AINET Jurnal Informatika

e-ISSN : 2686 – 1917
p-ISSN : 2657 – 0653

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

Muh Nur Aqsal Aminullah*[1], Rizki Yusliana Bakti[2], Muhyiddin AM Hayat[3], Lukman[4]
[1,2,3,4]Informatika, Universitas Muhammadiyah Makassar
e-mail: aqsa3236@gmail.com*

Abstract

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 steganography 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 steganography 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;

Abstrak

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;

AINET Jurnal Informatika
e-ISSN : 2686 – 1917
p-ISSN : 2657 – 0653

1. Pendahuluan

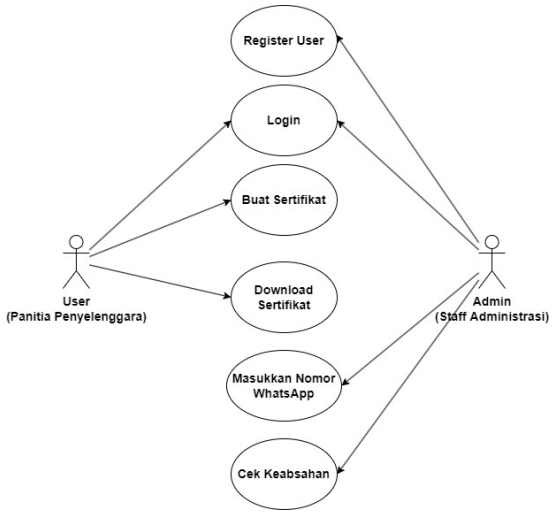
Sertifikat digital merupakan sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan penyelenggara sertifikasi elektronik [1]. Sertifikat digital ini dapat dikatakan adalah sebuah dokumen yang sangat penting karena seperti yang diketahui bahwa sertifikat digital adalah sebuah bukti hak kepemilikan seseorang terhadap sebuah produk dan juga dapat menjadi bukti untuk mewakili keampuan seseorang ataupun sebagai bukti untuk mengetahui seseorang tersebut pernah mengukuti sebuah kegiatan dan bisa mendapatkan sertifikatnya. Steganografi berasal dari bahasa Yunani yaitu Steganos yang berarti menyembunyikan dan Graptos yang artinya tulisan, sehingga secara keseluruhan artinya adalah tulisan yang disebunyikan. Secara umum steganografi adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia [2]. *Least Significant Bit* (LSB) adalah teknik yang umum digunakan dalam enkripsi dan dekripsi informasi rahasia. Cara kerja metode LSB yaitu mengubah bit redundan cover image yang tidak berpengaruh signifikan dengan bit dari pesan rahasia [3][4].

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. 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 [5]

Penelitian ini bertujuan untuk memberikan sebuah sistem autentikasi pada aplikasi pembuatan sertifikat digital agar memudahkan dalam mendapatkan tanda tangan digital penyelenggara sebuah kegiatan tanpa harus bertemu langsung untuk mendapatkannya. Memberikan sebuah sistem keamanan pada sertifikat digital yang akan dibuat dengan menggunakan algoritma steganografi dengan metode least significant bit sebagai keamanannya.

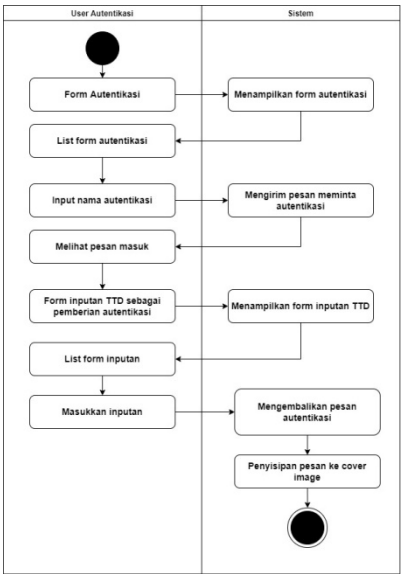
2. Metode Penelitian

Pada penelitian ini dilakukan pada kempus Universitas Muhammadiyah Makassar bagian administrasi mahasiswa. Berdasarkan permasalahan yang telah disebutkan maka diberikan sebuah gambaran sistem yang dibuatkan dalam pembuatan sertifikat digital.



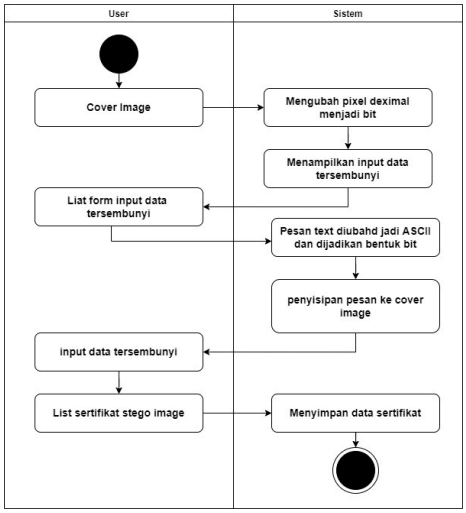
Gambar 1. Use Case Interaksi antara Sistem dan Actor

Pada gambar 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.



Gambar 2. Activity diagram dalam proses autentikasi

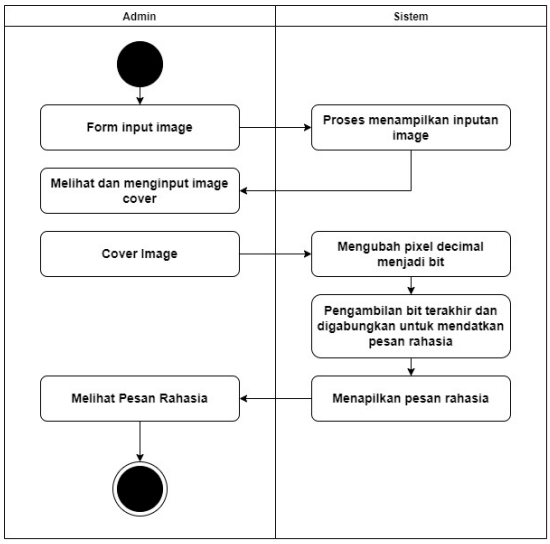
Pada gambar diatas diperlihatkan bagaimana cara kerja dalam melakukan autentikasi sertifikat yang dimana pada website sebelum melanjutkan penginputan data sertifikat pengguna harus melakukan autentikasi agar bisa mendapatkan tanda tangan pihak penyelenggara untuk dimasukkan tanda tangannya didalam sertifikat digital. Pada prosesnya yaitu melalaui penginputan nomor whatsapp tujuan dan penyelenggara mendapat notifikasi permintaan tanda tangan digital dan mengklik link yang telah disediakan dan dilanjutkan penginputan tanda tangan digital.



Gambar 3. 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.



Gambar 4. 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.

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 [6].

Pada penelitan ini pada penguian yang digunakan adalah pengujian *black box*. *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 [7].

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*[8]

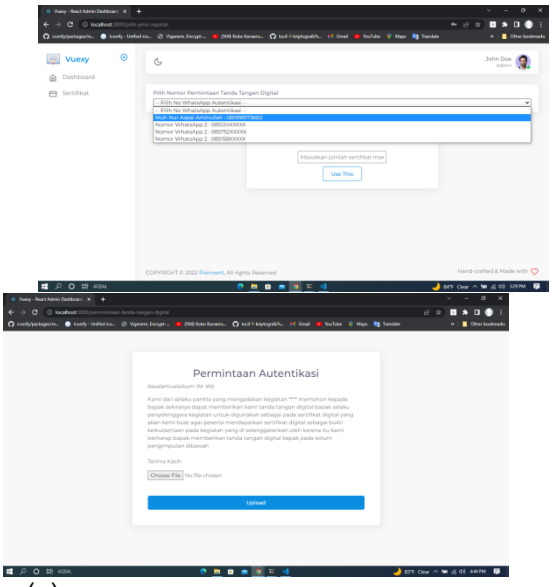
3. Hasil dan diskusi

pada bagian hasil penelitian ini akan terdapat hasil yang akan diperlihatkan yang merujuk pada rumusan masalah dan 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.

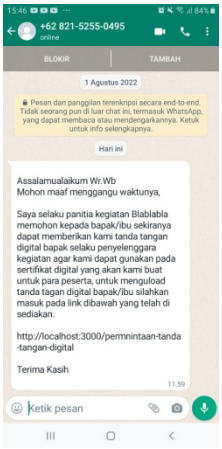
3.1. Autentikasi Tanda Tangan Digital

Berikut adalaah tahapan-tahapan pengujian implementasi antar muka yang akan di uji untuk melakukan autentikasi agar mendapatkan tanda tangan digital berdasarkan penelitian yang dilakukan.

AINET Jurnal Informatika
e-ISSN : 2686 – 1917
p-ISSN : 2657 – 0653



(a) (c)



(b)

Gambar 5. Hasil pengujian implementasi antar muka autentikasi tanda tangan digital

Pada gambar 5 diatas adalah hasil pengujian implamentasi antarmuka dalam proses pengujian autentikasi permintaan tanda tangan digital yang dimulia dari penginputan nomor whatsapp tujuan dan dikirimkan kepada tujan permintaan selanjutnya penerima menerima pesan notifikasi dan mengklik link yang tersedia untuk mengakses halaman penginputan tanda tangan digital.

Tabel 1. 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

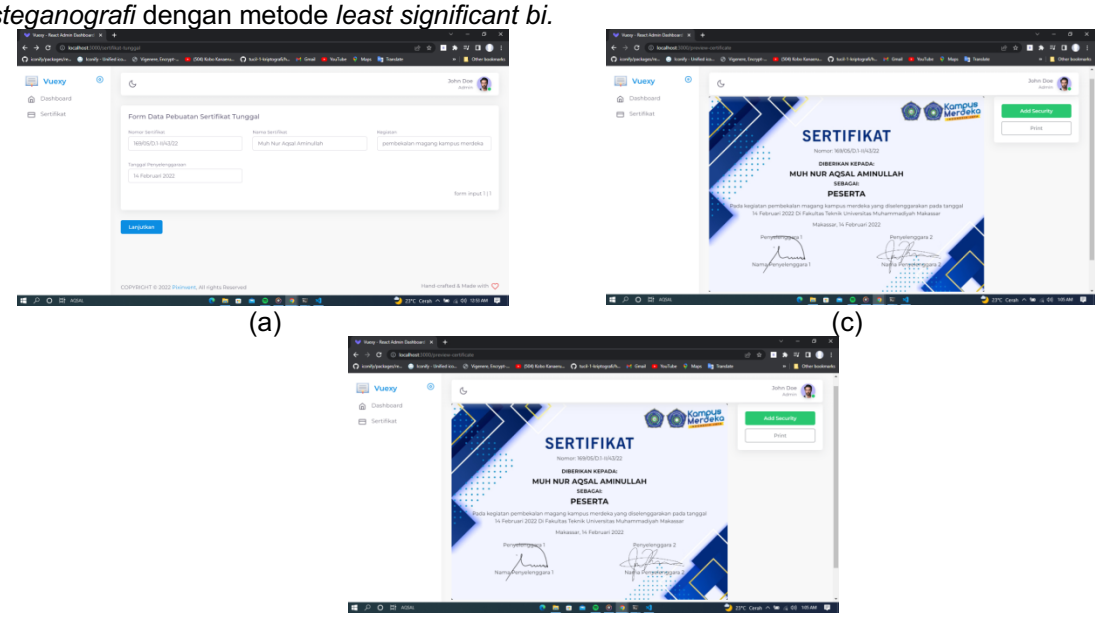
AINET Jurnal Informatika
e-ISSN : 2686 – 1917
p-ISSN : 2657 – 0653

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*.

3.2. Keamanan Sertifikat Digital

Berikut adalah hasil dan analias yang dilakukan pada sistem proses pemasangan keamanan pada sertifikat digital berhasil dilakukan dengan menggunakan algoritma *steganografi* dengan metode *least significant bi.*



(a) (c)

(b)

Gambar 6. Hasil pengujian implementasi antar muka pemasangan keamanan sertifikat digital

Gambar 6 diatas adalah hasil pengujian implementasi antar muka saat melakukan proses pemasangan sertifikat digital menggunakan algoritma steganografi dengan metode least significant bit.

Tabel 2. Pengujian black box testing proses pemasangan 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 pengujian yang dilakukan pada saat pembuatan sertifikat digital dalam hingga sertifikat digital selesai dibuat dan pemasangan keamanan pada sertifikat digital.

Pada proses pemasangan keamanan sertifikat digital dilakukan sebuah analisis untuk menguji waktu eksekusi pemasangan keamanan sertifiakt digital dimulai dari analisis berdasarkan ukuran size gambar, analisis berdasarkan pesan text yang disisipkan dan analisis kualitas gambar menggunakan PSNR dimana dimana nilai value semakin besar maka tingkat kesamaannya tinggi.

Tabel 3. Hasil analisis pengujian wektu eksekusi 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

Tabel 4. Hasil analisis pengujian wektu eksekusi 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

Tabel 5. 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

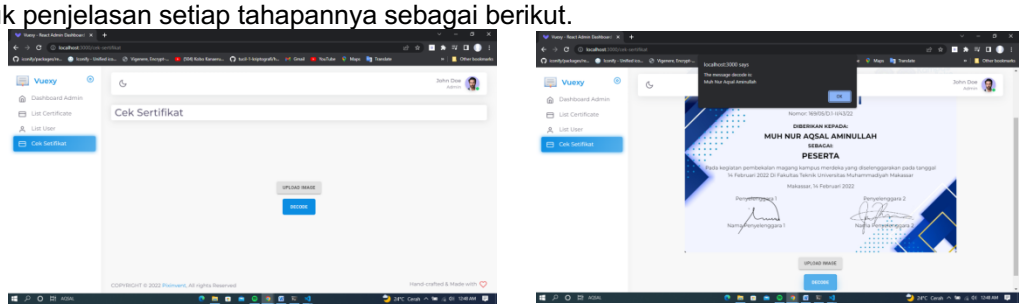
Pada Tabel 3 adalah analisis hasil pengujian pada pemasangan sertifiakt berdasarkan ukuran size gambar, Tebel 4 adalah analisis hasil pengujian pada pemasangan keamanan

AINET Jurnal Informatika
e-ISSN : 2686 – 1917
p-ISSN : 2657 – 0653

sertifikat berdasarkan text pesan dan pada Tabel 5 adalah analisis pengujian penggunaan least significant bit dengan menggunakan psnr

3.3. Pengecekan Keabsahan Setifiikat 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.



(a) (b)

Gambar 7. Hasil pengujian implementasi antar muka pengecekan keabsahan sertifikat digital

Gambar 7 diatas memperlihatkan hasil impleentasi antar muka saat melakukan sebuah kegiatan pengecekan pada sertifikat digital dengan hasil yang dikeluarkan dari pengecekan tersebut akan memperlihatkan pesan tersembunyi di dalam sertifiakt digital tersebut.

Tabel 2. Pengujian black box testing proses pengecekan keabsahan sertifikat digita

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 digital menggunkan least significant bit menggunkan pengujian black box.

4. Kesimpulan

Berdasarkan penelitian yang dilakukan maka didapatkan tiga hasil yaitu 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 penelitian dalam melakukan proses pengecekan keabsahan pada sertifikat digital berhasil dilakukan dengan dapat mengeluarkan pesan yang tertanam didalam sertifikat digital yang telah dilakukan pengecekan.

Referensi

[1] wibowo subekti, “Pengertian Sertifikat Elektronik (Digital Certificate),” *wibowopajak.com*, 2021. https://www.wibowopajak.com/2020/04/pengertian-sertifikat-elektronik.html

[2] A. Hafis, “Steganografi Berbasis Citra Digital untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB),” *Jurnal Cendikia*, vol. XVII, no. April, pp. 194–198, 2019.

[3] I. W. Ardiyasa, “Implementasi Teknik Data Hidding Untuk Pengamanan Pesan Rahasia Pada Media Digital,” *Seminar Nasional Sistem Informasi dan Teknologi Informasi 2018*, pp. 601–605, 2018.

[4] A. S. Girsang, “Steganografi dengan Least significant Bit (LSB),” *Binus University*, Jul. 08, 2017. https://mti.binus.ac.id/2017/06/08/steganografi-dengan-least-significant-bit-lsb/ (accessed Mar. 06, 2022).

[5] G. Ekonomi, “Verifikasi dan Validasi,” *sarjanaekonomi*, 2021. https://sarjanaekonomi.co.id/verifikasi-dan-validasi/

[6] Sugiyono, “Bab III Metode Penelitian Dan Analisis Data,” *Loc.cit*, 2019.

[7] Rony Setiawan, “Black Box Testing Untuk Menguji Perangkat Lunak,” *dicoding*, 2021. https://www.dicoding.com/blog/black-box-testing/

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