Butsianto, S. (2020). Pengembangan Sistem Informasi Penjualan Berbasis Web Menggunakan Metode Prototyping Pada Toko Bay Sticker. *Administrative Law Journal*, *60*, 53–77. https://doi.org/10.35979/alj.2020.02.60.53

Junianto, M. B. S., Ardiansyah, H., & ... (2020). Analisa Dan Perancangan Sistem Informasi Pengaman Dokumen Dengan Metode Algoritma XOR dan AES Berbasis Web (Studi Kasus: Bimbingan Belajar Matriks Pamulang). *JOAIIA: Journal of …*, *1*(2), 61–66.

Makiolor, A. A. A., Sinsuw, A., & B.N. Najoan, X. (2017). Rancang Bangun Pencarian Rumah Sakit, Puskesmas dan Dokter Praktek Terdekat di Wilayah Manado Berbasis Android. *Jurnal Teknik Informatika*, *10*(1). https://doi.org/10.35793/jti.10.1.2017.16552

Mubarak, A. (2019). Rancang Bangun Aplikasi Web Sekolah Menggunakan Uml (Unified Modeling Language) Dan Bahasa Pemrograman Php (Php Hypertext

Preprocessor) Berorientasi Objek. *JIKO (Jurnal Informatika Dan Komputer)*, *2*(1), 19–25. https://doi.org/10.33387/jiko.v2i1.1052

Novendri. (2019). Aplikasi Inventaris Barang Pada Mts Nurul Islam Dumai Menggunakan Php Dan Mysql. *Lentera Dumai*, *10*(2), 46–57.

Poetro, B. S. W., & Wardoyo, R. (2017). Perbandingan Efisiensi, Efektifitas dan Kualitas Algoritma Rijndael dengan Algoritma Camellia pada Citra Digital. *Bimipa*, *24*(3), 281–291.

Refialy, L. P. (2022). *KOMPUTA : Jurnal Ilmiah Komputer dan Informatika ALGORITMA XOR KOMPUTA : Jurnal Ilmiah Komputer dan Informatika*. *11*(1).

Santoso, M. H. (2019). *Perbandingan Algoritma Kriptografi Hash MD5 dan SHA-1*. *2*(November), 54–59.

Sidik, A. P., Komputer, S., Sains, F., Pembangunan, U., Budi, P., Gatot, J. J., Km, S., Sikambing, S., Medan, K., & Utara, S. (2019). Teknik Xor Pada Mode Operasi Algoritma Cipher Block Chaining (Cbc) Dengan Kunci Acak Blum Blum Shub Dalam Meningkatkan Keamanan Data. *Jurnal Mantik Penusa*, *3*(2), 130–135.

Siregar, H. F., & Sari, N. (2018). Rancang Bangun Aplikasi Simpan Pinjam Uang Mahasiswa Fakultas Teknik Universitas Asahan Berbasis Web. *Jurnal Teknologi Informasi*, *2*(1), 53. https://doi.org/10.36294/jurti.v2i1.409