PEMBUATAN VERIFIKASI SERTIFIKAT DIGITAL SEBAGAI BUKTI KEABSAHAN MENGGUNAKAN ALGORITMA STEGANOGRAFI DENGAN METODE *LEAST SIGNIFICANT BIT INSERTION* (LSB)

SKRIPSI

Diajukan sebagai Salah Satu Syarat untuk Mendapatkan
Gelar Sarjana Komputer (S.Kom) Program Studi Informatika

MUH. NUR AQSAL AMINULLAH

105841102918

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2022

UNIVERSITAS MUHAMMADIYAH MAKASSAR
FAKULTAS TEKNIK
GEDUNG MENARA IQRA LT. 3
Jl. Sultan Alauddin No. 259 Telp. (0411) 866 972 Fax (0411) 865 588 Makassar 90221
Website: www.unismuh.ac.id, e_mail: unismuh@gmail.com
Website: http://teknik.unismuh.makassar.ac.id

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

PENGESAHAN

Skripsi atas nama Muh. Nur Aqsal Aminullah dengan nomor induk Mahasiswa 105841102918, dinyatakan diterima dan disahkan oleh Panitia Ujian Tugas Akhir/Skripsi sesuai dengan Surat Keputusan Dekan Fakultas Teknik Universitas Muhammadiyah Makassar Nomor : 446/05/A.5-VI/VI/43/2022, sebagai salah satu syarat guna memperoleh gelar Sarjana Komputer pada Program Studi Informatika Fakultas Teknik Universitas Muhammadiyah Makassar pada hari Sabtu tanggal 30 Agustus 2022.

Makassar, 09 Safar 1444 H / 06 September 2022 M

Panitia Ujian :

1. Pengawas Umum
   a. Rektor Universitas Muhammadiyah Makassar
      Prof. Dr. H. Ambo Asse, M.Ag. : .....
   b. Dekan Fakultas Teknik Universitas Hasanuddin
      Prof. Dr. Eng. Muhammad Isran Ramli, ST., MT. : .....
2. Penguji
   a. Ketua : Dr. Ir. Zahir Zainuddin, M.Sc. : .....
   b. Sekertaris : Chyquitha Danuputri, S.Kom, M.Kom. : .....
3. Anggota : 1. Lukman Anas, S.Kom., MT. : .....
   2. Fahrim Irhamna Rahman S.Kom., MT. : .....
   3. Lukman, S.Kom., MT. : .....

Mengetahui :

Pembimbing I

Rizki Yusliana Bakti ST., MT.

Pembimbing II

Muhyiddin A. M. Hayat, S.Kom., MT

Dekan

Dr. Ir. Hj. Nurnawaty, ST., MT., IPM.
NBM : 795 108

UNIVERSITAS MUHAMMADIYAH MAKASSAR
FAKULTAS TEKNIK
GEDUNG MENARA IQRA LT. 3
Jl. Sultan Alauddin No. 259 Telp. (0411) 866 972 Fax (0411) 865 588 Makassar 90221
Website: www.unismuh.ac.id, e_mail: unismuh@gmail.com
Website: http://teknik.unismuh.makassar.ac.id

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

HALAMAN PENGESAHAN

Tugas Akhir ini diajukan untuk memenuhi syarat ujian guna memperoleh gelar Sarjana Komputer (S.Kom) Program Studi Informatika Fakultas Teknik Universitas Muhammadiyah Makassar.

Judul Skripsi : **PEMBUATAN VERIFIKASI SERTIFIKAT DIGITAL SEBAGAI BUKTI KEABSAHAN MENGGUNAKAN ALGORITMA STEGANOGRAFI DENGAN METODE LEASTSIGNIFICANT BIT INSERTION (LSB)**

Nama : Muh. Nur Aqsal Aminullah
Stambuk : 105841102918

Makassar, 06 September 2022

Telah Diperiksa dan Disetujui
Oleh Dosen Pembimbing;

Pembimbing I	Pembimbing II
Rizki Yusliana Bakti ST., MT	**Muhyiddin A. M. Hayat, S.Kom., MT**

Mengetahui,
Ketua Program Studi Informatika

Muhyiddin A. M. Hayat, S.Kom., MT
NBM : -

ABSTRAK

MUH. NUR AQSAL AMINULLAH. Pembuatan verifikasi sertifikat digital sebagai bukti keabsahan menggunakan Algoritma Steganografi dengan Metode *Least Significant Bit Insertion* (LSB) (dibimbing oleh Rizki Yusliana Bakti, ST.,MT dan Muhyiddin AM Hayat, S.Kom.,MT).

Tujuan dari penelitian ini adalah untuk memberikan sebuah kemudahan dalam proses pembuatan sertifikat terutama untuk mendapatkan tanda tangan digital menggunakan sistem autentikasi dan memberikan sebuah keamanan pada sertifikat digital menggunakan algoritma steganografi dengan metode least significant bit. Sertifikat digital adalah sebuah sertifikat yang bersifat elektronik dimana memuat sebuah tanda tangan digital penyelenggara kegiatan dan identitas dari pemilik sertifikat digital tersebut.

Pada sertifikat digital yang dibuat ini menggunakan algoritma steganografi dengan metode *least significant bit* sebagai sistem keamanan dari sertifikat digital tersebut. Steganografi ini adalah sebuah teknik penyembunyian pesan rahasia yang hanya dapat diketahui oleh pengirim dan penerima tanpa menimbulkan kecurigaan. Least significant bit ini adalah salah satu metode yang terdapat pada algoritma steganografi dimana proses penyembunyian pesannya adalah dengan menggunakan wadah dengan dengan format *image* JPG dan menyisipkan pesan rahasia ke dalam bit *pixel* pada wadah tersebut.

Hasil yang didapatkan dari penelitian yang dilakukan menunjukkan bahwa sistem autentikasi yang dibuat untuk mendapatkan tanda tangan digital penyelenggara berhasil dilakukan dengan mengirimkan pesan notifikasi permintaan untuk mendapatkan tanda tangan digital dan keamanan yang diberikan pada sertifikat digital yang berhasil dibuat juga berhasil dipasangkan dan pengecekan terhadap sertifikat digital juga berhasil dilakukan agar dapat mengetahui sertifikat digital tersebut asli atau hasil duplikasi atau modifikasi pihak ketiga.

Kata kunci : steganografi; LSB; sertifikat digital; autentikasi; verifikasi;

ABSTRACT

MUH. NUR AQSAL AMINULLAH. *Making digital certificate verification as proof of validity using the Steganographic Algorithm with the Least Significant Bit Insertion Method (LSB)* (*supervised by* Rizki Yusliana Bakti, ST.,MT *and* Muhyiddin AM Hayat, S.Kom.,MT).

The purpose of this study is to provide an convenience in the process of making certificates, especially to obtain digital signatures using an authentication system and provide security for digital certificates using a steganographic algorithm with the least significant bit method. A digital certificate is an electronic certificate which contains a digital signature of the event organizer and the identity of the owner of the digital certificate.

In this digital certificate, it uses a steganographic algorithm with the least significant bit method as a security system for the digital certificate. Steganography is a technique of hiding secret messages that can only be known by the sender and recipient without raising suspicion. This least significant bit is one of the methods found in the steganography algorithm where the message hiding process is to use a container with a JPG image format and insert a secret message into the pixel bits in the container.

The results obtained from the research conducted indicate that the authentication system created to obtain the organizer's digital signature was successfully carried out by sending a notification message requesting to get a digital signature and the security provided on the successfully created digital certificate was also successfully paired and checking the digital certificate as well. successfully carried out in order to determine whether the digital certificate is genuine or the result of a third party duplication or modification.

Keywords: steganography, LSB, digital certificate, authentication, verification

KATA PENGANTAR

بِسْـــمِ اللهِ الرَّحْمَنِ الرَّحِيْم

Segala puji bagi ALLAH SWT, yang telah memberikan rahmat dan hidayah-Nya kepada penulis, sehingga peneliti dapat melaksanakan pembuatan skripsi dan dapat diselesaikan sesuai dengan yang penulis harapkan

Dalam pembuatan skripsi dan proses penyusunannya, penulis mendapat banyak bantuan, dukungan dan bimbingan dari berbagai pihak. Oleh karena itu dalam kesempatan ini peneliti ingin menyampaikan ucapan terima kasih yang sebesar-besarnya kepada :

1. Terima kasih kepada Allah SWT
2. Ibu Dr.Ir.Hj Nurnawati, S.T.,M.T.,I.P.M, Selaku Dekan Fakultas Teknik
3. Bapak Muh. Syafaat S Kuba, ST.,MT Selaku Wakil Dekan Fakultas Teknik
4. Ibu Rizki Yusliana Bakti, S.T.,M.T selaku pembimbing pertama Universitas Muhammadiyah Makassar.
5. Bapak Muhyiddin AM Hayat, S.Kom.,M.T Selaku pembimbing kedua dan Ketua Jurusan Program Studi Informtika Fakultas Teknik
6. Kedua orang tua saya, Bapak Aminullah dan Ibu Nelda Arda

Penulis juga menyadari bahwa di dalam penyusunan skripsi ini terdapat banyak kekurangan dan kesalahan. Oleh karena itu penulis mengharapkan kritik dan saran yang bersifat membangun, sehingga laporan penulis selanjutnya dapat menjadi lebih baik.

Akhir kata semoga skripsi ini dapat memberi manfaat bagi pembaca umumnya dan bagi penulis pada khususnya.

Makassar, 2022

Hormat Saya

Peneliti

DAFTAR ISI

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR ISTILAH

Platform	*Platform* adalah sekelompok teknologi yang digunakan sebagai dasar di mana aplikasi, proses, atau teknologi lain dikembangkan.
Citra digital	*Citra digital* merupakan representasi dari fungsi intensitas cahaya dalam bentuk diskrit pada bidang dua dimensi.
Bit	*Bit* adalah kependekan dari "Binary Digit", yang berarti digit biner. Binary digit adalah unit satuan terkecil dalam komputasi digital.
Byte	*Byte* adalah sebuah kumpulan dari beberapa bit
Pixel	*Pixel* adalah unsur gambar atau representasi sebuah titik terkecil dalam sebuah gambar grafis yang dihitung per inci.
Kriptografi	Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi.
Encode	Encode adalah proses penempatan urutan karakter (huruf, angka, tanda baca, dan symbol tertentu) ke dalam format khusus sehingga menjadi sebuah sandi.
Decode	Decode adalah proses sebaliknya yaitu konversi dari format yang disandikan kembali pada karakter asli.
Invisible ink	*Invisible ink* adalah zat yang digunakan untuk menulis, yang tidak terlihat baik pada aplikasi atau segera sesudahnya, dan kemudian dapat dibuat terlihat dengan beberapa cara, seperti panas atau sinar ultraviolet.

Stego key	*Stego key* adalah kata kunci untuk mengimplementasikan algoritma steganografi
Embedding	*Embedding* adalah istilah yang digunakan untuk representasi kata untuk analisis teks, biasanya dalam bentuk vektor bernilai nyata yang mengkodekan arti kata sedemikian rupa schingga kata-kata yang lebih dekat dalam ruang vektor diharapkan.
Stego objeck	Kunci yang digunakan untuk menyisipan pesan dan mengekstraksi pesan dari *stegotext*.
Stego cover	Wadah yang sudah berisi pesan *embedded message*
Redundant	*Redudant* adalah nilai yang tidak akan terlalu mempengaruhi nilai yang lain saat diubah
Significant	*Significant* adalah nilai yang dianggap tidak terlalu penting
Biner	Sistem bilangan biner atau sistem bilangan basis dua adalah suatu sistem penulisan angka dengan menggunakan dua lambang adalah 0 dan 1.
ASCII	ASCII adalah singkatan dari American Standard Code for Information Interchange.
Digital signature	*Digital signature* adalah salah satu teknologi yang digunakan untuk meningkatkan keamanan jaringan.
Spread Spectrum	*Spektrum* tersebar adalah sebuah metode komunikasi dimana semua sinyal komunikasi disebar di seluruh spektrum frekuensi yang tersedia.
Pseudorandom	*Pseudirandom* adalah sebuah algoritma untuk menghasilkan urutan angka yang propertinya mendekati sifat-sifat urutan nomor acak.
Squared Error	*Square error* adalah selisih antara nilai target output

	dengan nilai actual output.
Peak Signal to-Noise Ratio	*Peak signal-to-noise ratio* adalah istilah rekayasa untuk rasio antara kekuatan maksimum yang mungkin dari sinyal dan kekuatan suara yang merusak yang mempengaruhi kesetiaan representasinya.
Kriptografi Triple Des	*Triple DES* adalah salah satu sistem enkripsi berlapis tiga dari sistem yang sebelumnya sudah ada, yaitu DES.
Stego file	*Stego file* adalah sebuah hasil proses pengolaan yang dihasilkan oleh steganografi
Qrcode	QR code adalah singkatan dari quick response code. Arti dari kode dalam QR code ini adalah barcode dua dimensi yang bisa memberikan beragam jenis informasi secara langsung.
Central Event Information	CEI (*Central Event Information*) merupakan sebuah sistem yang digunakan untuk mendokumentasikan sebuah pelatihan
Enkripsi Vigenere Cipher	*Enkripsi Vigenere Cipher* adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci.
Software	*Software* merupakan perangkat lunak yang biasa dikenal dengan aplikasi yang digunakan untuk mengolah data sesuai dengan fungsi masing-masing.
Inkonsistensi	*Inkonsistensi* suka berubah-ubah (tentang sikap atau pendirian seseorang, pemakaian atau pengejaan kata, dsb.
Independen	Independen adalah setuatu hal yang berdiri sendiri
Field notes	*Field note* dapat diartikan sebagai catatan kegiatan

	lapangan
Display	*Display* adalah suatu cara penataan produk, terutama produk barang yang diterapkan oleh perusahaan tertentu dengan tujuan untuk menarik minat konsumen.
Flowchart	*Flowchart* adalah diagram alir yang tersusun dari bagan dengan berbagai bentuk.
Freeze	*Freeze* adalah keadaan dimana sebuah layar halaman sebuah website ditak bisa di gunakan karena keadaan tertentu.

BAB I
PENDAHULUAN

A. Latar Belakang

Sertifikat yang sudah biasa kita ketahui adalah sebuah tanda hak yang berlaku sebagai alat bukti dan kokoh mengenai data fisik dan data hukum yang terkandung di dalamnya, sepanjang data fisik dan data hukum tersebut sesuai dengan data yang tercantum dalam sertifikat yang dimiliki. Seiring berkembangnya teknologi sekarang ini sertifikat sudah tidak banyak orang yang menggunakan sertifikat secara fisik yang diketahui secara luas dapat mudah hilang, oleh sebab itu saat ini orang-orang banyak menggunakan sertifikat digital yang lebih mudah digunakan dan dapat dibuka dimana saja.

Sertifikat digital merupakan sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan penyelenggara sertifikasi elektronik (wibowo subekti, 2021). Sertifikat digital menampilkan informasi seperti informasi kunci, identitas pemiliknya, serta tanda tangan digital suatu organisasi yang memverifikasi sertifikat. Sertifikat ini dapat dikatakan adalah sebuah document yang sangat penting karena sertifikat ini dapat menjadikan bukti untuk mewakili kemampuan seseorang ataupun bukti untuk mengetahui seseorang tersebut pernah mengikuti sebuah acara ataupun event formal dan juga sertifikat digital ini dapat dijadikan sebgai bukti sebuah kepemilikan benda berharga.

Sertifikat digital sendiri saat ini sudah sangat sering digunakan oleh berbagai instansi dan juga khalayak umum dalam sebuah organisasi yang kita ketahui banyak yang menyelenggarakan sebuah acara atau event formal yang dimana setiap peserta sudah pasti akan mendapatkan sertifikat mereka masing-masing sebagai bukti mengikuti acara tersebut dan juga salah satunya yang

paling banyak digunakan sekarang dalam bidang akademik yang banyak membuat *platform* pembelajaran online dengan banyak menawarkan berbagai kelas yang berbayar maupun gratis. Sertifikat digital sendiri juga dapat lebih mempermudah orang-orang dalam mengakses sertifikat tanpa perlu menyimpan bukti fisiknya yang beresiko rusak ataupun hilang.

Dibalik banyaknya keuntungan yang didapatkan dalam memperoleh sertifikat digital, namun tidak akan terlepas dari berbagai resiko, ancaman dan tantangan yang perlu dihadapi, dalam hal ini yang dimaksud adalah bagaimana membuat sebuah sertifikat digital dengan mudah tanpa harus menemui pihak yang bersangkutan untuk mendapatkan tanda tangan digitalnya, bagaimana memberitahukan pihak yang bersangkutan tentang pemakaian tanda tangan nya dan jumlah sertifikat yang akan di buat agar tanda tangan dari pihak yang bersangkutan tidak di salah gunakan dan tentu saja dalam sebuah sertifikat digital harus diberikan sebuah pengamanan di setiap sertifikat digital agar sertifikat ini tidak dapat dimodifikasi oleh pihak ketiga.

Ada beberapa teknik atau algoritma yang dapat digunakan untuk membuats sistem keamanan dalam sebuah pengaplikasian seperti pesan teks, video, dan pengamanan data penting. Seperti penelitian yang dilakukan oleh Swastika, santo dan Kelana yaitu membuat sebuah rancang bangun website akademik untuk penyimpanan sertifikat digital dengan menggunakan Teknologi *Blockchain.* Penelitian ini memberikan sebuah tempat untuk menyimpan data dari sebuah sertifikat digital untuk mengamankan sertifikat digital tersebut (Swastika et al., 2022). Penelitian selanjutnya yang dilakukan oleh Hafis yaitu *Steganografi* berbasis citra digital untuk menyembunyikan data menggunakan metode *least significa nt bit* (Hafis, 2019) yang dimana pada penelitian ini mencoba menyembunyikan sebuah data rahasia berbasis citra.

Berdasarkan latar belakang dan hasil penelitian sebelumnya, maka pada penelitian ini penulis mencoba memberikan sebuah solusi untuk mengefektifkan dalam pembuatan sertifikat digital dengan mudah dan dapat dilakukan oleh setiap

pihak yang ingin membuat sertifikat untuk setiap mengadakan acara atau event. Dari hal tersebut maka diterapkan algoritma *steganografi* dengan metode LSB dalam memberikan keamanan serta untuk mengetahui keabsahan setiap sertifikat karena dapat membuat sebuah teks pesan yang diinginkan bisa disisipkan kedalam sertifikat digital ini sebagai sistem keabsahan sertifikat digitalnya. Selain itu bentuk pengeluaran yang diinginkan peneliti pada aplikasi pembuatan sertifikat digital ini yaitu menggunakan format image. Format pengeluaran image ini digunakankan karena pada dasarnya sebuah sertifikat digital format yang sering digunakan yaitu image dan pdf, oleh karen itu pada penelitian ini akan menggunakan format image karena berhubungan dengan metode penelitian yang digunakan.

B. Rumusan Masalah

Adapun beberapa rumusan yang dapat diambil dari latar belakang yang telah dipaparkan di atas adalah:

1. Bagaimana mendapatkan tanda tangan digital dari penyelenggara acara atau event dengan sistem autentikasi ?
2. Bagaimana memberikan keamanan untuk membuktikan keabsahan sertifikat digital ?
3. Bagaimana memperlihatkan bukti keabsahan terhadap sertifikat digital yang dibuat ?

C. Tujuan Penelitian

Adapun tujuan yang hendak dicapai dalam penelitian ini adalah sebagai berikut :

1. Memberikan sebuah aplikasi pembuatan sertifikat digital dengan sistem autentikasi.
2. Memberikan sebuah keamanan terhadap sertifikat digital menggunakan algoritma *steganograf* dengan metode (LSB)
3. Memperlihatkan sebuah bukti keabsahan sertifikat digital.

D. Manfaat Penelitian

Adapun beberapa manfaat dari penelitian yang dilakukan bagi penulis dan juga bagi pengguna yaitu:

1. Bagi penulis

   Dapat memberikan wawasan lebih luas dalam memberikan pengetahuan dalam membangun aplikasi pembuatan sertifikat digital yang menggunakan sistem verifikasi dan memberikan pengetahuan yang lebih dalam tentang keamanan data untuk penyembunyian data rahasia.

2. Bagi pengguna

   Bisa membantu dalam menyelesaikan masalah dalam hal kemudahan pembuatan sertifikat yang memiliki keamanan untuk tetap menjaga keabsahan dari sertifikat digital.

E. Ruang Lingkup Penelitian

Agar pembahasan penelitian ini tidak meluas, maka perlu pembatasan masalah, Batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Aplikasi pembuatan sertifikat digital hanya bisa digunakan di ruang lingkup tertentu seperti sebuah Institut atau sebuah organisasi.
2. Pembuatan sertifikat hanya bisa dilakukan apabila pemilik tanda tangan yang di inginkan terdaftar di dalam aplikasi pembuatan sertifikat ini.
3. System Autentikasi bisa dilakukan apabila nomor WhatsApp yang akan inginkan tanda tangannya terdaftar pada aplikasi pembuatan sertifikat digital ini.
4. Keamanan pada sertifikat digital ini hanya sebatas menyembunyikan pesan rahasia di setiap sertifikat agar ada bukti keabsahan setiap sertifikat menggunakan *steganografi* sebagai keamanan dengan metode yang digunakan adalah metode LSB.
5. Ukuran keluaran sertifikat yang digunakan 768 x 543 *pixel*
6. File pengeluaran sertifikat menggungunakan image

F. Sistematika Penulisan

Adapun sistematika penulisan yang digunakan dalam proposal penelitian yang dibuat saat ini sebagai berikut:

BAB I Pendahuluan

Adalah dimana akan menuliskan latar belakang dari penelitian yang akan diteliti, berlanjut dengan menuliskan rumusan masalah pada penelitian, selanjutnya menuliskan tujuan dari penelitian dan terakhir menyebutkan manfaat dari penelitiannya.

BAB II Tinjauan Pustaka

Adalah berisikan landasan teori dari apa yang diteliti oleh peneliti, teori-teori terkait yang digunakan oleh peneliti, dan menyebutkan kerangka pemikiran dari peneliti.

BAB III Metode Penelitian

Adalah mengenai metode penelitian secara jelas dan rinci. menggambarkan secara utuh, dari rancangan penelitian yang akan dilakukan peneliti yang dimulai dari menentukan tempat dan waktu penelitian, alat bahan yang digunakan peneliti, memperlihatkan rancangan sistem yang ingin dibuat peneliti, menunjukkan teknik pengujian pada sistem yang diteliti, dan memberitahukan bagaimana teknik analisis data yang digunakan peneliti.

Daftar Pustaka

Daftar pustaka digunakan untuk memperlihatkan sumber-sumber dari teori atau analisis yang peneliti gunakan yang bisa berupa buku, jurnal, ataupun dari website.

BAB II
TINJAUAN PUSTAKA

A. Landasan Teori

1. Autentikasi

Autentikasi adalah suatu proses yang menjadi tindakan atau pembuktian (validasi) terhadap identitas pengguna ketika ingin memasuki dan mengakses sistem penting tertentu. Proses dari pengambilan data digital yang berupa tanda tangan akan membuktikan bahwa user dapat melanjutkan penginputan data karena telah mendapatkan izin validasi.

2. Verifikasi

Verifikasi adalah proses menetapkan kebenaran, akurasi, atau validitas sesuatu. Verifikasi juga dapat diartikan sebagai persyaratan untuk memenuhi atau mengidentifikasi perbedaan hasil yang diharapkan dan fakta yang ditemukan. Sistem inilah yang akan mengetahui kebenaran dari apakan syarat verifikasi suatu sistem tertentu di lanjutkan bila kebenaran validasinya tercapai (H Kara, 2014).

Proses verifikasi ini biasanya diperlukan untuk mengukur akurasi dan kompatibilitas timbal balik. Misalnya, lembaga keuangan yang memeriksa detail pelanggan dan calon peminjam untuk memastikan bahwa informasi yang diberikan oleh pelanggan akurat.

3. *Steganografi*

a. Apa itu *steganografi*

Steganografi atau *Steganography* adalah ilmu, teknik, atau teknik yang menyembunyikan suatu pesan rahasia sehingga pesan tersebut hanya diketahui oleh pengirim dan penerima pesan rahasia tersebut. *Steganografi* berasal dari kata Yunani *steganografi*, yang berarti tersembunyi, dan grafik, yang berarti "menulis", jadi *steganografi* adalah menulis atau menyembunyikan pesan. *Steganografi* adalah kebalikan dari Kriptografi,

mengaburkan makna pesan rahasia, tetapi tidak menyembunyikan keberadaan pesan tersebut. Kelebihan *steganografi* dibandingkan kriptografi adalah pesan tidak disembunyikan meskipun sulit untuk didekripsi, namun berbeda dengan enkripsi yang menimbulkan kecurigaan terhadap pesan, pesan tersebut menarik, tidak menimbulkan kecurigaan.

b. Sejarah *steganografi*

Steganografi telah digunakan sejak sekitar 2.500 tahun yang lalu untuk kepentingan politik, militer dan diplomatik. Catatan pertama tentang *steganografi* ditulis oleh Herodotus, yaitu seorang sejarawan Yunani. Herodatus mengirim pesan rahasia dengan menggunakan kepala budak atau prajurit sebagai media. Caranya dengan menuliskan pesan di atas kepala budak yang telah dibotaki, ketika rambut budak telah tumbuh, budak tersebut diutus untuk membawa pesan rahasia di balik rambutnya.

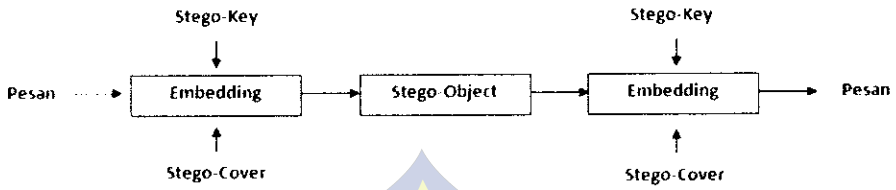
Sementara itu penggunaan *Steganografi* oleh bangsa Romawi dilakukan dengan menggunakan tinta tak-tampak (*invisible ink*) untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampak. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Di era modern, teknik *steganografi* menjadi populer setelah kasus pemboman gedung WTC pada 11 September 2001 di Amerika Serikat. Pada saat itu, teroris menyembunyikan pesan-pesan kegiatan terornya dalam berbagai media yang dapat dijadikan penampung untuk menyembunyikan file seperti pada image, audio dan video. Pada peristiwa tersebut disebutkan bahwa para teroris menyembunyikan peta-peta dan foto-foto target dan juga perintah untuk aktivitas teroris di ruang chat sport, bulletin boards porno dan website lainnya (Stefan Katzenbeisser and Fabien A. P. Petitcolas, n.d.).

c. Prinsip kerja *steganografi*

Prinsip kerja *steganografi* pesan rahasia yang tersembunyi diletakkan pada media wadah seperti gambar, audio dan video, dan tidak diragukan lagi

bahwa mereka menyimpan pesan rahasia. Pesan rahasia tersebut memerlukan kunci rahasia yang disebut *stego key*, sehingga hanya pihak yang berwenang yang dapat membuka dan mengekstrak pesan rahasia tersebut.



Gambar 1. Konsep penggunaan *steganografi*(Muchlisin Riadi, 2017)

4. *Least significant Bit* (LSB)

a. Apa itu *Least significant Bit* (LSB)

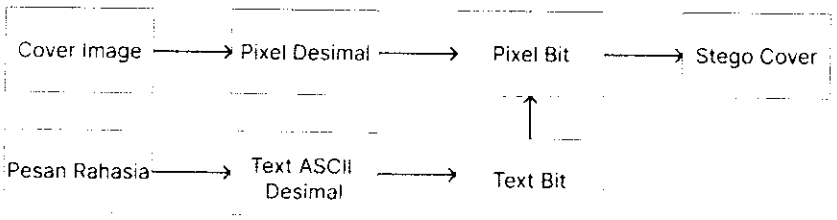
Least significant bit (LSB) adalah teknik yang umum digunakan untuk mengenkripsi dan mendekripsi informasi sensitif. Skema LSB bekerja dengan mengubah *bit* redundant dari gambar sampul yang tidak secara signifikan mempengaruhi *bit* dari pesan rahasia (Abba Suganda Girsang, 2017).

Least significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan *bit* .

Contohnya adalah bilangan biner dari 255 adalah 11111111, dari barisan angka 1 di atas, angka 1 paling kanan bernilai 1, dan itu adalah yang paling kecil. Bagian tersebut disebut dengan *least significant bit* (*bit* yang paling tidak berarti). *Least significant bit* sering kali digunakan untuk kepentingan penyisipan data ke dalam suatu media digital lain (Rajab, 2017).

b. Konsep *Least significant Bit (LSB)*

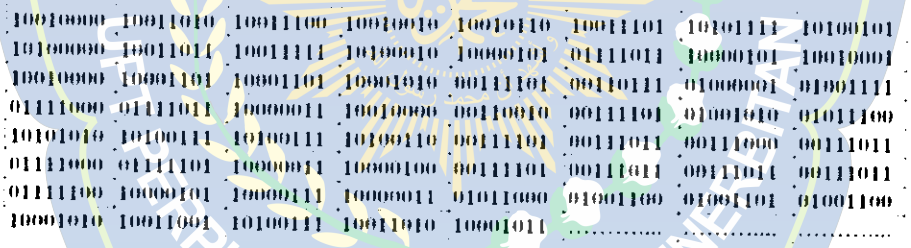
Berikut contoh konsep cara kerja dari metode *Least significant bit* . Ubah gambar menjadi nilai *pixel* desimal dan *pixel* desimal setiap *pixel* ini yang akan disisipi pesan rahasia didalamnya.



Gambar 2. Konsep penggunaan *least significant bit*

Seperti contoh pada Gambar 2. Diatas yaitu konsep penggunaan dari *least significant bit* , maka berikut adalah contoh sederhana implementasi dari konsep *least significant bit* dalam penyisipan pesan rahasia pada wadah gambar.

Gambar 3. Sebuah gambar yang diubah dalam bentuk *pixel*



Gambar 4. *Pixel* yang di ubah dalam bentuk *bit*

Selnjutnya pada contoh gambar di atas akan dimasukkan pesan rahasia, sebagai contoh pesan rahasia yang akan dimasukkan adalah "A" dan pesan tersebut di ubah menjadi dalam bentuk ASCII dan "A" = 65 dan nilai tersebut akan diubah menjadi *bit* yaitu 65 = 1000001 dan sebagai contoh akan di masukkan pada 8 *bit* pertama.

10010000	10011010	10011100	10010010	10010110	10011101	10101111	10100101

Gambar 5. Pilihan 8 *bit* pertama yang akan dimasukkan pesan rahasia

Sebelum disisipkan	Sesudah disisipkan
10010000	10010001
10011010	10011010
10011100	10011100
10010010	10010010
10010110	10010110
10011101	10011100
10101111	10101110
10100101	10100101

Gambar 6. Hasil penyisipan pesan rahasia kedalam *bit* image

5. *Recommended Process* Model

Recommended Process model adalah sebuah kumpulan, tindakan, dan tugas yang harus dijalankan berdasarkan proses langkah kerja dalam sistem pengembangan ini sesuatu yang dikerjakan tidak harus lengkap dalam menyiapkan sesuatu sebelum memulai mengerjakan sebuah produk, tetapi hanya perlu diketahui dari mana memulai memulai proses tersebut.

Sistem pengembangan ini dipilih karena dalam pengembangan perangkat lunak dapat dengan mudah terjadi kekacauan tanpa ada kendali proses pengerjaan yang ditentukan. Dalam proses pengerjaan pada sistem pengembangan ini harus disesuaikan untuk memenuhi kebutuhan sebuah produk yang sedang dibangun. Berdasarkan pernyataan tentang pengembangan sistem dari Recommended process model menyatakan dalam proses seharusnya hanya mencangkup aktivitas, kontrol, dan produk kerja yang sesuai produk yang akan diproduksi (Pressman S & Bruce R, 2006).

B. Penelitian Terkait (*State of the Art*)

Dalam penulisan ini peneliti mencoba menggali beberapa informasi dari penelitian-penelitian sebelumnya sebagai bahan perbandingan, baik dari kekurangan maupun kelebihan yang sudah ada. Adapun beberapa penelitian terdahulu yang relevan untuk digunakan sebagai pembanding dan penelitian tersebut sebagai berikut.

Penelitian pertama yang dilakukan oleh Egi Cahyo Prabowo, dan Irawan Afrianto. Mahasiswa Universitas Komputer Indonesia, Bandung tahun ajaran 2017 dengan judul "Penerapan *Digital Signature* dan *Kriptografi* pada *Otentikasi* Sertifikat Tanah Digital". Berdasarkan hasil dan pengujian yang telah dilakukan maka dapat diperoleh kesimpulan yaitu Penerapan mekanisme pembuatan dokumen digital dalam sistem dapat memberikan layanan alternatif untuk menerbit kan dokumen digital, Penerapan mekanisme keamanan *digital signature* dapat memberikan layanan keamanan berupa otentikasi dokumen yang diterapkan pada dokumen digital pemohon oleh kepala kantor sehingga pemohon dapat mengetahui validitas dokumen yang diterima (Cahyo Prabowo & Afrianto, 2017).

Penelitian kedua yang dilakukan oleh Muhammad Maulana Assyahid, Rihartanto, dan Didi Susilo Budi Utomo. Mahasiswa Universitas Politeknik Samarinda, Samarinda tahun ajaran 2018 dengan judul "Implementasi *Steganografi* Pesan Text ke dalam Audio dengan Metode *Spread Spectrum*". Berdasarkan percobaan yang telah dilakukan maka dapat disimpulkan adalah Proses penyisipan pesan menggunakan metode *Spread Spectrum* menjadikan pesan yang disisipkan menjadi lebar dan acak, Untuk bisa mengekstraksi pesan hasil penyisipan, maka kata kunci yang digunakan untuk membangkitkan bilangan Pseudorandom untuk proses ekstraksi harus sama seperti kata kunci yang digunakan untuk membangkitkan bilangan Pseudorandom di proses penyisipan, Hasil pengujian performansi MSE dan PSNR menunjukkan bahwa dengan data audio yang memiliki durasi 2 detik dan 3 pesan yang memiliki jumlah karakter yang berbeda, dengan pengujian sebanyak 3 kali diperoleh nilai rata-rata *Mean Squared Error* (MSE) sebesar 2,2692e-06 dengan nilai rata-rata *Peak Signal to-Noise Ratio* (PSNR) sebesar 111,9842 dB (Assyahid et al., 2018).

Penelitian ketiga yang dilakukan oleh I Wayan Ardiyasa. Mahasiswa Universitas STIKOM Bali, Denpasar Bali tahun ajaran 2018 dengan judul "Implementasi Teknik Data Hiding Untuk Pengamanan Pesan Rahasia Pada

Media Digital". Berdasarkan kesimpulan dari penelitian ini dapat disimpulkan bahwa Telah dihasilkan aplikasi teknik data hiding untuk membantu pengamanan pesan rahasia dengan menggunakan *kriptografi Triple Des* dan *steganography* LSB (*Least significant Bit*) menggunakan menggunakan visual studio C#. Dari hasil pengujian dengan metode Blackbox testing proses enkripsi dan stego file serta dekripsi ciphertext berjalan sesuai dengan yang diharapkan. setelah melakukan uji file dengan menggunakan HxD didapatkan pattern pada file berubah serta size file bertambah besar (Ardiyasa, 2018).

Penelitian keempat yang dilakukan oleh Erick Febriyanto, Untung Rahardja, Adam Faturahman, dan Ninda Lutfiani. Mahasiswa universitas STIMIK Raharja tahun ajaran 2018 dengan judul "Sistem Verifikasi Sertifikat Menggunakan Qrcode Pada Central Event Information". Berdasarkan hasil penelitian yang dilakukan dapat disimpulkan bahwa Dalam penerapan Qrcode sebagai sistem verifikasi sertifikat pada sistem CEI (*Central Event Information*) ini terdapat 2 (dua) uraian permasalahan dan dapat diselesaikan dengan menggunakan 3 (tiga) tahap, menghasilkan 2 (dua) kesimpulan yaitu: 1. Aplikasi Qrcode sebagai sistem verifikasi sertifikat pada sistem CEI (*Central Event Information*) merupakan media yang dapat digunakan untuk verifikasi keaslian sertifikat secara online. Terbukti dari hasil kuesioner 40 responden dengan hasil rata-rata Skor SUS 83,33 yang menunjukkan sistem CEI dapat diterima oleh pengguna, 2. Dengan adanya Qrcode tersebut mampu meningkatkan unsur keamanan sertifikat guna menghindari terjadinya manipulasi atau penggandaan sertifikat secara resmi yang diter*bit* kan oleh CEI (*Central Event Information*). Dimana sertifikat tersebut bisa dicek dengan mudah dimana saja dan kapan saja (Erick Febriyanto et al., 2018).

Penelitian kelima yang dilakukan oleh Niria Laila dan Anita Sindar RMS. Mahasiswa Universitas STIMIK Pelita Nusantara, Medan tahun ajaran 2019 dengan judul "Implementasi *Steganografi* LSB Dengan *Enkripsi Vigenere Cipher* Pada Citra". Berdasarkan hasil penelitian yang dilakukan dapat

disimpulkan bahwa Proses penyandian dan penyisipan pesan dengan metode *Vigenere Cipher* dan LSB yaitu langkah awal input file teks dan kata kunci, seterusnya file teks dan kata kunci diubah kedalam bilangan desimal, seterusnya diproses sesuai dengan rumus Vigenere Cipher diharapkan data yang dikirim tidak mudah dibaca oleh pihak ketiga. Algoritma *Vigenere Cipher* dan teknik LSB (*Last Significant Bit*) dapat dijadikan sebagai solusi untuk keamanan pesan rahasia yang disisipkan ke dalam image, dan dapat diungkap kembali sama persis dengan bentuk asli dan tidak mengalami kerusakan sedikitpun. Merancang aplikasi pengamanan data dengan metode *Vigenere Cipher* dan LSB yaitu dengan langkah awal merancang form penyisipan dan ekstraksi, setelah itu merancang form untuk menampilkan hasil penyisipan dan form untuk menampilkan hasil ekstraksi.(Laila & Sinaga, 2019).

Penelitian keenam yang dilakukan oleh Aliy Hafiz. Mahasiswa AMIK Dian Cipta Cendikia, Bandar Lampung tahun ajaran 2019 dengan judul "*Steganografi* Berbasis Citra Digital untuk Menyembunyikan Data Menggunakan Metode *Least significant Bit* (LSB)". Penyisipan pesan tersembunyi berupa data dapat dilakukan ke dalam wadah citra digital berformat JPEG dan format citra digital lainnya, kemudian dapat mengekstraksi kembali data tersembunyi tersebut dari dalam citra digital. Terjadi perubahan pada ukuran citra digital namun secara kasat mata perbedaan antara gambar sebelum dan sesudah disisipkan pesan tidak terlihat. Selain itu waktu yang dibutuhkan untuk proses enkripsi dan dekripsi dipengaruhi oleh kecepatan komputer yang digunakan dan ukuran citra (Hafis, 2019).

Table 1. Daftar penelitian terkait

No	Judul Penelitian	Nama Peneliti	Metode Penelitian	Hasil
1	Penerapan *Digital Signature* dan *Kriptografi* pada *Otentikasi* Sertifikat Tanah	Egi Cahyo Prabowo, dan Irawan Afrianto	Digital *signature* dengan fungsi algoritma *hash* dan *kriptografi*	Penerapan mekanisme keamanan digital signature dapat memberikan

	Digital 2017		pada *otentikasi*	keamanan berupa otentikasi document.
2	Implementasi *Steganografi* Pesan Text ke dalam Audio dengan Metode *Spread Spectrum* 2018	Muhammad Maulana Assyahid, Rihartanto, dan Didi Susilo Budi Utomo	Teknik *steganografi* metode *spread spectrum*	Data audio yang memiliki durasi 2 detik dan 3 pesan yang memiliki jumlah karakter yang berbeda, dengan pengujian sebanyak 3 kali.
3	Implementasi Teknik Data Hiding Untuk Pengamanan Pesan Rahasia Pada Media Digital 2018	I Wayan Ardiyasa	Teknik data *hidding*, *steganografi* metode *least significant bit* dan *kriptografi* algoritma *triple DES*	Dapat menghasilkan aplikasi teknik data hiding untuk membantu pengamanan pesan rahasia
4	Sistem Verifikasi Sertifikat Menggunakan Qrcode Pada Central Event Information 2018	Erick Febriyanto, Untung Rahardja, Adam Faturahman, dan Ninda Lutfiani	Verifikasi Qrcode sertifikat	Penerapan Qrcode sebagai sistem verifikasi dapat digunakan untuk verifikasi keaslian sertifikat secara online
5	Implementasi *Steganografi* LSB Dengan *Enkripsi Vigenere Cipher* Pada Citra 2019	Niria Laila dan Anita Sindar RMS	*Steganografi* metode *least significant bit* dan *enkripsi vigenere cipher*	Merancang aplikasi pengamanan data dengan metode Vigenere Cipher dan LSB
6	*Steganografi* Berbasis Citra Digital untuk Menyembunyikan Data Menggunakan Metode *Least significant Bit* (LSB) 2019	Aliy Hafiz	*Steganografi* basis citra metode *least significant bit* (LSB)	Penyisipan pesan tersembunyi dapat merubah ukuran citra digital namun secara kasat mata perbedaan gambar tidak terlihat

C. Kerangka Pikir

Dalam melaksanakan sebuah acara ataupun event apapun itu sudah pasti membutuhkan yang namanya sertifikat karena sertifikat ini digunakan sebagai sebuah bukti bahwa kita mengikuti acara tersebut dan dalam pembuatan sertifikat inilah yang menjadi masalah karena banyak yang harus dilakukan seperti harus bertemu secara langsung kepada seseorang yang ingin kita minta tanda tangannya dan itu sangat menyusahkan dan ditambah lagi sertifikat seperti ini masih dikatakan masih bisa di duplikat oleh pihak ketiga.

Oleh karena itu dibutuhkan sebuah cara bagaimana membuat agar pembuatan sertifikat ini dapat dilakukan dengan mudah tanpa harus bertemu oleh pihak yang bersangkutan, maka dengan ini dilakukanlah sebuah penelitian dalam bentuk bagan kerangka pikir untuk menyelesaikan permasalahan tersebut.

Gambar 7. Konsep kerangka pemikiran

BAB III
METODE PENELITIAN

A. Tempat dan Waktu Penelitian

Penelitian ini akan dilaksanakan yang lebih tepatnya yaitu kampus Universitas Muhammadiyah Makassar bagian administrasi mahasiswa yang berlokasi di jalan Jl. Sultan Alauddin No.259, Gn. Sari, Kec. Rappocini, Kota Makassar, Sulawesi Selatan 90221.

Peneliti memilih lokasi di kampus Universitas Muhammadiyah Makassar, karena berdasarkan pengamatan peneliti yang dilakukan bahwa dalam pembuatan sertifikat mahasiswa biasanya hanya mengandalkan aplikasi yang sudah ada di internet tanpa mengetahui keamanan yang dimilikinya dan sulit membuktikan keabsahannya. Juga bila ingin membuat sertifikat masih harus meminta langsung tanda tangan seseorang menjadi penyelenggara. Dan ada juga mahasiswa masih menggunakan word untuk membuat sertifikatnya tanpa ada keamanan di dalamnya atau dapat diduplikasi.

B. Alat dan Bahan

Alat dan bahan yang diperlukan dalam melakukan penelitian ini agar penelitian dapat dilakukan dengan lancar terdapat dua kategori dalam keperluan alat dan bahan yaitu keperluan perangkat keras, dan perangkat lunak sebagai berikut:

1. Kebutuhan Implementasi

a. Perangkat keras

- Komputer PC / Laptop
- Processor AMD A8-7410 APU with AMD Radeon R5 Graphics 2.20 GHz
- RAM 4 GB
- Perangkat *mouse* dan *keyboard* standar

b. Perangkat lunak

- Sistem operasi windows 10
- Javascript sebagai bahasa *web-programming*
- Postgresql *database*
- Web Browser Mozilla Firefox, Chrome
- *Text editor* Visual Studio Code
- PDF Dokumen

2. Kebutuhan pengguna

a. Perangkat keras

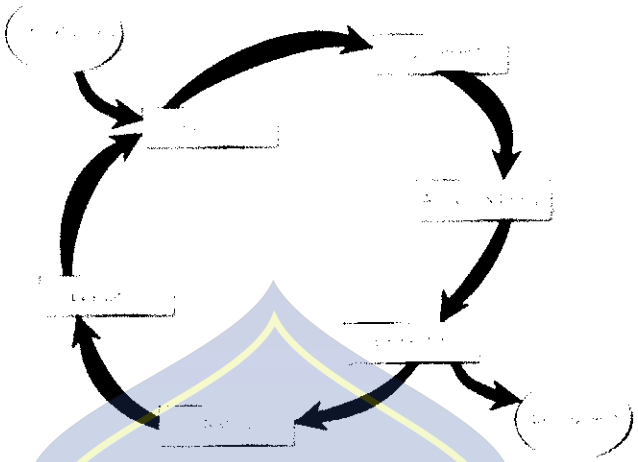
- Komputer PC / Laptop
- Processor Intel Pentium 4 atau yang lebih baru
- RAM 4 GB
- Perangkat *mouse* dan *keyboard* standar

b. Perangkat lunak minimal

- Sistem operasi linux, windows 7, windows 8, windows 8.1 dan windows 10
- Web Browser Mozilla Firefox versi 52, Chrome versi 52, Opera versi 42, Safari versi 10.1, Edge versi 14
- PDF Dokumen

C. Perancangan Sistem

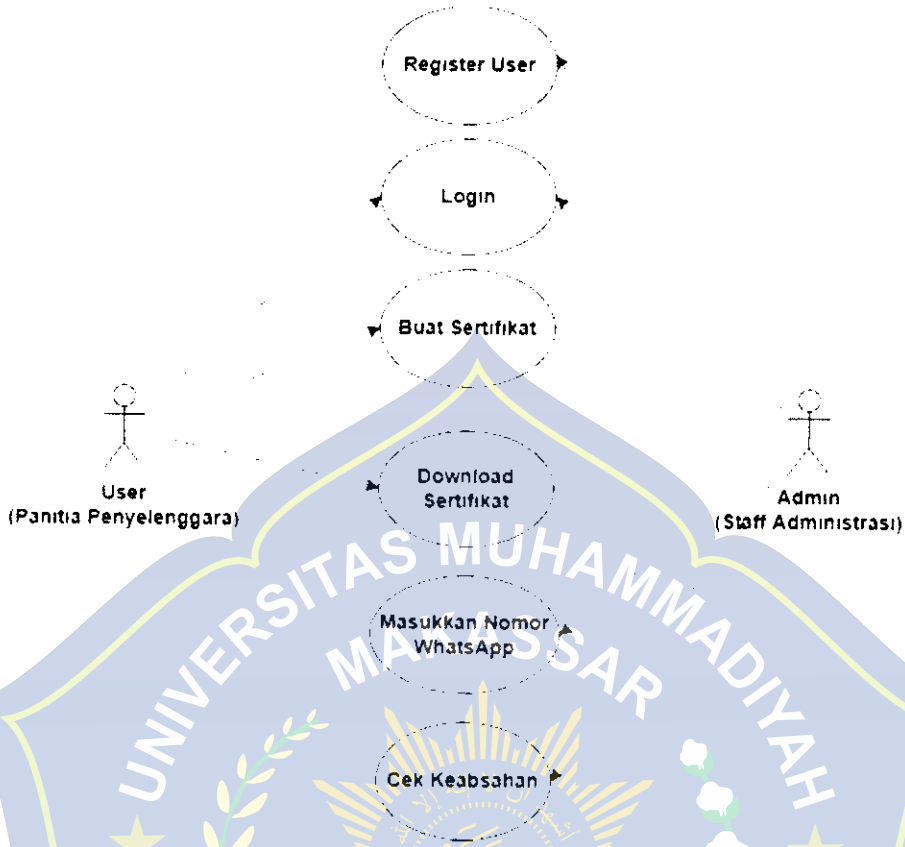
Perancangan yang akan dilakukan pada sistem yang akan diteliti ini dalam pengembangannya akan menggunakan sebuah jenis perancangan sistem pengembangan yang disebut *Recommended Process Model* yang dimana akan melakukan penembangan sistem perangkat perangkat lunak yang terkendali dalam pengerjaan proses pengembangan yang dilakukan dengan mengikuti proses pengembangan yang telah ditentukan.



Gambar 8. Alur pengembangan perangkat lunak(Pressman S and Bruce R, 2006)

Dalam perancangan sistem ini peneliti akan menjelaskan prosedur atau langkah kerja sistem yang akan di uji dengan menguraikan sebuah pemodelan sistem menggunakan *use case* untuk mendeskripsikan interaksi antara actor dan sistem, membuat *activity* diagram sistem autentikasi dan proses dalam memberikan keamanan sertifikat agar dapat menjaga keabsahan sertifikat digital dan pengecekan yang akan dilakukan untuk membuktikan keabsahan sertifikat digital tersebut.

Pada awal perancangan ini akan memperlihatkan sebuah sistem yang akan dilakukan oleh pengguna dan admin dalam aplikasi pembuatan sertifikat digital dalam bentuk use case dibawah ini.



Gambar 9. *Use case* interaksi antara sistem dan actor

Pada gambr diatas mempertihatkan bagaimana interaksi para aktor kepada sistem seperti apa yang dilakukan oleh *user* di sistemnya dan apa yang bisa dilakukan oleh admin terhadap sistem.

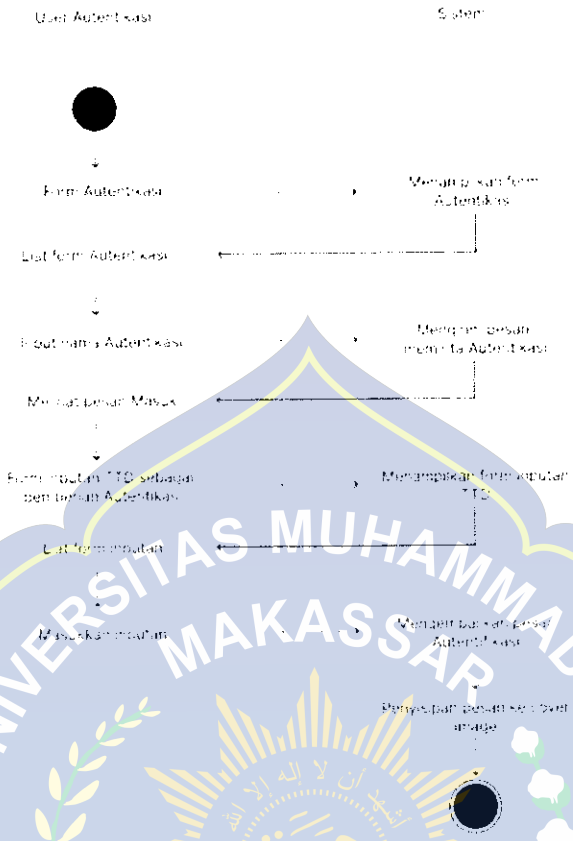
Table 2. Keterangan sistem yang pada user

User (Panitia Penyelenggara)	
sistem	Keterangan
Login	Login menggukana akun yang telah didiberikan oleh admin agar bisa mengakses alikasi sertifikat digital
Buat Sertifikat	Melakukan pembuatan sertifikat digital
List Sertifikat	Melihat hasil jadi sertifikat digital yang dibuat
Download Sertifikat	Dapat mendownload sertifikat digital yang dibuat

Table 3. Keterangan sistem yang ada pada admin

Admin (Staff Administrasi)	
sistem	keterangan
Register user	Membuatkan akun agar user bisa login ke dalam aplikasi pembuatan sertifikat
Login	Login menggunakan akun yang sudah tersedia untuk mengolah aplikasi
Masukkan Nomor WhatsApp	Melakukan Input nomor whatsapp yang akan di gunakan oleh user untuk melakukan permintaan Autentikasi
Cek Keabsahan	Dapat melakukan pengecekan sertifikat digital untuk mengetahui keabsahannya saat pengurusan berkas

Pada dua table diatas adalah penjelasan pengenai use case yang di buat yang terdiri dari table keterangan untuk kegiatan user dan kegiatan untuk admin.



Gambar 10. *Activity* diagram dalam proses autentikasi

Pada gambar diatas diperlihatkan bagaimana cara kerja dalam melakukan autentikasi sertifikat yang dimana pada website sebelum melanjutkan penginputan data sertifikat pengguna haru melakukan autentikasi agar bisa mendapatkan tanda tangan pihak penyelenggara untuk dimasukkan tanda tangannya didalam sertifikat dengan memilih nama penyelenggara itu dan pesan permintaan verifikasi ke nomor *whatsapp* nya dan pada pesan itu terdapat sebuah *link* agar dapat dialihkan ke sebuah halaman untuk memasukkan tanda tangan digital agar dapat digunakan oleh si pembuat sertifikat dan tanda tangan dan data-data yang akan dimasukkan di sertifikat dapat tersimpan di *database*. Untuk mengetahui lebih jelas proses yang akan dilakukan untuk melakukan autentikasi agar mendapatkan tanda tangan digital.

Berdasarka gambar diatas pada saat melakukan permintaan autentikasi untuk mendapatkan tanda tangan digital dapat dijelaskan sebagai berikut.

1. Masuk kehalaman penginputa nomor tujuan autentikasi
2. Melakukan input nomor whatsapp tujuan
3. Pesan didapatkan oleh penerima pesan
4. Masuk kelink yang tercantum di dalam pesan
5. Penginputan tanda tangan digital dilakukan

Gambar 11. *Activity* diagram proses pemasangan keamanan sertifikat

Pada gambar diatas dapat dilihat bagaimana cara atau alur aktivitas dari pembuatan sistem keamanan setiap sertifikat dimulai dari membuat *cover image* yang di ubah ke dalam bentuk *pixel* decimal dan berubah menjadi bentuk *bit* , dan dilanjutkan dengan memasukkan pesan rahasianya dan juga diubah menjadi *bit* nilai dari ASCII setiap huruf dan akhirnya melakukan penyisipan pesan

tersembunyinya di setiap akhir *bit cover image* dan akhirnya *stego image* sertifikat digital telah terbuat.

Berdasarka gambar diatas pada saat melakukan pemasangan keamanan pada sertifikat digital yang telah dibuat dan dapat dijelaskan sebagai berikut.

1. Preview sertifikat digital yang telah dibuat
2. Klik add security
3. Proses peasangan keamanan
4. Tampilan sertifikat digital ditampilkan setelah keamanan dipasangkan

Gambar 12. *Activity* diagram proses admin pengambilan pesan rahasia

Pada gambar diatas dijelaskan cara mengambil pesan rahasia yang terdapat pada *cover image* yang dimulai dari menginput *cover image* yang ingin dilihat pesan rahasianya selanjutnya sistem akan memproses *cover image* tersebut untuk menampilkan pesan rahasianya apakah sama dengan isi tampilan yang ada.

Berdasarka gambar diatas pada saat melakukan proses pengecekan pada sertifikat digital yang telah dibuat dan dapat dijelaskan sebagai berikut.

1. Penginputan sertifikat digital
2. Proses pengecekan dilakukan
3. Pesan tersebunyi ditapilkan

D. Teknik Pengujian Sistem

Pada penelitian yang dilakukan oleh peneliti untuk menguji sistem yang dibuat yaitu akan menggunakan teknik *black box testing*. *Black box testing* atau dapat disebut juga *Behavioral testing* adalah pengujian yang dilakukan untuk mengamati hasil input dan output dari perangkat lunak tanpa mengetahui struktur kode dari perangkat lunak. Pengujian ini dilakukan di akhir pembuatan perangkat lunak untuk mengetahui apakah perangkat lunak dapat berfungsi dengan baik (Rony Setiawan, 2021).

Menurut Imperva, ada tiga tipe pengujian *black box* yang bisa kamu lakukan pada sistem aplikasi yang dibuat, yaitu *Functional testing, Non-functional testing, Regresion testing* (Rahmalia, 2021), pada penelitian ini akan menggunakan *functional testing*.

Functional testing adalah proses pengujian terhadap fungsi atau fitur spesifik sebuah *software*. Contoh dari pengujian ini adalah untuk mengecek apakah pengguna *software* mampu melakukan *login* dengan lancar menggunakan *password*, *email*, dan *username*-nya masing-masing.

Pengujian ini dapat dilakukan untuk memastikan bahwa pengguna benar-benar tidak bisa masuk tanpa informasi tersebut untuk menjaga keamanan program. Biasanya, *functional testing* berfokus pada pengujian aspek-aspek paling penting dari sebuah software dan integrasi antara komponen-komponen utamanya. Akan tetapi, *functional testing* pun dapat dilakukan untuk menguji sistemnya secara keseluruhan.

Contoh aspek fungsional yang diuji pada kasus ini adalah fitur yang tidak lagi bekerja dengan baik pada versi terbaru. Sementara itu, aspek non fungsional

yang diuji contohnya adalah performa yang melambat di versi *software* yang baru.

Pada *black box* testing juga sudah pasti memiliki keuntungan dan kekurangngannya, Ketika *behavioral testing* digunakan dalam pengujian perangkat lunak, ada beberapa keuntungan yang dapat diperoleh dari pengujian tersebut. Berikut ini adalah keuntungannya (Rony Setiawan, 2021):

- Penguji tidak harus memiliki pengetahuan tentang suatu bahasa pemrograman.
- Pengujian dilakukan berdasarkan sudut pandang pengguna. Hal tersebut dilakukan agar dapat menemukan *inkonsistensi* dalam perangkat lunak.
- Pengembang dan penguji memiliki ketergantungan satu dengan yang lainnya.
- Penguji tidak perlu memeriksa kode.
- Memungkinkan pengguna dan pengembang bekerja secara *independen* tanpa mengganggu proses kerja satu sama lain.

Selain memiliki keuntungan, *behavioral testing* juga memiliki kekurangan. Berikut ini adalah beberapa kekurangannya:

- Memiliki kemungkinan kesalahan tidak terdeteksi karena kurang teliti dan tidak adanya pengetahuan teknis.
- Ada bagian *back-end* yang tidak diuji sama sekali.
- Kemungkinan pengujian dilakukan kembali oleh programmer.

E. Teknik Analisis Data

Dalam penelitian ini data dapat diperoleh dari berbagai sumber dengan menggunakan pengumpulan data yang bermacam-macam sampai mencapai titik maksimal yang sering dinamakan dengan titik jenuh. Menurut sugiyono terdapat tiga model interaktif dalam analisis data, yaitu reduksi data, penyajian data, serta penarikan kesimpulan (Sugiyono, 2019).

1. Pengumpulan Data

Instrumen pengumpulan data merupakan suatu alat yang digunakan dalam penelitian untuk mengumpulkan data dan supaya pengumpulan tersebut sistematis dan mudah. Instrumen penelitian merupakan sesuatu yang sangat

penting dan strategi kedudukannya dalam keseluruhan kegiatan penelitian. Dengan instrumen, akan diperoleh data yang merupakan bahan penting untuk menjawab permasalahan, mencari sesuatu yang akan digunakan untuk mencapai tujuan dan membuktikan hipotesis. Data yang dikumpulkan ditentukan oleh variabel-variabel yang ada dalam hipotesis.

2. Reduksi Data

Reduksi data termasuk dalam kategori pekerjaan analisis data. Data yang berupa catatan lapangan (*field notes*) jumlahnya cukup banyak, untuk itu maka perlu dicatat secara teliti dan rinci. Mereduksi data berarti merangkum, memilih hal-hal yang penting, dicari tema polanya. Dengan demikian data yang telah direduksi akan memberikan gambaran yang lebih jelas, dan mempermudah peneliti untuk melakukan pengumpulan data selanjutnya, dan mencarinya bila diperlukan.

Dalam mereduksi data, setiap peneliti akan dipandu oleh tujuan yang akan dicapai. Tujuan utama dari penelitian kualitatif adalah pada temuan. Oleh karena itu, apabila peneliti dalam melakukan penelitian menemukan segala sesuatu yang dipandang asing, tidak dikenal, belum memiliki pola, justru hal tersebut yang harus dijadikan perhatian peneliti dalam melakukan reduksi data. Reduksi data merupakan proses berfikir sensitif yang memerlukan kecerdasan dan kedalaman wawasan yang tinggi.

3. *Display* Data

Hasil reduksi tersebut akan di *display* dengan cara tertentu untuk masing-masing pola, kategori, fokus, tema yang hendak dipahami dan dimengerti persoalannya. Penggunaan *display* data dapat membantu peneliti untuk dapat melihat gambaran keseluruhan atau bagian-bagian tertentu dari hasil penelitian. Dalam penelitian kualitatif, penyajian data bisa dilakukan dalam bentuk uraian singkat, bagan, hubungan antar kategori, *flowchart*, dan sejenisnya. Teks naratif merupakan jenis yang sering digunakan untuk menyajikan data dalam penelitian kualitatif.

4. Penarikan Kesimpulan

Langkah ketiga dalam analisis data kualitatif menurut Miles dan Huberman adalah penarikan kesimpulan dan verifikasi. Kesimpulan awal yang dikemukakan masih bersifat sementara, dan akan berubah bila tidak ditemukan bukti-bukti yang mendukung pada tahap pengumpulan data berikutnya. Dengan demikian, kesimpulan dalam penelitian kualitatif mungkin dapat menjawab rumusan masalah yang dirumuskan sejak awal, tetapi mungkin juga tidak, karena seperti telah dikemukakan bahwa masalah dan rumusan masalah dalam penelitian kualitatif masih bersifat sementara dan akan berkembang setelah penelitian berada di lapangan.

BAB IV
HASIL DAN PEMBAHASAN

Pada bab ini akan menyajikan sebuah pembahasan tentang hasil penelitian yang berupa hasil pengujian pada penelitian yang digunakan. Hasil dari pengujian pada penelitian ini adalah inti dari skripsi karena pada bagian ini akan menyajikan hasil-hasil pengujian sistem yang telah dilakukan pada penelitian ini. Pada setiap hasil pengujian yang dilakukan akan diberikan sebuah alasan penjelasan mengapa hasil yang diujikan bisa didapatkan bedasarkan teori hasil penelitian terdahulu dengan alasan yang teoritis. Hasil penelitian pada skripsi ini akan berupa sub-subbab yang merujuk pada rumusan masalah atau tujuan. Deskripsi pada penelitian ini berupa (a) autentikasi tanda tangan digital, (b) keamanan sertifikat digital, (c) pengecekan keabsahan setifiikat digital, maka pembahasan dapat dibagi menjadi tiga subbab, seperti berikut.

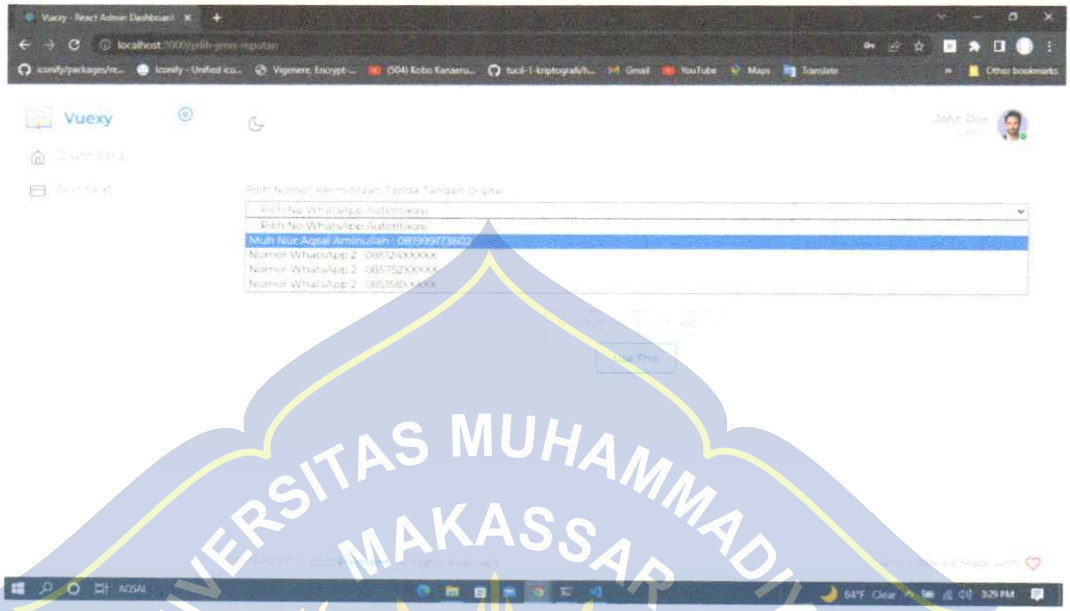
A. Autentikasi Tanda Tangan Digital

Pada tahapan ini akan menjelaskan mekanisme sistem yang dibuat yaitu sistem autentikasi. Sistem autentikasi ini dilakukan untuk mendapatkan tanda tangan digital sesorang dengan mengirimkan pesan pemberitahuan atau notifikasi ke nomor whatsappnya melalui website aplikasi pembuatan sertifikat digital, pesan yang dikirimkan akan berupa pesan seperti pesan whatsapp seperti pesan biasa dengan dilengkapi dengan sebuah link didalam pesan tersebut yang akan mengerahkan penerima pesan ke halaman website untuk melakukan penginputan tanda tangan digital.

1. Pengujian Implementasi Antar Muka Autentikasi Tanda Tangan Digital

Berikut adalaah tahapan-tahapan pengujian implementtasi antar muka yang akan di uji untuk melakukan autentikasi agar mendapatkan tanda tangan digital berdasarkan penelitian yang dilakukan. Untuk memulai awalnya akan diperlihatkan sebuah halaman untuk melakukan autentikasi dengan menginput

atau memilih nomor whatsapp yang tersedia di kolom inputan tersebut seperti dibawah ini.

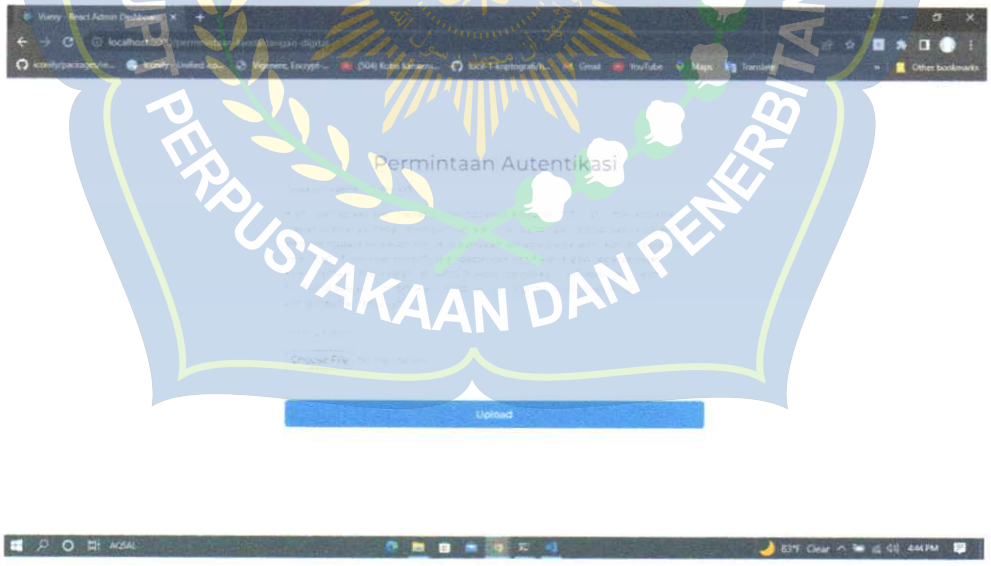


Gambar 13. Input nomor whatsapp tujuan

Pada gambar di atas menunjukkan langkah pemilihan nomor tujuan autentikasi untuk mendapatkan tanda tangan digital orang tersebut. Setelah memilih nomor tujuan selanjutnya mengirimkan pesan notifikasi kepada penerima dengan cara mengklik tombol "Use This" tetapi jangan lupa memasukkan juga jumlah sertifikat digital yang diinginkan.

Gambar 14. Pesan notifikasi yang diterima nomor tujuan

Seperti gambar diatas diperlihatkan bahwa proses pengiriman pesan sudah dapat dilakukan dan terdapat pesan permintaan autentikasi untuk mendapatkan tanda tangan digital.



Gambar 15. Halaman penginputan tanda tangan digital

Selanjutnya seperti yang terdapat pada pesan notifikasi tersebut terdapat sebuah link untuk mengarahkan kesebuah halaman untukmelakukan penginputan tanda tangan digital yang dibutuhkan.

2. Pengujian Sistem Autentikasi Tanda Tangan Digital

Berikut adalah hasil pengujian yang dilakukan pada sistem autentikasi untuk mendapatkan tanda tanga digital menggunakan pengujian black box.

Table 4. Pengujian black box testing autentikasi sertifikat digital

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian
1	Nomor whatsaap tujuan dan jumlah sertifikat diisi kemudian klik tombol Use This untuk mengirimkan pesan notification.	Nomor wahtsaap tujuan dan jumlah sertifiakat berhasil di input dan berhasil mengirimkan pesan notifikasi	berhasil
2	Nomor whatsapp tujuan berhasil menerima pasan notifikasi dan mendapatkan link untuk menginput tanda tangan digital.	Nomor whatsapp tujuan berhasil menerima pesan notifikasi dan sebuah link untuk menginput tanda tangan digital	berhasil
3	Menginput tanda tangan digital pada halaman inputan yang telah disediakan kemudian klik tombol upload	Tanda tangan digital berhasil di input	berhasil

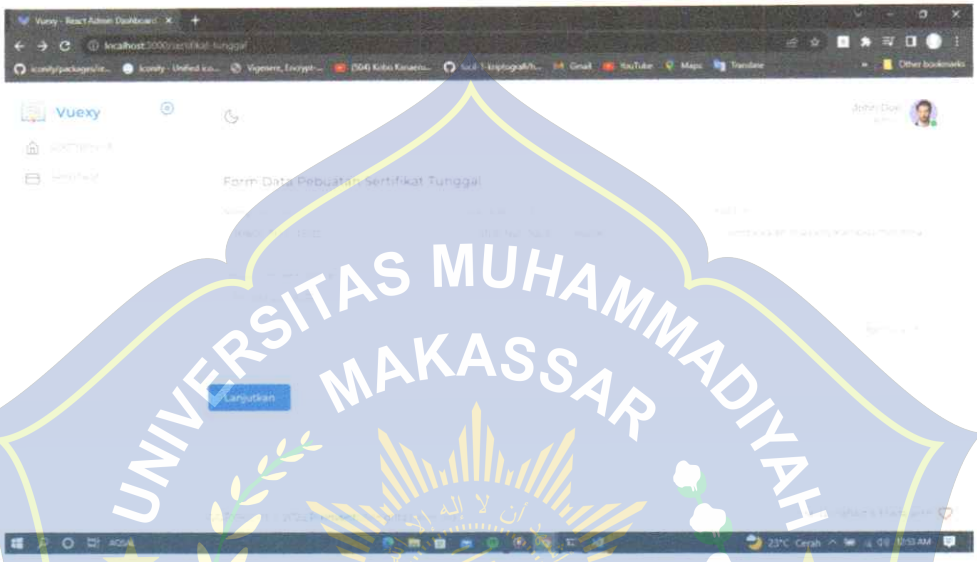
Pada table diatas adalah pengujian yang dilakukan pada sistem autentikasi menggunkanan pengujian black box.

B. Keamanan Sertifikat Digital

Selanjutnya berdasarkan hasil dan analias yang dilakukan pada sistem proses pemasangan keamanan pada sertifikat digital berhasil dilakukan dengan menggunakan algoritma *steganografi* dengan metode *least significant bit*.

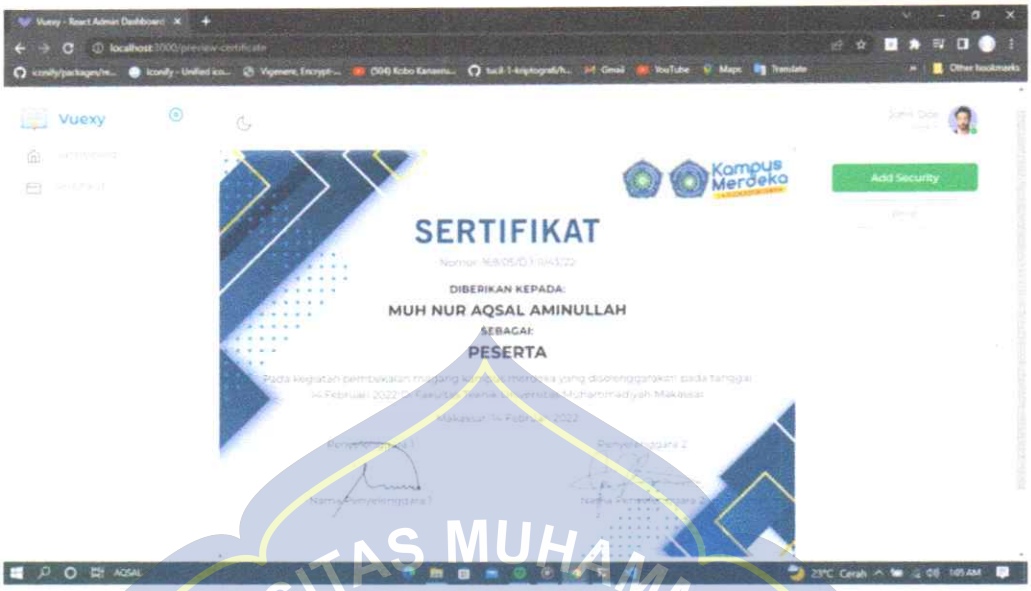
1. **Pengujian Implementasi Antar Muka Pemasangan Keamanan Sertifikat Digital**

Berikut tahapan visual yang dilakukan pada aplikasi pembuatan sertifikat digital saat melakukan proses pemasangan keamanan pada sertifikat digital yang akan di jelaskan dibawah ini.



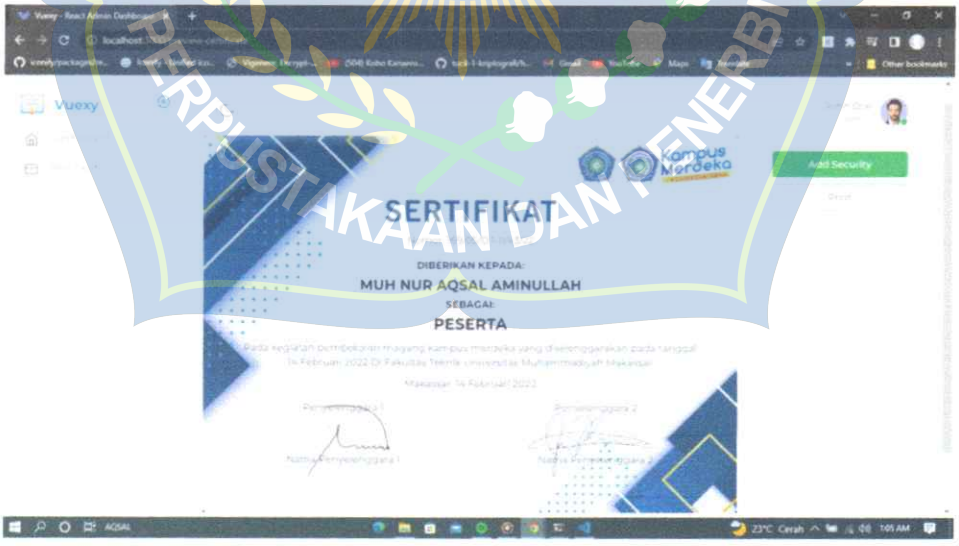
Gambar 16. Penginputan data sertifikat

Pada tahpan diatas adala tahapan yang akan dikakukan apabila telah melakukan autentikasi dan mendapatkan tanda tangan digital. Taapan diatas berupa penginputan data yang akan di tapilkan pada sertifikat yang akan dibuat, setelah menginput data yang diperlukan selanjutnya klik tombol "Lanjutkan" untuk melanjutkan pada tahapan selanjutnya yaitu akan memperlihatkan preview hasil sertifikat yang telah dibuat.



Gambar 17. Preview sertifikat digital

Pada gambar diatas adalah sebuah halaman preview yang menapilkan hasil sertifikat digital namun, preview yang ditapilkan masuk mebul bisa di save atau disimpan karena sertifikat tersebut masih belum selesai dan belum terpasang keamanan didalamnya, untuk melanjutkan pemasangan keamanan yaitu dengan mengklik tombol "Add Security" yang telah disediakan dan setelah itu tunggu proses pemasangannya.



Gambar 18. Sertifikat hasil pemasangan keamanan

Pada gambar diatas adalah hasil visual yang dibuat pada sertifikat yang dibuat yang telah dipasangkan keamanan dengan menggunkan algoritma *steganografi* dengan metode least signifincant *bit* . Pada hasil ini sesuai yang diharapkan dengan yang diingikan tanpa adanya perubahan yang terlalu terlihat seperti warnanya walaupun pesan rahasianya ditanamkan pada *pixel bit* pada gambar. Alasan dari keberhasilan pemasangan keamanan pada sertifikat tersebut dikarenakan pada metode yang hanya mengubah *bit* terakhir yang tidak akan mengubah *pixel* gambar secara drastis.

2. Pengujian Sistem Keamanan Sertifikat Digital

Berikut adalah hasil pengujian yang dilakukan pada sistem pemasangan keamanan sertifikat digital menggunakan pengujian black box.

Table 5. Pengujian black box testing keamanan sertifikat digital

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian
1	Penginputan data sertifikat kemudian klik tombol lanjutkan	Penginputan data sertifikat berhasil dilakukan.	berhasil
2	Menampilkan preview sertifikat kemudian klik add security untuk melakukan proses pemasangan keamanan pada sertifikat.	Preview sertifikat berhasil di tampilkan.	berhasil
3	Menampilkan sertifikat digital yang telah dipasangana keamanan didalamnya dan dapat di simpan atau di download.	Proses pemasangan keamanan pada sertifkat digital berhasil dilakukan dan menampilkan sertifiakt digitalnya dan berhasil di simpan .	berhasil

Pada table diatas adalah sebuah pengujian yang dilakukan pada sistem pemberian keamanan pada sertifikat menggunakan least significant bit dengan pengujian black box.

Pada penelitian ini telah dilakukan bebera kali pengujian untuk memasangkan keamanan pada sertifikat yang dibuat dengan berbagai ukuran *pixel* sertifikat dan berdasarkan analisis yang dilakukan maka didapatkan sebuah hasil sebagai berikut.

Table 6. Hasil analisis pengujian waktu eksekusi pemasangan keamanan berdasarkan ukuran *pixel* gambar

***Pixel* Gambar**	**Waktu**
768 x 543	44 – 71 ms
1024 x 768	63 – 86 ms
1360 x 768	79 – 127 ms
1752 x 1241	148 – 282 ms

Gambar 19. Diagram hasil pengujian waktu eksekusi

Selanjutnya pengujian yang dilakukan adalah pengujian terhadap min max ukuran dari gambar sertifikat digital. Berdasarkan analisis yang telah dilakukan dalam pemasangan keamanan pada sertifikat digital dengan berbagai ukuran gamba, maka didapatkan hasil eksekusi pemasangan keamanan pada sertifikat digital sebagai berikut.

Table 7. Hasil analisis pengujian waktu eksekusi pemasangan keamanan berdasarkan size gambar

Nama file	*Pixel* gambar sebelum disisipkan pesan tersembunyi	Ukuran gambar sebelum disisipi pesan tersembunyi	*Pixel* gambar setelah disisipkan pesan tersembunyi	Ukuran gambar setelah disisipi pesan tersembunyi	Waktu eksekusi
sertifikat1.jpg	768 x 543	237 kb	768 x 543	309 kb	42 – 51 ms
sertifikat2.jpg	768 x 543	212 kb	768 x 543	248 kb	42 – 54 ms
sertifikat3.jpg	768 x 543	391 kb	768 x 543	495 kb	42 – 73 ms
sertifikat4.jpg	768 x 543	390 kb	768 x 543	496 kb	43 – 75 ms
sertifikat5.jpg	768 x 543	207 kb	768 x 543	250 kb	33 – 49 ms

Table 8. Hasil analisis pengujian waktu eksekusi pemasangan keamanan berdasarkan pesan text

Nama file	Pixel gambar	Pesan text	Waktu eksekusi
sertifikat1.jpg	768 x 543	Muh Nur Aqsal Aminullah	341 - 391 ms
sertifikat1.jpg	768 x 543	Muh Aqsal	176 - 255 ms
sertifikat1.jpg	768 x 543	Muh Nur Aqsal Aminullah 105841102918	509 - 528 ms
sertifikat2.jpg	768 x 543	Muh Nur Aqsal Aminullah	358 - 425 ms
sertifikat2.jpg	768 x 543	Muh Aqsal	159 - 173 ms
sertifikat2.jpg	768 x 543	Muh Nur Aqsal Aminullah 105841102918	558 - 584 ms
sertifikat3.jpg	768 x 543	Muh Nur Aqsal Aminullah	343 - 378 ms
sertifikat3.jpg	768 x 543	Muh Aqsal	167 - 174 ms
sertifikat3.jpg	768 x 543	Muh Nur Aqsal Aminullah 105841102918	509 - 618 ms

Table 9. pengujian penggunaan least significant bit dengan menggunakan psnr

Nama file	Pesan text	PNSR
sertifikat1.jpg	Muh Nur Aqsal Aminullah	73.55
sertifikat1.jpg	Muh Aqsal	73.59
sertifikat1.jpg	Muh Nur Aqsal Aminullah 105841102918	73.51

sertifikat2.jpg	Muh Nur Aqsal Aminullah	72.39
sertifikat2.jpg	Muh Aqsal	72.43
sertifikat2.jpg	Muh Nur Aqsal Aminullah 105841102918	72.33
sertifikat3.jpg	Muh Nur Aqsal Aminullah	78.09
sertifikat3.jpg	Muh Aqsal	78.15
sertifikat3.jpg	Muh Nur Aqsal Aminullah 105841102918	78.01

Pada table dan diagram diatas dapat dilihat hasil pengujian yang dilakukan pada saat eksekusi atau proses pemasangan keamanan dilakukan dan berdasarkan hasil didapatkan diatas bahwa waktu eksekusi pada ukuran gambar yang berbeda akan memberikan jangka waktu eksekusi yang berbeda semakin besar ukuran gambar maka waktu eksekusi akan lebih lama dan juga pesan tersembunyi yang dimasukkan juga akan berpengaruh semakin panjang pesan yang ingin dimasukkan waktu eksekusi juga semakin lama. Pada table pengujian juga terdapat pada table pengujian PNSR dimana pengujian ini bertujuan untuk melihat perbandingan kualitas gambar antara gambar sebelum diberikan keamanan dan sesudah diberikan kemanan. Setelah melakukan pengujian dapat diketahui bahwa semakintinggi nilai PSNR nya maka secara kasat mata hamper tidak mengenali perbedaan gambarnya dari sebelum dan sesudah dilakukan pemasangan keamanan

Setelah melakukan pengecekan menggunakan black box selanjutnya untuk membuktikan penggunaan steganografi dengan metode least significant bit maka akan dijelaskan proses hasil uji coba menggunakan metode tersebut dengan secara sistematis untuk membuktikan proses penyisipan pesan tersembunyi ke dalam sertifikat digital dengan wadah yang digunakan yaitu file image.

Dalam proses penyisipan pesan tersembunyi ini akan diberikan sebagai contoh kata yaitu "Aqsal" dengan kode ASCII sebagai berikut :

A	q	s	a	l
65	113	115	97	108

Gambar 20. Nilai ASCII setiap huruf

Diperlihatkan diatas adalah bentuk ASCII dari kata yang akan digunakan untuk disisipkan kedalam sertifikat setelah mengetahui kode ASCII setiap huruf maka setiap kode ASCII tersebut akan di ubah menjadi sebuah bit. Pada kasus ini akan menggunakan 8 bit, yang artinya setiap 1 byte akan terdiri dari 8 bit dengan menggunakan rumus dibawah ini :

n	7	6	5	4	3	2	1	0
2^n	128	64	32	16	8	4	2	1

Gambar 21. Rumus perubahan dari nilai ASCII ke bit

Diatas adalah rumus yang akan digunakan untuk mengubah nilai ASCII setiap huruf yang di gunakan menjadi sebuah bit. Setelah mengetahui rumuys yang di gunakan maka perubahan ASCII menjadi sebuah bit dapat dilaksanakan yang akan dimulai dari huruf pertama yaitu M sampai dengan huruf h dan untuk perubahannya adalah sebagai berikut :

Table 10. Tabel perhitungan perubahan nilai ASCII setiap huruf menjadi nilai bit

				A = 65				
n	7	6	5	4	3	2	1	0
2n	128	64	32	16	8	4	2	1
d_n x 2^n	0 x 128	1x 64	0 x 32	0 x 16	0 x 8	0 x 4	0 x 2	1 x 1
				64 + 1 = 65				
Binner	0	1	0	0	0	0	0	1
				q = 113				
n	7	6	5	4	3	2	1	0
2n	128	64	32	16	8	4	2	1
d_n x 2^n	0 x 128	1x 64	1 x 32	1 x 16	0 x 8	0 x 4	0 x 2	1 x 1
				64 + 32 + 16 + 1 = 77				
Binner	0	1	1	1	0	0	0	1
				s = 115				

n	7	6	5	4	3	2	1	0
2n	128	64	32	16	8	4	2	1
$d_n \times 2^n$	0 x 128	1x 64	1 x 32	1 x 16	0 x 8	0 x 4	1 x 2	1 x 1
			64 + 32 + 16 + 2 + 1 = 115					
Binner	0	1	1	1	0	0	1	1

			a = 97					
n	7	6	5	4	3	2	1	0
2n	128	64	32	16	8	4	2	1
$d_n \times 2^n$	0 x 128	1x 64	1 x 32	0 x 16	0 x 8	0 x 4	0 x 2	1 x 1
			64 + 32 + 1 = 97					
Binner	0	1	1	0	0	0	0	1

			l = 108					
n	7	6	5	4	3	2	1	0
2n	128	64	32	16	8	4	2	1
$d_n \times 2^n$	0 x 128	1x 64	1 x 32	0 x 16	1 x 8	1 x 4	0 x 2	0 x 1
			64 + 32 + 8 = 4 = 108					
Binner	0	1	1	0	1	1	0	0

Setelah semua huruf di ubah menjadi menjadi sebuah bit dengan jumlah 1 byte terdari dari 8 bit maka hasil keseluruhannya akan seperti dibawah.

A = 65	q = 113	s = 115	a = 97	l = 108
01000001	01110001	01110011	01100001	01101100

Gambar 22. Hasil perubahan setiap huruf menjadi bit

Seperti yang diperlihatkan di atas adalah nilai bit setiap huruf yang telah di ubah menjadi sedemikian rupa dan setelah mendapatkan nilai bit setiap huruf kata yang akan disispkan ke sertifikat digital maka selanjutnya dalah memilih wadah yang akan disisipi oleh kata tersembunyi diatas untuk contoh yang akan di gunakan adalah file image seperti berikut.

Gambar 23. Sertifikat digital sebagai wadah

Setelah menentukan wadah untuk disisipi pesan tersembunyi untuk contoh kasus ini menggunakan sertifikat digital dengan ukuran 768 x 543 *pixel*. Untuk melakukan penyesipan maka nilai setiap *pixel* akan di ubah menjadi sebuah bit dan apa bila sertifiat diatas dilihat nilai *pixel*nya maka akan terluhat seperti dibawah ini.

[1, 1, 1, 255, 1, 1, 1, 255, 1, 1, 1, 255, 175, 176, 181, 255, 236, 236, 246, 255, 242, 244, 255, 255, 242, 244, 255, 255, 242, 244, 255, 255, 241, 245, 254, 255, 239, 246, 254, 255, 241, 244, 253, 255, 242, 244, 255, 255, 242, 246, 255, 255, 242, 246, 249, 255, 245, 244, 250, 255, 248, 236, 212, 255, 230, 216, 117, 255, 230, 202, 40, 255, 244, 199, 20, 255, 249, 198, 29, 255, 245, 208, 78, 255, 251, 236, 169, 255, 248, 245, 230, 255, 244, ...]

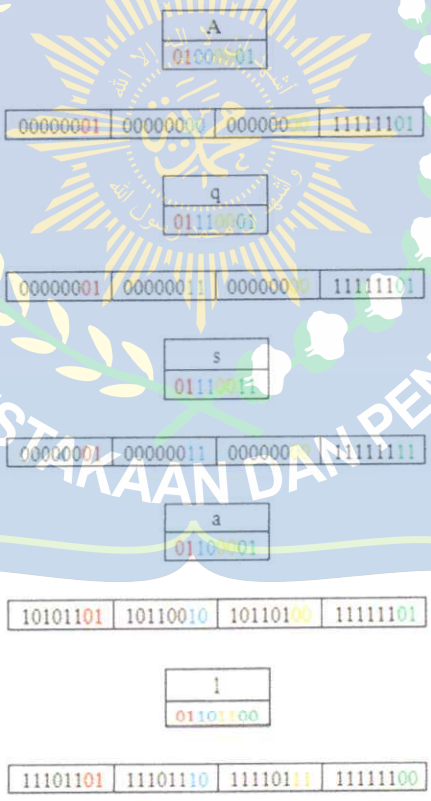
Gambar 24. Nilai *pixel* dari gambar sertifikat

Setelah mengetahui nilai *pixel*nya maka nilai *pixel* diatas akan diubah menjadi sebuah byte dengan berisikan 8 bit setiap byte nya, maka setiap *pixel* diatas akan diubah menjadi 1 byte yang terdiri dari 8 bit seperti dibawah ini.

```
00000001 00000001 00000001 11111111 00000001 00000001 00000001 11111111
00000001 00000001 00000001 11111111 10101111 10110000 10110101 11111111
11101100 11101100 11110110 11111111 11110010 11110100 11111111 11111111
11110010 11110100 11111111 11111111 11110010 11110100 11111111 11111111
11110001 11110101 11111110 11111111 11101111 11110110 11111110 11111111
11110001 11110100 11111101 11111111 11110010 11110100 11111111 11111111
11110010 11110110 11111001 11111111 11110101 11110100 11111010 11111111
11111000 11101100 11010100 11111111 11100110 11011000 11011001 11111111
11100110 11001010 00101000 11111111 11110100 11000111 00010100 11111111
11111001 11000110 00011101 11111111 11110101 11010000 01001110 11111111
11111011 11101100 10101001 11111111 11111000 11110101 11100110 11111111
11110100 ...
```

Gambar 25. Perubahan *pixel* setelah menajadi bit

Setelah setiap *pixel* diubah menjadi sebuah bit maka penyisipan pesan tersembunyi dapat dilakukan untuk memulai penyisipan huruf ke dalam bit gambar, penyisipannya untuk untuk huruf peratama yaitu A dengan bit 01000001 dan akan disisipkan di 2 bit terkhir setiap byte seperti dibawah ini.



Gambar 26. Penyisipan setiap bit huruf kedalam bit *pixel* sertifikat

Setelah setiap bit huruf disisipkan kedalam byte pada wadah sertifikat maka penyisipan akan berhenti dan hasil bit yang akan di dapatkan akan seperti berikut.

00000001	00000000	00000000	11111101	00000001	00000011	00000000	11111101
00000001	00000011	00000000	11111111	10101101	10110010	10110100	11111101
11101101	11101110	11110111	11111100	11110010	11110100	11111111	11111111
11110010	11110100	11111111	11111111	11110010	11110100	11111111	11111111
11110001	11110101	11111110	11111111	11101111	11110110	11111110	11111111
11110001	11110100	11111101	11111111	11110010	11110100	11111111	11111111
11110010	11110110	11111001	11111111	11110101	11110100	11111010	11111111
11111000	11101100	11010100	11111111	11100110	11011000	11011001	11111111
11100110	11001010	00101000	11111111	11110100	11000111	00010100	11111111
11111001	11000110	00011101	11111111	11110101	11010000	01001110	11111111
11111011	11101100	10101001	11111111	11111000	11110101	11100110	11111111
11110100	...						

Gambar 27. Hasil peyisipan bit huruf kedalam bit *pixel* sertifikat

Setelah mendapatkan bitnya maka apabila nilai *pixel* dari bit di atas di perlihatkan akan terlihat sebagai berikut.

[1, 0, 0, 253, 1, 3, 0, 253, 1, 3, 0, 255, 173, 178, 180, 253, 237, 238, 247, 252, 242, 244, 255, 255, 242, 244, 255, 255, 242, 244, 255, 255, 241, 245, 254, 255, 239, 246, 254, 255, 241, 244, 253, 255, 242, 244, 255, 255, 242, 246, 255, 255, 242, 246, 249, 255, 245, 244, 250, 255, 248, 236, 212, 255, 230, 216, 117, 255, 230, 202, 40, 255, 244, 199, 20, 255, 249, 198, 29, 255, 245, 208, 78, 255, 251, 236, 169, 255, 248, 245, 230, 255, 244, ...]

Gambar 28. Hasil penyisipan bit setelah diubah kembali menjadi nilai *pixel*

Setelah mendapatkan nilai *pixel* yang baru maka *stego image* yang akan didapatkan akan menjadi seperti dibawah ini.

Gambar 29. Sertifikat digital setelah disisipi pesan tersembunyi

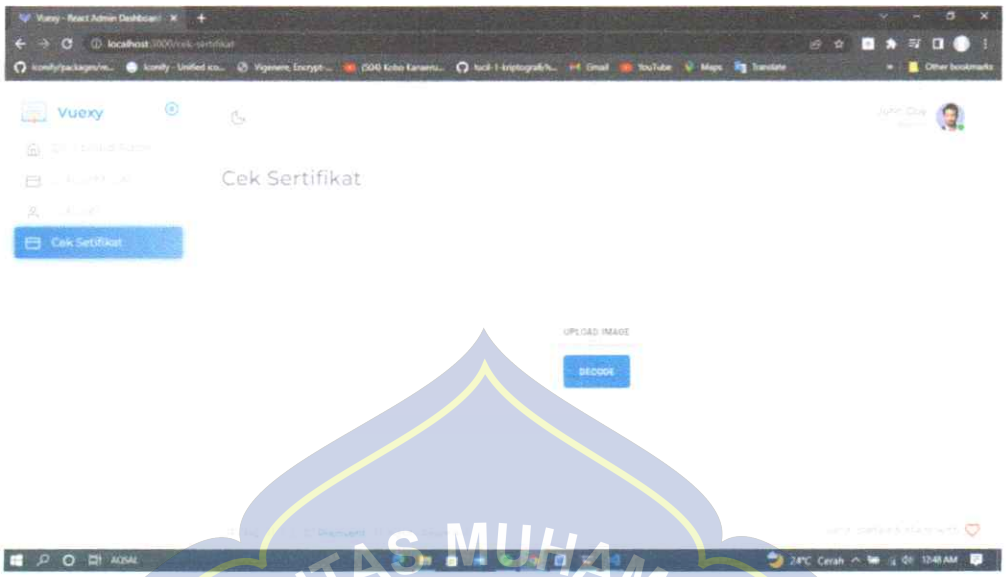
Seperti yang terlihat diatas setelah penyisipan pesan tersembunyi pada sertifikat yang memiliki format image maka hasilnya akan sama seperti sebelumnya walaupun sebenarnya terdapat perubahan terhadap *pixel* yang disisipi tapi perubahan itu tidak akan terlihat karena hanya menyisipkan kedalam bit yang significant tidak akan terlihat perubahannya pada kasus ini penyisipan dilakukan pada 2 bit terakhit setiap byte. Maka dari itu sertifikat sebelum di sisipi dan sertifikat setelah di sisipi tidak akan terlihat perbedaannya.

C. Pengecekan Keabsahan Sertifikat Digital

Pada hasil dan analisis yang dilakukan pada pengecekan keabsahan terhadap sertifikat digital terdapat dua hasil yang didapatkan dan pada sistem pengecekan keabsahan sertifikat ini hanya bisa akses oleh admin saja.

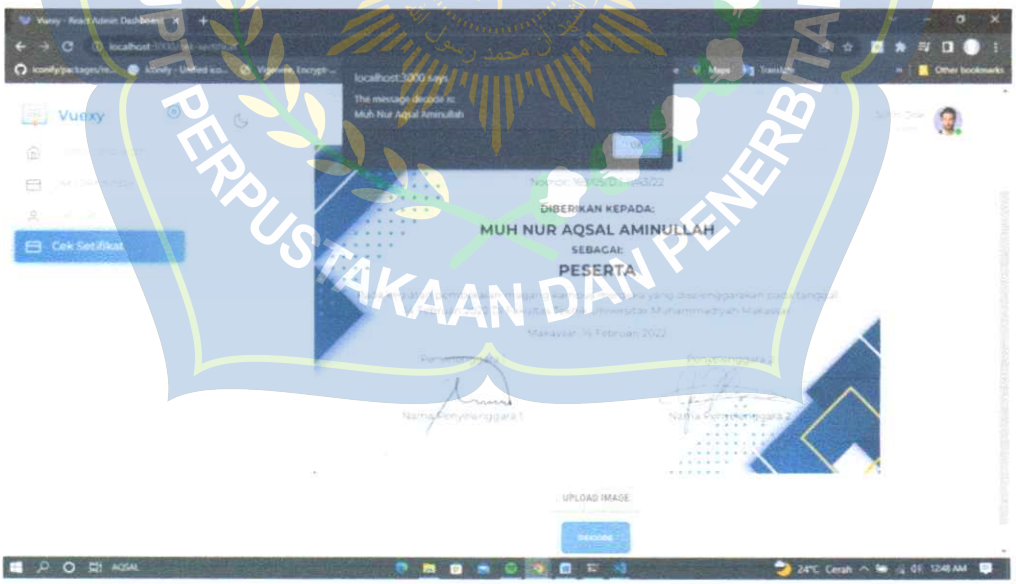
1. Pengujian Implementasi Antar Muka Pengecekan Keabsahan Sertifikat Digital

Berikut adalah hasil pengujian visual yang dilakukan pada sistem pengecekan keabsahan sertifikat digital dimana hanya admin yang dapat mengakses halaman pengecekan ini, untuk penjelasan setiap tahapannya sebagai berikut.



Gambar 30. Halaman pengecekan sertikat digital

Pada gambar diatas menggambarkan visual halaman dari admin untuk melakukan proses pengecekan sertifikat digital, pada halaman diatas diperlihatkan 2 tombol yaitu tombol untuk mengupload sertifikat digital tersebut yang berupa file image dan tombol decode untuk melakukan pengekstrakan pesan rahasia yang terkandung didalam sertifikat digital.



Gambar 31. Hasil pengecekan sertifikat

Pada gambar diatas diperlihat sebuah hasil yang diinginkan dimana hasil yang didapatkan yaitu sertifikat dapat di cek keabsahannya dengan memunculkan pesan tersembunyi didalam sertifikat digital tersebut. Dan berdasarkan hasil dalam penelitian yang dilakukan pengecekan keabsahan keabsahan sertifikat digital berhasil dijalankan dan memperlihatkan hasilnya seperti gambar diatas.

Sama seperti proses penyisipan pesan tersebunyi ke dalam sertifikat digital pada proses pengecekan pada sertifikat akan dilakukan penarikan pesan tesembunyi pada sertifikat digital untuk melakukan hal tersebut akan dilakukan seperti berikut.

Gambar 32. Sertifikat digital setelah disisipi pesan tersembunyi

Pada gambar diatas adalah sebuah sertifikat yang telah di sisipi pesan tersebunyi dan akan ditarik kembali pesan tersembunyi didalamnya, setelah sertifikat telah dipilih maka kita akan melihat nilai *pixel*nya seperti berikut.

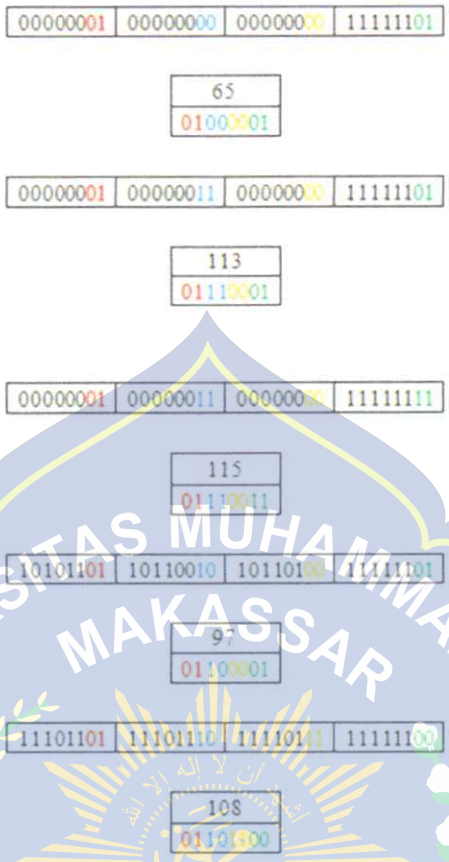
[1, 0, 0, 253, 1, 3, 0, 253, 1, 3, 0, 255, 173, 178, 180, 253, 237, 238, 247, 252, 242, 244, 255, 255, 242, 244, 255, 255, 242, 244, 255, 255, 241, 245, 254, 255, 239, 246, 254, 255, 241, 244, 253, 255, 242, 244, 255, 255, 242, 246, 255, 255, 242, 246, 249, 255, 245, 244, 250, 255, 248, 236, 212, 255, 230, 216, 117, 255, 230, 202, 40, 255, 244, 199, 20, 255, 249, 198, 29, 255, 245, 208, 78, 255, 251, 236, 169, 255, 248, 245, 230, 255, 244, ...]

Gambar 33. *Pixel stego image*

Setelah nilai setiap *pixel* diketahui maka setiap *pixel* tersebut akan di ubah menjadi sebuah bit dan akan terlihat seperti berikut.

Gambar 34. Gambar *pixel* yang telah diubah menjadi bit

Pada bit yang memiliki warna adalah bit yang akan diambil dan disatukan kembali dan akan menghasilkan nilai ASCII pesan tersembunyi yang tertanam di dalam sertifikat dan akan menghasilkan seperti berikut.



Gambar 35. Penarikan bit untuk mendapatkan setiap huruf yang tersembunyi

Setelah mendapatkan nilai ASCII dari pesan tersembunyi maka nilai tersebut sudah dapat di ubah menajadi sebuah huruf yang telah tersebunyi di dalam sertifikat tersebut dan hasilnya akan seperti berikut.

65	113	115	97	108
A	q	s	a	l

Gambar 36. Hasil pengambilan pesan tersembunyi pada *stego image*

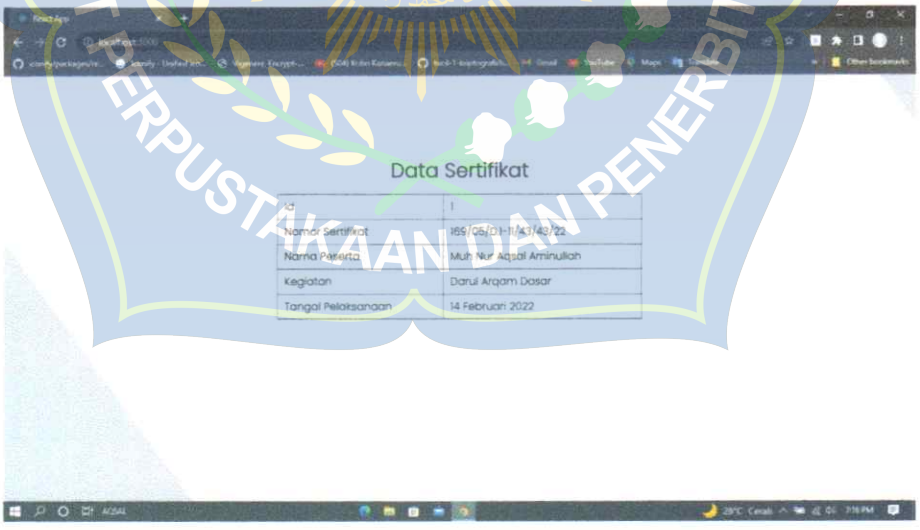
Setelah melakukan penecekan pada sertifikat maka akan mengasilkan atau menampilkan pesan tersembunyinya seperti gambar diatas.

Pada pengecekan diatas yang dilakukan menggunakan metode least significant bit hanya dapat mengambil kembali pesan tersebunyi pada sertifikat file yang asli dan tidak dapat mengecek apabila sertifikat tersebut

telah dimodifikasi atau pun bila file yang asli hilang tapi masih memiliki sertifikat fisik. Apabila kodisi tersebut terjadi maka pengecekan menggunakan least significant bit tidak dapat dilakukan lagi. Ole karena itu apabila kondisi tersebut terjadi maka diberikan alternative lain yaitu mengukanan barcode seperti berikut.

Gambar 37. Sertifikat yang meiliki barcode

Apabila barcode yang terdapat pada sertifikat discan maka barcode tersebut akan mengarahkan ke sebuah halama website yang menapilkan detail dari sertifikat yang di scan atau dicek seperti berikut.



Gambar 38. Detail data sertifikat

Pada gambar diatas diperlihatkan sebuah website yang menampilkan detail data dari sertifikat yang telah discan.

2. Pengujian Sistem Pengecekan Keabsahan Sertifikat Digital

Berikut adalah hasil pengujian yang dilakukan pada sistem pengecekan keabsahan pada sertifikat digital menggunakan pengujian black box.

Table 11. Pengujian black box testing pengecekan keabsahan sertifikat digital

No	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian
1	Klik Upload Image untuk memilih image sertifikat digital dan sertifikat yang dipilih akan ditampilan ke halaman website.	Sertifikat yang di upload akan ditampilkan di halaman website.	berhasil
2	Klik Decode untuk melakukan proses ekstrak untuk mendapatkan pesan tersembunyi pada sertifikat.	Sertifikat setelah diekstrak akan memunculkan pesan rahasia yang tertanam didalamnya.	berhasil

Pada table diatas adalah tabel pengujian yang dilakukan pada saat melakukan pengecekan sertifikat menggunkan least significant bit menggunkan pengujian black box.

BAB V
PENUTUP

A. Kesimpulan

Berdasarkan penelitian yang telah dilakukan dalam pengujian sistem pembuatan autentikasi untuk mendapatkan tanda tangan sertifikat digital, memberikan keamanan pada sertifikat digital menggunakan algoritma *steganografi* dengan metode *least significant bit* dan peengecekan keabsahan sertifikat digital sebagai berikut.

1. Hasil pengujian dalam memberikan sistem autentikasi yang telah dilakukan pada sistem ini dapat digunakan dan berhasil mengirimkan pesan notifikasi kepada tujuan dari website ke whatsapp dan pada pesan tersebut terdapat sebuah link untuk dialikan kehalaman form yang disediakan untuk melakukan penginputan tanda tangan digital.
2. Pengujian pada penelitian yang dilakukan untuk proses pemberian keamanan pada sertifikat digital proses pemasangannya dapat berjalan dengan baik dan pesan yang ditanamkan bisa di sisipikan kedalam gambar sertifikat digital tersebut melalui penyisipan setiap *bit pixel* gambar.
3. Hasil penelitana dalam melakukan proses pengecekan keabsahan pada sertifikat digital berhasil dilakukan dengan dapat mengeluarkan pesan yang tertanam didalam sertifikat digital yang telah dilakukan pengecekan.

B. Saran

Berdasarkan pengalaman dalam melaksanakan penelitan yang telah dilakukan dalam penerapan pada sistem yang telah dibuat tetapi pada yang bersamaan penulis juga berpikir masih adanya kekurangan yang dilakukan walaupun penulis ingin memberikan sebuah kesempurnaan oleh karena itu untuk menyempurnakan penelitan yang telah dilakukan maka akan diberikan saran untuk penelitan kedepanya agar kesempurnaan itu bisa didapatkan. Saran yang diberikan untuk penelitan kedepanya adalah sebagai berikut.

1. Pada sistem autentikasi sebaiknya diberikan batas waktu permintaan autentikasi agar permintaan dapat dilakukan secepatnya. Bila waktu yang ditentukan habis maka halaman form yang dikirimkan tidak dapat diakses dan harus melakukan permintaan autentikasi lagi.
2. Disarankan agar hasil sertifikat digital yang dibuat dikeluarkan menggunakan format file pdf.
3. Disarankan pada penelitian selanjutnya untuk proses pengecekan keabsahan apabila sertifikat digital telah dimofikasi maka pesan tersembunyi yang telah berubah tersebut dapat dimunculkan.

DAFTAR PUSTAKA

Abba Suganda Girsang, P. (2017). *Steganografi dengan Least significant Bit (LSB)*. Binus University Graduate Program. https://mti.binus.ac.id/2017/06/08/*steganografi* -dengan-least-significant-*bit* -lsb/

Ardiyasa, I. W. (2018). Implementasi Teknik Data Hidding Untuk Pengamanan Pesan Rahasia Pada Media Digital. *Seminar Nasional Sistem Informasi Dan Teknologi Informasi 2018*, 601–605.

Assyahid, M. M., Rihartanto, R., & Utomo, D. S. B. (2018). Implementasi *Steganografi* Pesan Text ke Dalam Audio Dengan Metode Spread Spectrum. *Ilmu Komputer Dan Teknologi Informasi*, *3*(2), 27–34.

Cahyo Prabowo, E., & Afrianto, I. (2017). PENERAPAN DIGITAL SIGNATURE DAN KRIPTOGRAFI PADA OTENTIKASI SERTIFIKAT TANAH DIGITAL. *Jurnal Ilmiah Komputer Dan Informatika (KOMPUTA)*, *6*(2), 83–90.

Erick Febriyanto, Untung Rahardja, Faturahman, A., & Nida Lutfiani. (2018). Sistem Verifikasi Sertifikat Menggunakan Qrcode Pada Central Event Information. *Techno.Com*, *18*(1), 50–63.

H Kara, O. A. M. A. (2014). Rekayasa Perangkat Lunak. *Paper Knowledge . Toward a Media History of Documents*, *7*(2), 107–115.

Hafis, A. (2019). *Steganografi* Berbasis Citra Digital untuk Menyembunyikan Data Menggunakan Metode *Least significant Bit* (LSB). *Jurnal Cendikia*, *XVII*(April), 194–198.

Indahyanti, U. (2020). Buku Ajar Algoritma Dan Pemrograman Dalam Bahasa C++. In *Buku Ajar Algoritma Dan Pemrograman Dalam Bahasa C++*. https://doi.org/10.21070/2020/978-623-6833-67-4

Laila, N., & Sinaga, A. S. R. (2019). Implementasi *Steganografi* LSB Dengan Enkripsi Vigenere Cipher Pada Citra. *ScientiCO : Computer Science and Informatics Journal*, *1*(2), 47–58.

https://doi.org/10.22487/j26204118.2018.v1.i2.11221

Muchlisin Riadi. (2017). *Sejarah, Prinsip Kerja dan Teknik Steganografi* . KAJIANPUSTAKA.COM. https://www.kajianpustaka.com/2017/09/sejarah-prinsip-kerja-teknik-*steganografi* .html

Pressman S, R., & Bruce R, M. (2006). *Software Engineering A Practitioners Approach*. https://doi.org/10.1049/ic:20040411

Rahmalia, N. (2021). *Apa Itu Black Box Testing? Yuk, Kenali Arti, Manfaat, dan Jenis-jenisnya*. Glints. https://glints.com/id/lowongan/black-box-testing/#.YqdZkKjP3Dc

Rajab, A. (2017). Studi Komparasi Metode *Least significant Bit* Dan Metode Echo Hiding Pada Audio Watermarking. *Doctoral Dissertation, STMIK AKAKOM Yogyakarta*.

Rony Setiawan. (2021). *Black Box Testing Untuk Menguji Perangkat Lunak*. Dicoding. https://www.dicoding.com/blog/black-box-testing/

Stefan Katzenbeisser and Fabien A. P. Petitcolas. (n.d.). *Information Hiding Techniques for Steganography and Digital Watermarking*.

Sugiyono. (2019). Bab III Metode Penelitian Dan Analisis Data. *Loc.Cit*.

Swastika, W., Santo, H. W., & Kelana, O. H. (2022). Rancang Bangun Website Akademik Dengan Penyimpanan Sertifikat Digital Menggunakan Teknologi Blockchain. *Jurnal Teknologi Informasi Dan Ilmu Komputer (JTIIK)*, *9*(1), 33–40. https://doi.org/10.25126/jtiik.202293645

wibowo subekti. (2021). *Pengertian Sertifikat Elektronik (Digital Certificate)*. Wibowopajak.Com. https://www.wibowopajak.com/2020/04/pengertian-sertifikat-elektronik.html

LAMPIRAN

Lampiran 1 : Source Code

```
// Fungsi penyisipan pesan kedalam gambar asli dan menampilkan gambar yang telah
  disisipi pesan
function encode() {
  if (isImageUpload) {      //Checks if an image is uploaded
    let message = document.getElementById('secret').value
    if (message.length > 1000) {
      alert("The message is too big to encode")
    } else {
      document.getElementById('encoded-image').style.display = 'none'
      document.getElementById('secret').value = ''
      let output = document.getElementById('encoded-image')
      let canvas = document.getElementById('canvas')
      let ctx = canvas.getContext('2d')
      let imgData = ctx.getImageData(0, 0, ctx.canvas.width, ctx.canvas.height)
      encodeMessage(imgData.data, message)
      ctx.putImageData(imgData, 0, 0)
      alert('Image encoded!\n Save below image for further use!')
      output.src = canvas.toDataURL()
    }
  } else {
    document.getElementById('upload-photo').value = ''
    alert("Please upload an image!")
  }
}
```

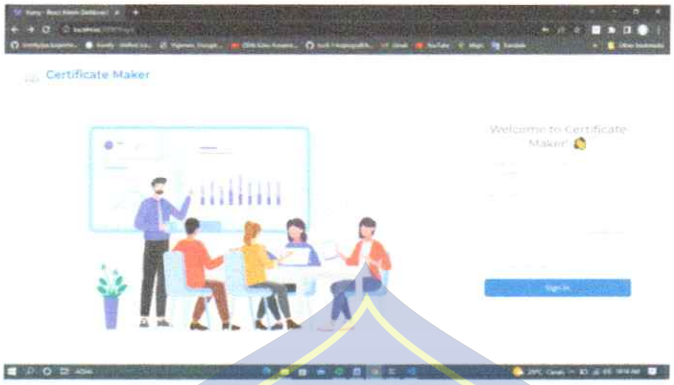
```
// fungsi mengambil pesan tersembunyi pada gambar dalam bentuk alert
function decode() {
  let ctx = document.getElementById('canvas').getContext('2d')
  let imgData = ctx.getImageData(0, 0, ctx.canvas.width, ctx.canvas.height)
  let message = decodeMessage(imgData.data)
  alert('The message decode is:\n' + message)
}

// Mengkodekan pesan menggunakan LSB
function encodeMessage(colors, message) {
  let messageBits = getBitsFromNumber(message.length)
  messageBits = messageBits.concat(getMessageBits(message))
  let history = []
  let pos = 0
  while (pos < messageBits.length) {
    let loc = getNextLocation(history, colors.length)
    colors[loc] = setBit(colors[loc], 0, messageBits[pos])
    while ((loc + 1) % 4 !== 0) {
      loc++
    }
    colors[loc] = 255
    pos++
  }
}

// Decode pesan dari gambar
function decodeMessage(colors) {
  let history = []
```

```
  let messageSize = getNumberFromBits(colors, history)
  if ((messageSize + 1) * 8> colors.length * 0.75) {
    return ''
  }
  if (messageSize === 0) {
    return ''
  }
  let message = []
  for (let i = 0; i < messageSize; i++) {
    let code = getNumberFromBits(colors, history)
    message.push(String.fromCharCode(code))
  }
  return message.join('')
}

function getBit(number, location) {
  return ((number >> location) & 1)
}

// set bit di lokasi ke bit antara 1 dan 0
function setBit(number, location, bit) {
  return (number & ~(1 << location)) | (bit << location)
}

// mengembalikan array 1 dan 0 dari 2 bit terakhir
function getBitsFromNumber(number) {
  let bits = []
  for (let i = 0; i < 8; i++) {
    bits.push(getBit(number, i))
```

```
  }
  return bits
}

// mengembalikan 2 bit terakhir dari bit berikutnya
function getNumberFromBits(bytes, history) {
  let number = 0,
    pos = 0
  while (pos < 8) {
    let loc = getNextLocation(history, bytes.length)
    let bit = getBit(bytes[loc], 0)
    number = setBit(number, pos, bit)
    pos++
  }
  return number
}

// mengembalikan array 1 dan 0 untuk menjadi string 'pesan'
function getMessageBits(message) {
  let messageBits = []
  for (let i = 0; i < message.length; i++) {
    let code = message.charCodeAt(i)
    messageBits = messageBits.concat(getBitsFromNumber(code))
  }
  return messageBits
}

// mendapatkan lokasi berikutnya untuk menyimpan bit
function getNextLocation(history) {
```

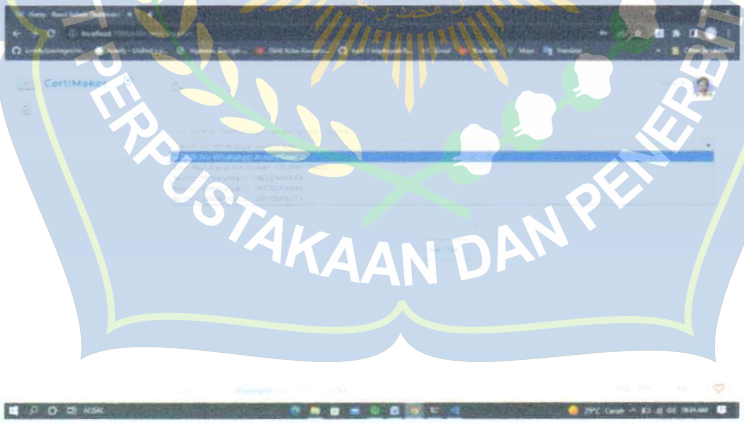
```
let loc = 0
while (true) {
  if (history.indexOf(loc) >= 0) {
    loc++
  } else if ((loc + 1) % 4 === 0) {
    loc++
  } else {
    history.push(loc)
    return loc
  }
}
}
```

Lampiran 2 : Hasil Pengujian Sistem

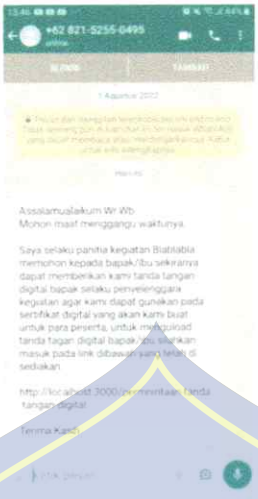


Gambar 1. Halaman login user

Gambar 2. Halaman dashboard user

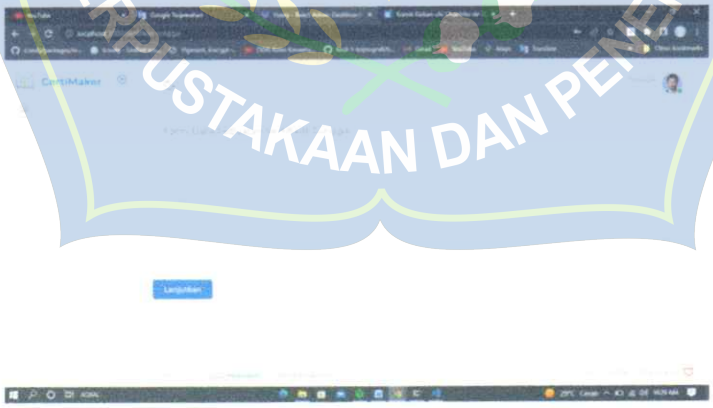


Gambar 3. Halaman input nomor whatsapp

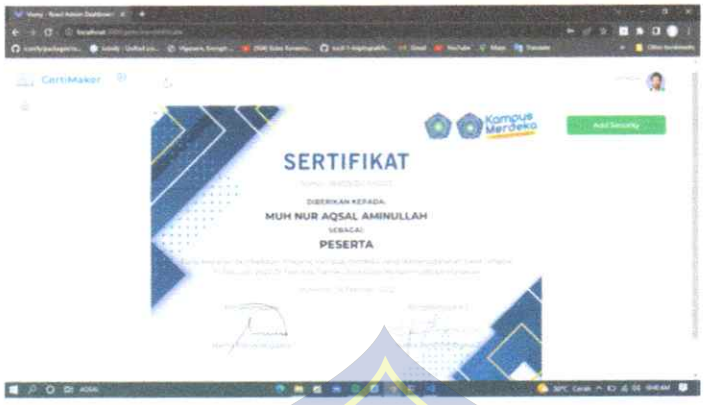


Gambar 4. Pesan notifikasi permintaan autentikasi

Gambar 5. Halaman input tanda tangan digital



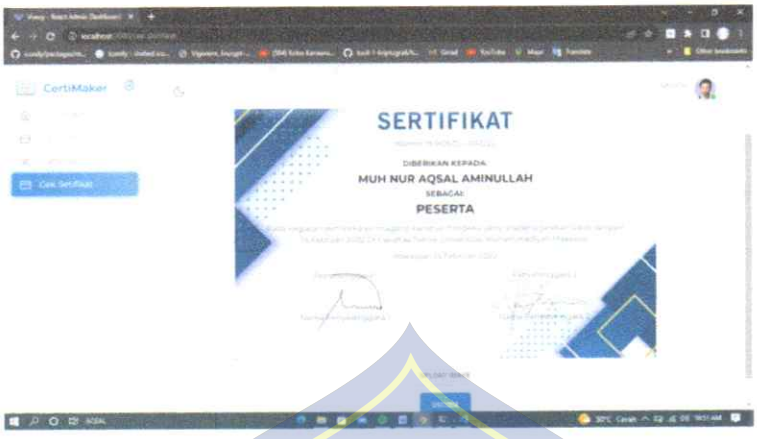
Gambar 6. Halaman input data sertifikat



Gambar 7. Halaman Preview sertifikat

Gambar 8. Halaman login admin

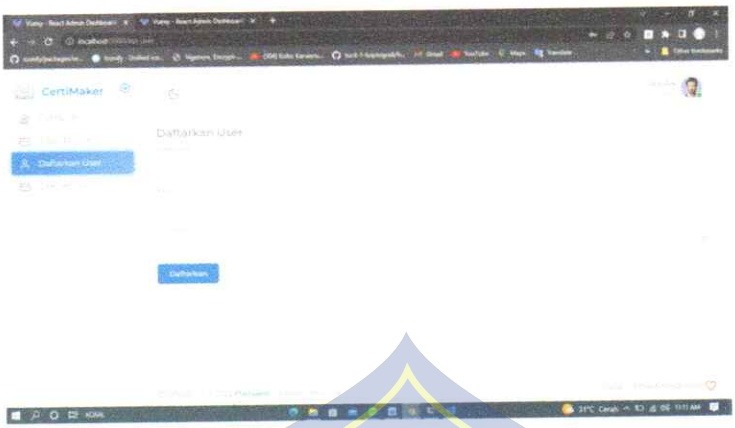
Gambar 9. Halaman cek sertifikat



Gambar 10. Halaman cek sertifikat seletah upload sertifikat

Gambar 11. Halaman cek sertifikat dan menampilkan pesan tersebunyi

Gambar 12. Halaman meninput nomor whatsapp



Gambar 13. Halaman daftarkan user