JIKA (Jurnal Informatika) Universitas Muhammadiyah Tangerang *P ISSN : 2549-0710*
Tangerang, November 2020, pp. 87- 93 *E ISSN : 2722-2713*

MENYISIPKAN PESAN RAHASIA KEDALAM GAMBAR DENGAN METODE BLOWFISH DAN LEAST SIGNIFICANT BIT (LSB)

Siti Muryanah[1], Ismatul Maula[2], Intan Murniasih[3]
[1] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Islam Syekh Yusuf, Tangerang
Jalan Maulana Yusuf No. 10 Babakan Kota Tangerang
[2,3] Program Studi Teknik Informatika, Fakultas Teknik, Universitas Budi Luhur, Jakarta
Jalan Ciledug Raya, Petukangan Utara, Jakarta Selatan
Email: siti.muryanah@unis.ac.id[1], iismatull@gmail.com[2] ,intan.reyy@yahoo.com[3]

Article history
Received Jul 28, 2020
Revised Okt 13, 2020
Accepted Nov 02, 2020
Available Online Nov 28 , 2020

Keywords
steganography,
blowfish,
least significant

Abstract

Current technological developments make information needs very important. However, information that becomes confidential will become public information due to insecurity of the information in the process of exchanging information from the sender to the recipient of the information. In this regard, there are several things that must be considered during the process of sending messages, namely confidentiality, integrity, availability, authenticity, and non-repudiation. On this basis, the authors combine information security with cryptographic and steganographic methods. Cryptography is the change of the original message into a secret message, while steganography is the art of inserting messages into a media so that other people do not realize that there is a secret message in the media. The cryptographic methods that I use are the Blowfish method and the LSB steganography method. The insertion method using the LSB method is the process of inserting messages by presenting binary image files or images with binary representations of secret messages to be hidden. Thus, at every pixel a 24-bit BMP image or image file can be inserted with 3 message bits. The result is a secret message successfully inserted into the picture and reduce the suspicion of others that the picture has confidential information.

Riwayat
Diterima 28 Jul 2020
Revisi 13 Okt 2020
Disetujui 02 Nov 2020
Terbit 28 Nov 2020

Kata Kunci
steganografi,
blowfish,
least significant bit

Abstrak

Perkembangan teknologi saat ini membuat kebutuhan informasi menjadi sangat penting. Namun informasi yang menjadi rahasia akan menjadi informasi umum karena kurang amannya informasi tersebut dalam proses pertukaran informasi dari pengirim ke penerima informasi. Berkaitan dengan hal ini, ada beberapa hal yang harus diperhatikan ketika proses pengiriman pesan yaitu confidentiality, integrity, availability, authenticity, dan non-repudiation. Atas dasar ini penulis melakukan pengabungan keamanan informasi dengan metode kriptografi dan steganografi. Kriptografi adalah perubahan pesan asli menjadi pesan rahasia, sedangkan steganografi merupakan seni dalam menyisipkan pesan ke dalam suatu media agar orang lain tidak menyadari bahwa dalam media tersebut terdapat pesan rahasia. Metode kriptografi yang penulis gunakan adalah metode Blowfish dan metode steganografi LSB. Metode penyisipan dengan mengunakan metode LSB merupakan proses menyisipkan pesan dengan presentasi biner file gambar atau citra dengan representasi biner pesan rahasia yang akan disembunyikan. Sehingga, pada setiap pixel file gambar atau citra BMP 24 bit dapat disisipkan dengan 3 bit pesan. Hasilnya pesan rahasia berhasil disisipkan ke dalam gambar dan mengurangi kecurigaan orang lain bahwa gambar tersebut terdapat informasi rahasia.

PENDAHULUAN

Dengan perkembangan media komunikasi yang semakin berkembang, diperlukan suatu metode keamanan dalam menyampaikan informasi dari pengirim ke penerima informasi agar tidak diketahui atau dicurigai oleh pihak atau orang yang tidak berwenang. Melalui penelitian ini diharapkan dapat menjadi alternatif dalam menjaga keamanan informasi atau data. Cara atau teknik yang penulis lakukan adalah dengan menyembunyikan pesan melalui gambar atau steganografi dengan menggunakan metode LSB dan Blowfish untuk kriptografinya. Metode LSB (Least Significant Bit) adalah menyisipkan atau menyembunyikan pesan rahasia dengan cara mengganti bit ke 8, 16 dan 24 pada representasi biner di file gambar atau citra, sehingga pada setiap pixel file gambar atau citra BMP 24 bit dapat disisipkan dengan 3 bit pesan. (Andrian, 2013) memaparkan hal yang sama mengenai steganografi dengan metode LSB, tetapi penulis dalam penelitian ini menambahkan suatu fitur baru yaitu dengan pengiriman hasil enkripsi pesan ke aplikasi WhatsApp. Terkait mobilitas yang tinggi saat ini, penerima pesan akan lebih cepat mengetahui bahwa telah menerima pesan rahasia melalui media sosial tersebut.

Blowfish merupakan salah satu dari metode kriptografi yang hingga saat ini tidak dipatenkan dan dirasa cukup kuat dikarenakan metode ini memiliki ruang kunci yang cukup besar dan panjangnya pun bisa beragam. Dalam hal ini akan dirasa tidak mudah ketika diserang pada bagian kuncinya. "Blowfish merupakan algoritma kriptografi kunci simetrik cipher blok dengan panjang blok tetap sepanjang 64 bit" (Springer-Verlag, 1994). Algoritma dalam metode Blowfiah juga mengunakan teknik kunci yang berukuran tidak tetap atau sembarang. "Ukuran kunci yang dapat diterima oleh blowfish adalah antara 32 hingga 448 bit, dengan ukuran standar sebesar 128 bit" (Ariyus, 2008). Blowfish mengunakan teknik pemanipulasian bit, pemutaran ulang dan pergiliran kunci yang dilakukan sebanyak 16 kali.(Wardoyo, Imanullah, & Fahrizal, 2016)

Steganografi dapat diartikan sebagai ilmu ataupun seni dalam menyembunyikan pesan rahasia (*hiding message*) yang sedemikian rupa sehingga keberadaan (*eksistensi*) pesan tersebut tidak terlhat oleh indera atau mata manusia. "Media yang digunakan umumnya merupakan suatu media yang berbeda dengan media pembawa informasi rahasia, disinilah fungsi dari teknik *steganography* yaitu sebagai teknik penyamaran menggunakan media lain yang berbeda sehingga informasi rahasia dalam media awal tidak terlihat secara jelas" (William, 2011).

Kata steganografi *(steganography)* berasal dari bahasa Yunani yang terdiri dari kata *steganos* yang artinya tersembunyi dan *graphien* yang artinya menulis, sehingga dapat berarti tulisan yang tersembunyi. Dapat disimpulkan bahwa, "Steganografi adalah ilmu yang mempelajari teknik pengembangan pesan rahasia di dalam pesan yang lainnya, sedemikian rupa sehingga orang lain tidak akan tahu bahwa terdapat pesan rahasia di dalam pesan yang mereka baca" (William, 2011). "Metode Steganografi menyembunyikan sebuah pesan dalam *cover carriers* sehingga pesannya tidak dapat dilihat pada saat dikirimkan melalui kanal komunikasi publik seperti jaringan komputer" (Lou & Liu, 2002).

Penyisipan pesan dengan metode *Least significant bit* (LSB) merupakan pendekatan yang umum untuk menyisipkan informasi ke dalam media gambar atau citra. (Monica, 2016) *S*ebagian atau seluruh byte diubah menjadi sebuah bit dalam sebuah citra dari pesan rahasia. Jika menggunakan citra dengan 24-bit, maka bit dari masing-masing komponen warna merah, hijau dan biru dapat digunakan, dikarenakan masing-masing komponen dapat ditampilkan dalam bentuk byte. Dengan kata lain, kita dapat menyimpan 3 bit dari setiap pixel yang ada. Citra dengan pixel 500 × 500, dapat menyimpan total 750,000 bit atau 93.750 byte data yang dapat disisipkan. "Dalam metode yang ada, dibutuhkan representasi biner dari data yang akan disembunyikan dengan metode LSB" (William, 2011). Dapat dicontohkan apabila kita memiliki tiga

pixel yang berdekatan (sembilan bytes) dengan kode RGB sebagai berikut:

11110101	00010110	10101010
11000100	11111001	00000001
00000001	11110001	00011101

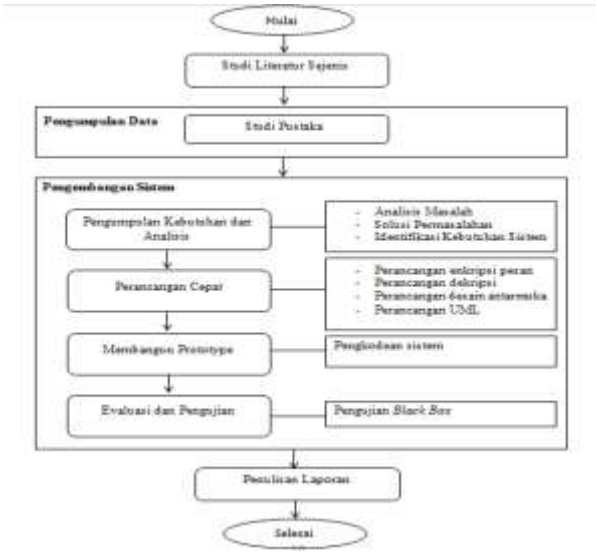
Terdapat karakter "S" yang akan disisipkan dengan nilai biner "01010011", maka citra hasil dengan urutan bit sebagai berikut:

1111010**0**	0001011**1**	1010101**0**
1100010**1**	1111100**0**	0000000**0**
0000000**1**	1111000**1**	0001110**1**

Dengan menggunakan metode ini seseorang yang tidak berwenang dapat dengan mudah mengurai pesan yang terdapat di dalam citra. Dalam perubahan nilai LSB tersebut, semua pixel menjadi nilai "0" atau "1", maka pesan rahasia dapat rusak. "Penghancuran pesan ini hanya mengubah sedikit kualitas gambar, yaitu di kisaran 1 atau -1 pada setiap posisi piksel" (Andrian, 2013).

- **Metode Penelitian**

Metode penelitian yang penulis gunakan dalam penelitian ini diawali dengan studi literatur sejenis, studi pustaka dalam pengumpulan data, pengembangan sistem dan penulisan laporan. Metode penelitian tersebut dapat diperjelas dalam bentuk gambar dibawah ini:



Gambar 1. Metode Penelitian

Dalam studi literatur sejenis, penulis melakukan perbandingan penelitian ini dan mencari kekurangan serta kelebihan terhadap penelitian lainnya. Penulis menggunakan studi pustaka dalam metode pengumpulan datanya. Penulis melakukan studi pustaka dengan informasi yang terdapat dalam buku yang berkaitan dengan penelitian ini dan mengumpulkan jurnal-jurnal sebagai referensi.

Pengembangan sistem yang penulis lakukan diantaranya, pengumpulan kebutuhan dan analisis, perancangan cepat, membangun prototype, evaluasi dan pengujian sistem. Bagian terakhir dari metode penelitian ini adalah melakukan penulisan laporan.

- **Temuan Hasil Penelitian**

Dalam bab ini penulis akan membahas tentang implementasi terhadap sistem yang sesuai dengan metode pengumpulan data, metode pengembangan sistem yang digunakan dan temuan hasil penelitiannya. Dalam mengembangkan sistem ini, penulis menggunakan metode pengembangan sistem prototype yang terdiri dari :

Perancangan Enkripsi Pesan

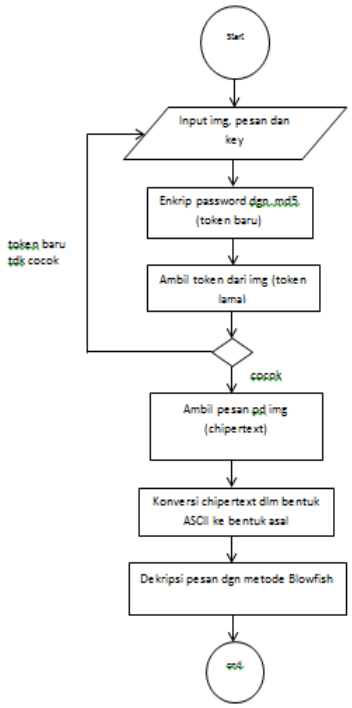
Gambar dibawah ini merupakan perancangan flowchart proses enkripsi pesan.

Gambar 2. Flowchart Enkripsi Pesan

P ISSN : 2549-0710
E ISSN : 2722-2713

Perancangan Dekripsi Pesan

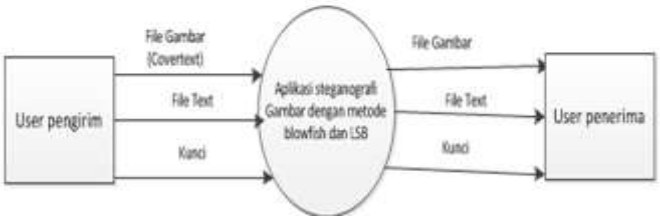
Gambar dibawah ini merupakan perancangan flowchart proses dekripsi pesan.



Gambar 3. Flowchart Dekripsi Pesan

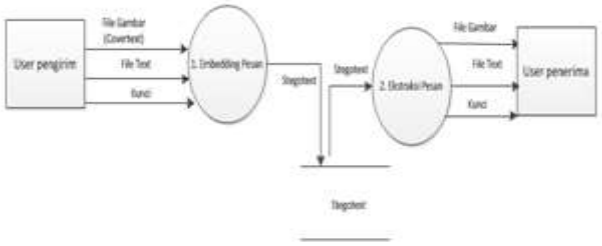
Perancangan penyisipan pesan ke dalam gambar

Perancangan sistem dalam aplikasi ini mengunakan diagram konteks, dimana diagram yang menjelaskan sistem secara umum, dengan memberikan gambaran terkait hubungan lingkungan di dalam sistem (*internal entity*) dan lingkungan di luar sistem (*external entity*). Berikut diagram konteks dari aplikasi steganografi yang penulis gunakan:



Gambar 4. Konteks Diagram

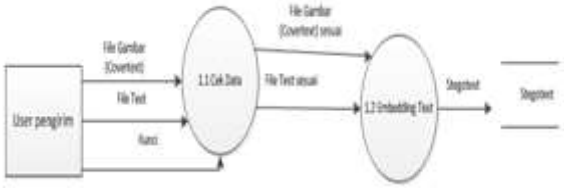
Pada diagram konteks diatas, dapat dijelaskan bahwa untuk proses steganografi (penyisipan pesan ke dalam gambar berlangsung 2 arah. User pengirim menginput atau memasukkan citra/gambar dan file teks, selanjutnya user penerima menerima file gambar dan file teks dalam sebuah file berupa *stegotext*. DFD level 0 dari pengembangan aplikasi ini adalah:



Gambar 5. DFD Level 0 Aplikasi Steganografi

Pada DFD Level 0, juga ada 2 proses yaitu proses penyisipan pesan atau *embedding* dan ekstraksi pesan. Dimana dalam proses penyisipan pesan ini, user pengirim menginput file gambar dan file teks kemudian menjadi *stegotext*. User penerima menerima *stegotext* tersebut dan diekstrak kembali menjadi file teks dan file gambar aslinya.

DFD level 1 dari Proses pertama yaitu *embedding* pesan yaitu:

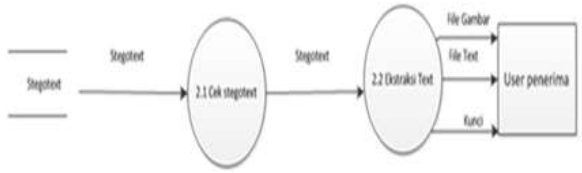


Gambar 6. DFD Level 1 Proses *embedding* pesan

Dalam DFD Level 1 (proses *embedding* pesan) terdapat 2 proses yaitu proses cek data dan *embedding* teks. Pada proses cek data, file gambar atau citra dilakukan pengecekan terlebih dahulu apakah terdapat *fleck* atau tidak, dimana *fleck* adalah tanda apakah file gambar telah disisipkan pesan

rahasia sebelumnya atau belum. Jika tidak muncul *fleck*, proses *embedding* teks dapat diteruskan atau dilakukan.

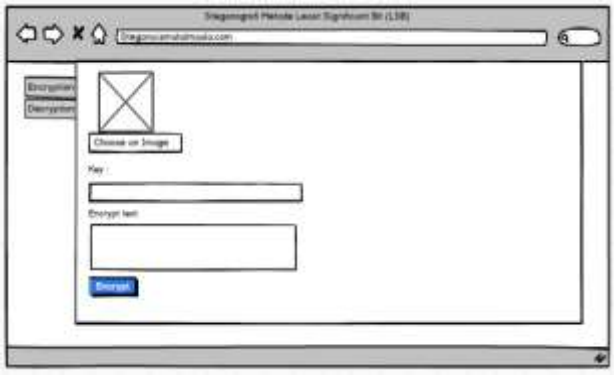
DFD level 1 dari proses 2 (proses ekstraksi pesan) sebagai berikut :



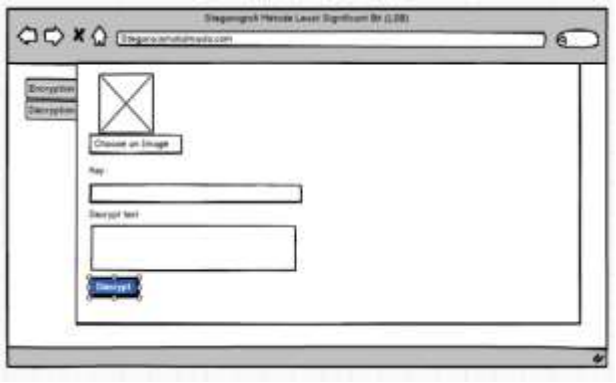
Gambar 7. DFD Level 1 Proses Ekstraksi Pesan

Perancangan Desain Antarmuka

Perancangan desain antarmuka pada sistem ini terdiri dari 2 antarmuka yakni desain antarmuka enkripsi dan desain antar muka dekripsi.



Gambar 8. Desain antarmuka enkripsi



Gambar 9. Desain antarmuka dekripsi

Membangun Prototype

Pada tahap ini penulis melakukan tahap pembangunan dengan melakukan proses penulisan program (*coding*) terhadap hasil rancangan yang sebelumnya sudah didefinisikan dan yang akan dijadikan sistem. Pembuatan sistem ini menggunakan beberapa alat bantu diantaranya XAMPP versi 1.8.2 sebagai *software package* yang di dalamnya sudah termasuk Apache 2.4.7, MySQL 5.5.34, PHP 5.4.22, phpMyAdmin 4.0.9, FileZilla FTP Server 0.9.41, dan Tomcat 7.0.42, Editor Sublime 3 untuk membuat *source code website*.

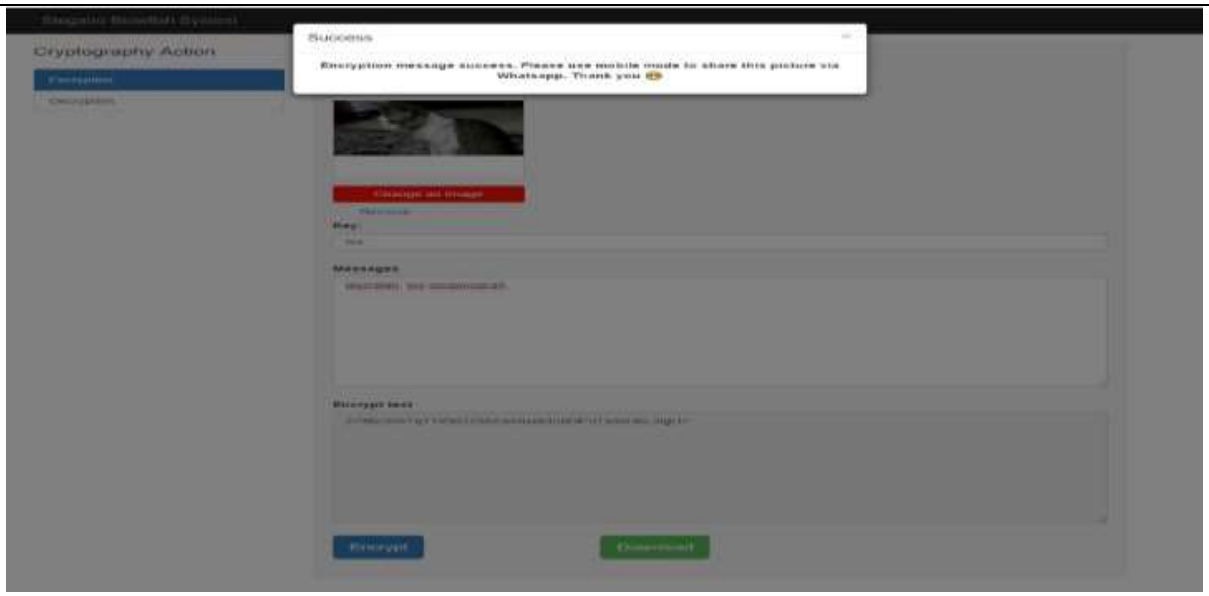
Evaluasi dan Pengujian

Pada tahap ini sistem dilakukan pengujian dengan black box. Pengujian ini ditujukan untuk meyakinkan semua perintah masukan dan keluaran yang dihasilkan sesuai dengan perancangan sebelumnya. Setelah dilakukan pengujian, semua tampilan berhasil lolos pengujian dimana apa yang diinputkan menghasilkan apa yang diharapkan.

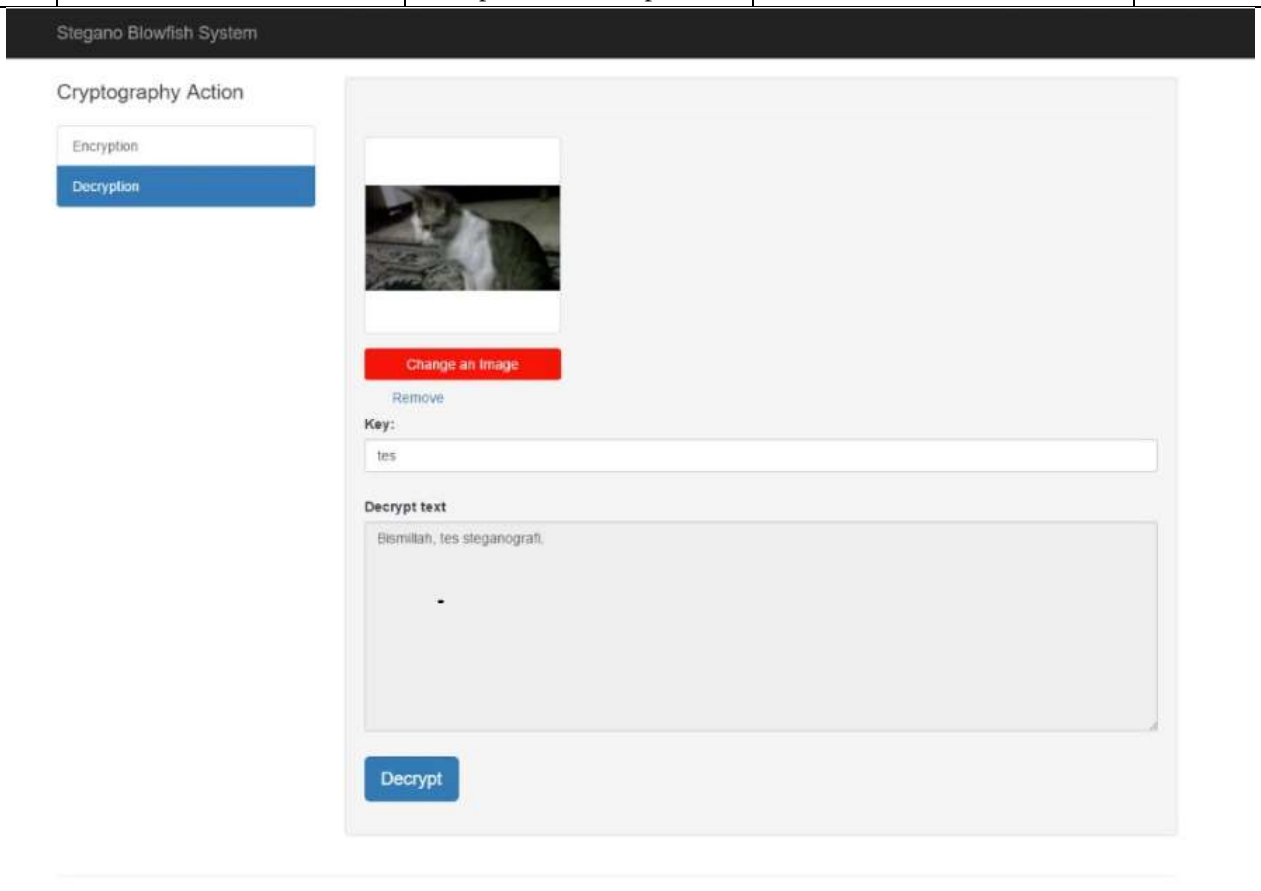
Tabel 1 Hasil Evaluasi dan Pengujian

No	Item Uji	Kegiatan	Hasil yang diharapkan	Ket
1	Enkripsi pesan	Memilih gambar, memasukkan key, dan pesan asli	Dapat menghasilkan pesan yang terenkripsi dengan disisipi gambar yang telah didownload pada proses enkripsi	Valid

P ISSN : 2549-0710
E ISSN : 2722-2713



	Dekripsi pesan	Memilih gambar dari antar muka yang disediakan, memasukkan key dan pesan terenkripsi	Dapat menampilkan pesan asli dan sisipan gambar dari yang telah dipilih	Valid



- **Kesimpulan**

Berdasarkan keseluruhan proses yang dilakukan untuk membangun sistem steganografi mengunakan algoritma Blowfish dan metode LSB ini, dapat disimpulkan bahwa sistem ini telah berhasil dibangun dan dapat berfungsi sesuai tujuan yaitu menyisipkan pesan rahasia ke dalam gambar. Sistem ini juga telah berhasil mengembalikan pesan rahasia dengan menggunakan kunci yang sama sewaktu melakukan enkripsi.

Referensi

Andrian, Y. (2013). Modifikasi Metode Least Significant Bit (LSB) Pada Steganografi Citra Digital. Medan: Seminar Nasional Ilmu Komputer Universitas Methodist Indonesia.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi : Teori, Analisis, dan Implementasi*. Yogyakarta: Andi.

Lou, D. C., & Liu, J. L. (2002). Steganographic method for secure communications. *Computers and Security*, *21*(5), 449–460. https://doi.org/10.1016/S0167-4048(02)00515-1

Monica, F. (2016). Aplikasi Steganografi Citra Digital Menggunakan Metode LSB (Least Significant Bit) Visual Basic 6, (May). https://doi.org/10.13140/RG.2.1.4988.7605

Permana, A, A,. 2017, Aplikasi Penyisipan Teks Pada Gambar dengan Algoritma Blowfish dan Least Significant Bit, JIKA (Jurnal Informatika) Vol 1 No 1, ISSN : 2549-0710.

Springer-Verlag. (1994). Fast Software Encryption, Cambridge Security Workshop Proceedings.

Wardoyo, S., Imanullah, Z., & Fahrizal, R. (2016). Enkripsi dan Dekripsi File dengan Algoritma Blowfish pada Perangkat Mobile Berbasis Android. *Jurnal Nasional Teknik Elektro*, *5*(1), 36. https://doi.org/10.25077/jnte.v5n1.199.2016

William, S. (2011). *Criptography and Network Security": United States of America, Rose Kernan*.