2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)
21 Maret 2023 – Jakarta, Indonesia
Volume 2, Nomor 1, April 2023 - ISSN 2962-8628 (*online*)

IMPLEMENTASI *STEGANOGRAPHY* DENGAN METODE LSB PADA PT SAMASEDIA JASA TEKNOLOGI

Abiyu Almer Bahy[1*], Imelda[2], Mardi Hardjianto[3], Sejati Waluyo[4]

[1,2,3,4]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta, Indonesia

Email:[1*]abiyualmer11@gmail.com, [2]imelda@budiluhur.ac.id, [3]mardi.hardjianto@budiluhur.ac.id, [4]sejati.waluyo@budiluhur.ac.id
(* : *corresponding author*)

Abstrak- Ketika data tersimpan pada sistem komputer, jaringan komputer atau bahkan internet, kerahasiaan data menjadi sangat penting baik untuk organisasi maupun untuk pribadi. Kebutuhan untuk memastikan keamanan dan kerahasiaan data saat ini sangat tinggi karena kejahatan seperti pembajakan atau pencurian data semakin marak. Salah satu solusi guna terjaganya data adalah dengan menggunakan steganografi. Di PT. Samasedia Jasa Teknologi, data pada file laporan masih rentan terhadap akses oleh orang yang tidak berkepentingan karena masih disimpan secara umum. Oleh karena itu, data perlu disembunyikan dengan menggunakan steganografi sehingga hanya orang yang berkepentingan yang dapat mengaksesnya. Peningkatan keamanan file laporan dengan kombinasi algoritma steganografi menjamin keamanan data terhadap serangan yang dapat merusak isi data yang disimpan. Salah satu algoritma steganografi yang digunakan adalah LSB, yang memungkinkan perlindungan file gambar lebih efektif. Teknik *Least Significant Bit* dapat digunakan untuk menyembunyikan data pada citra yang diinginkan dengan menambahkan bit-bit data pada bit-bit citra digital sehingga bit-bit data tersebut tersembunyi di dalam bit-bit citra digital. Dengan menggunakan metode steganography dan *least significant bit*, data dapat disembunyikan kemudian diambil kembali sehingga dapat dibaca oleh pemilik data tersebut. Pada PT. Samasedia Jasa Teknologi metode yang steganography sudah dapat digunakan sebagai perlindungan file yang di sembunyikan ke dalam sebuah *cover image.*

Kata Kunci: Steganografi, LSB, Keamanan File.

THE IMPLEMENTATION OF FILE SECURITY USING STEGANOGRAPHY WITH LSB METHOD AT PT SAMASEDIA JASA TEKNOLOGI

Abstract- *When data is stored on computer systems, computer networks or even the internet, data confidentiality becomes very important for both organizations and individuals. The need to ensure data security and confidentiality is currently very high because crimes such as piracy or data theft are increasingly prevalent. One solution for data preservation is to use steganography. At PT Samasedia Jasa Teknologi, the data in the report file is still vulnerable to access by unauthorized persons because it is still stored in general. Therefore, the data needs to be hidden using steganography so that only interested people can access it. Increasing the security of report files with a combination of steganography algorithms ensures data security against attacks that can damage the contents of the stored data. One of the steganography algorithms used is LSB, which allows for more effective protection of image files. The least significant bit technique can be used to hide data in the desired image by adding data bits to the digital image bits so that the data bits are hidden in the digital image bits. By using steganography and least significant bit methods, data can be hidden and then retrieved so that it can be read by the owner of the data. At PT. Samajadi Jasa Technology, the steganography method can already be used to protect files that are hidden in a cover image.*

Keywords*: Steganography, LSB, Security File.*

1. PENDAHULUAN

Informasi penting tentang seseorang atau perusahaan, apakah itu laporan rahasia perusahaan, strategi bisnis rahasia perusahaan, atau sejarah perusahaan [1]. Oleh karena itu, keamanan pesan diperlukan agar pesan rahasia tidak dapat dengan mudah sampai ke pihak lain yang berkepentingan [2]. Penelitian ini membahas tentang steganografi menggunakan medote LSB (*Least Significant Bit*) untuk mengamankan file pada PT Samasedia Jasa Teknologi. Salah satu teknik paling populer untuk menyembunyikan informasi adalah steganografi.[3] Teknik ini mengelabui penyadap data untuk melindungi informasi sensitif. Steganografi dapat digunakan dengan menerapkan beberapa algoritma dengan bantuan pemrosesan komputer [4].

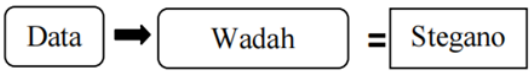
Steganografi adalah ilmu yang mempelajari teknik dan cara penyembunyian pesan rahasia pada suatu file, sehingga pihak yang tidak bertanggung jawab tidak dapat melihat pesan rahasia tersebut dan tidak tahu keberadaannya[5]. Salah satu metode steganografi yaitu LSB (*Least Significant Bit*) [6]. Masalah yang ada pada PT Samasedia Jasa Teknologi yaitu file masih disimpan pada Google Drive sehingga sangat rawan disalin dan

disebarluaskan oleh pihak yang tidak berwenang [7]. Berbeda dengan penelitian sebelumnya, penelitian ini memiliki solusi pengamanan file menggunakan steganografi. Keunikan penelitian ini pengamanan filenya disembunyikan di dalam pesan. Metode penelitian yang digunakan adalah LSB (*Least Significant Bit*) [8]. Alasan menggunakan metode LSB dikarenakan lebih baik dari segi kualitas, LSB (*Least Significant Bit*) memasukan bit data tersembunyi (pesan) ke bit terakhir.[9] Berkat metode menambahkan pesan, Lakukan penyimpanan data menggunakan file bit 'file'; yang tidak memiliki arti untuk bit file yang ada [10].

2. METODE PENELITIAN

2.1 Data Penelitian

Pada penelitian saat ini, yaitu pengamanan file menggunakan steganografi dengan metode LSB (*Least Significant Bit).* Pada pengamanan *file* ini dilakukan menggunakan steganografi yaitu berupa file laporan yang akan disisipkan pada sebuah gambar sebagai wadah untuk steganografi yang memiliki alur singkat seperti pada gambar 1.

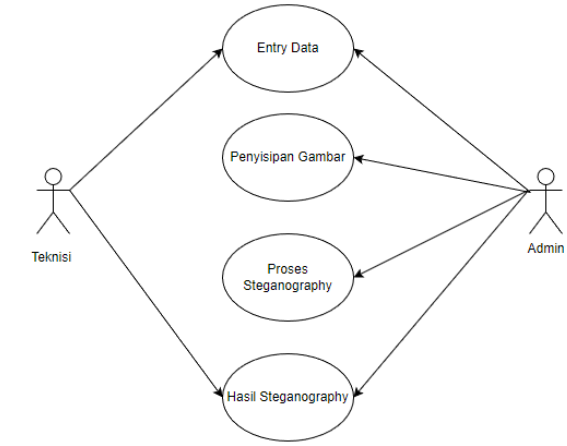


Gambar 1. Alur Steganografi

Pada gambar 1 menampilkan alur sederharana pada proses steganografi, data yang dimaksud adalah file yang akan di sisipkan, sedangkan wadah adalah *cover image* yang akan digunakan sebagai gambar yang akan di sisipkan file tersebut.

2.2 Penerapan *Use Case Diagram*

Use case diagram adalah diagram hubungan yang menggambarkan pengguna dan sistem. Setiap *use case* diagram memiliki atribut seperti pengguna, *use case*, dan relasi. memiliki diagram kasus penggunaan fungsi yang mendefinisikan fungsi-fungsi yang termasuk dalam sistem dan aliran yang digunakan oleh pengguna.



Gambar 2. Use Case Diagram

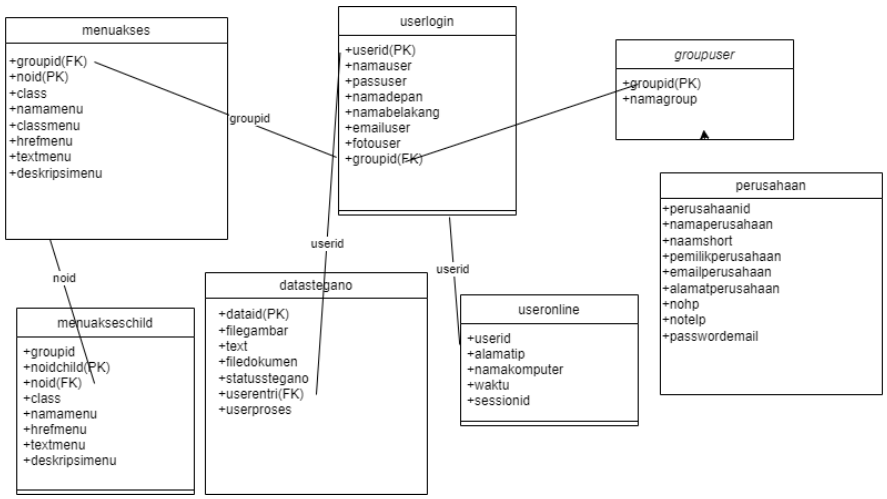
Pada gambar 2 mempunyai 2 pengguna yaitu, teknisi dan admin. Pada 2 pengguna tersebut memiliki masing-masing fitur yang bisa digunakan pada sistem yaitu, teknisi dapat melakukan *entry data* dan melihat hasil steganografi, sedangkan admin dapat melakukan *entry data*, penyisipan gambar, memproses steganografi dan melihat hasil steganografi.

2.3 Rancangan Pengujian

Pada pengujian ini, akan dilakukannya pengujian guna mengetahui telah berjalan dengan baik dan sesuai harapan. Untuk melakukan pengujian pada penelitian ini menggunakan metode *Mean Square Error, Mean Square Error* digunakan untuk mencari nilai *error* rata-rata diantara *cover image* dengan *stego image.*

2.4 Rancangan Basis Data

Rancangan basis data pada website aplikasi steganografi digambarkan dengan menggunakan LRS (*Logical Record Structure)* seperti pada gambar 3 yang menghasilkan menuakses, userlogin, groupuser, menuakseschild, data stegano, useronline, perusahaan.



Gambar 3. Rancangan Basis Data

3. HASIL DAN PEMBAHASAN

Pada penelitian yang telah dilakukan didapatkan hasil implementasi metode dan hasil pengujian menggunakan *mean square error* sebagai berikut:

3.1 Lingkungan Percobaan (Spesifikasi *Hardware* dan *Software*)

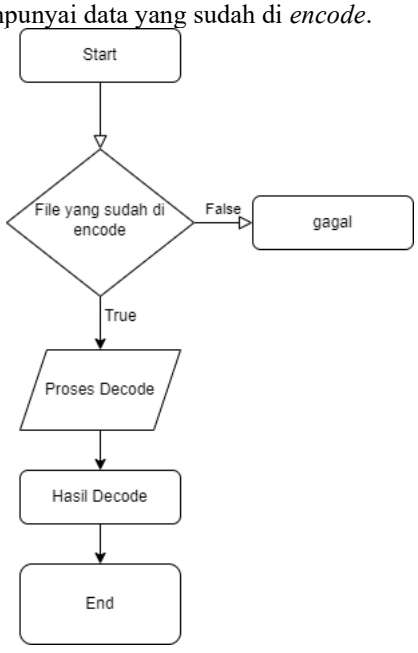
a. Spesifikasi *Hardware* dan *Software*

Berikut merupakan spesifikasi *hardware* yang digunakan adalah Processor dengan spesifikasi AMD ® Ryzen™ 5 4500U, RAM 8 GB, SSD 500 GB, VGA AMD Radeon Graphics. Spesifikasi *Software* diantaranya Sistem Operasi Windows 11, Bahasa Pemrogramana Utama dengan HTML 5, PHP, IDE Visual Studio Code, MySQL MariaDB, Google Chromer, XAMPP v3.3.0

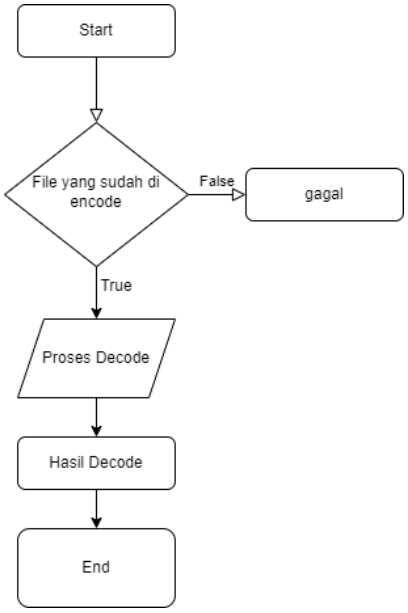
3.2 *Flowchart*

a. *Flowchart Encode dan Decode*

Flowchart yang ditunjukan pada gambar 4 merupakan *flowchart encode* yang dimana proses *encode* terjadi ketika data sudah di entri jika data belum di entri, maka proses *encode* akan gagal. *Flowchart* yang ditunjukan pada gambar 5 merupakan *flowchart decode* yang dimana pada proses *decode* hanya bisa dilakukan jika mempunyai data yang sudah di *encode*.



Gambar 4. *Flowchart Encode*



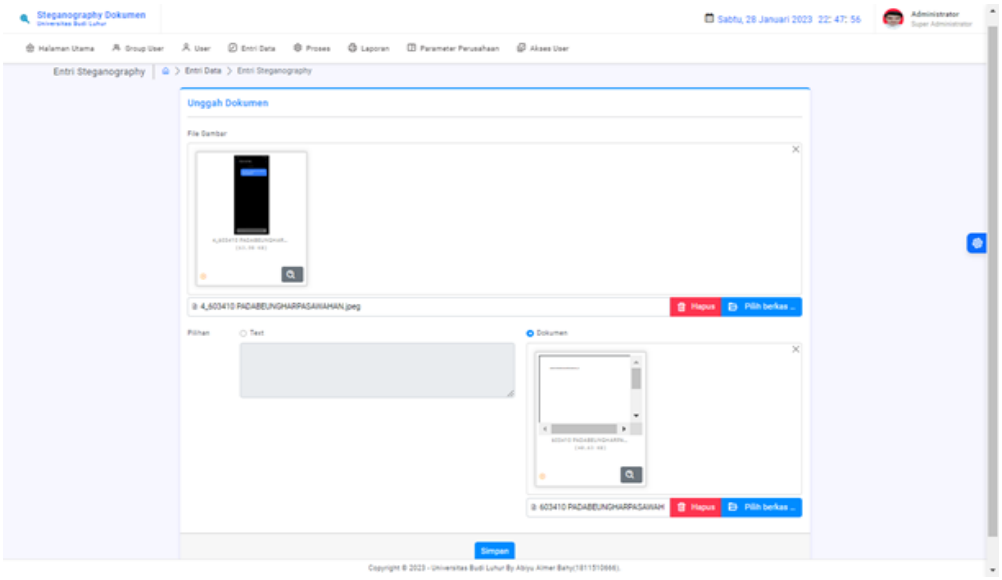
Gambar 5. *Flowchart Decode*

3.3 Implementasi Metode

Berdasarkan penerapan metode pada penelitian ini, berikut adalah implementasi pada website yang sudah dibuat.

a. Entri Data *Encode*

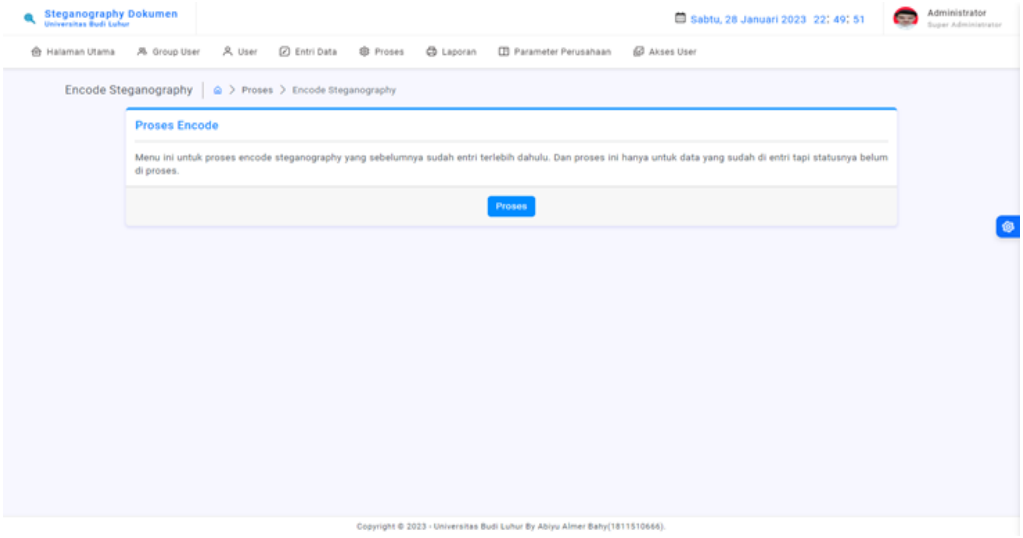
Pada gambar 6 menampilkan entri data berupa cover image dan dokumen yang akan di encode. Cover image yang digunakan pada poses steganogrfi harus lebih besar ukurannya daripada dokumen yang akan di Steganografi.



Gambar 6. Entri Data *Encode*

b. Proses Encode

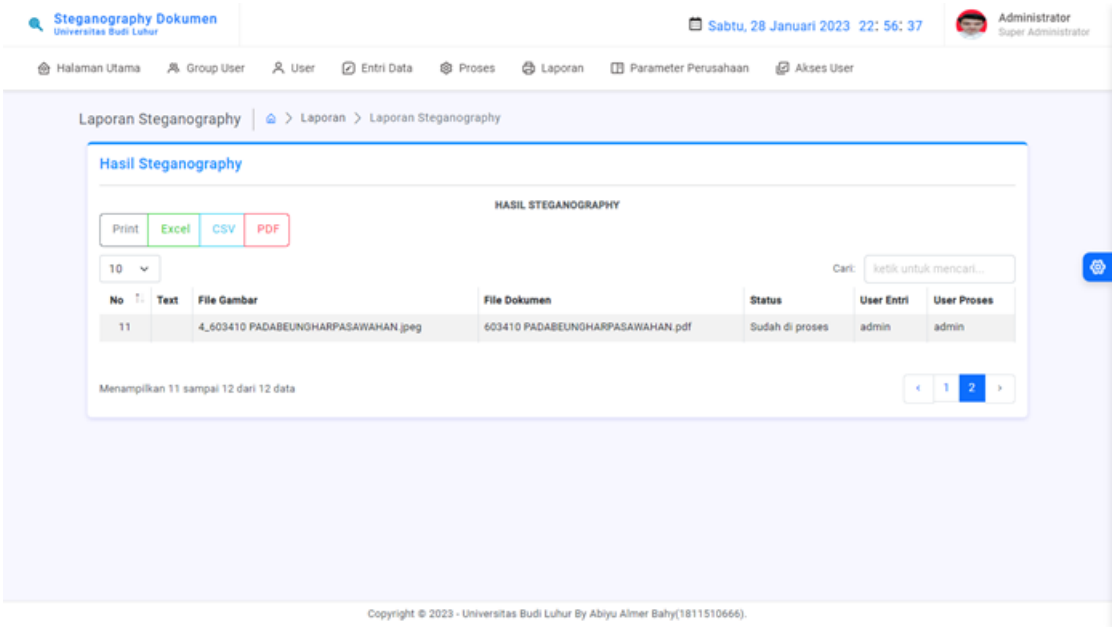
Pada gambar 7 menampilkan proses encode steganografi dari data yang sudah di entri. Jika data belum di entri, maka proses encode tidak akan berjalan.



Gambar 7. Proses Encode

c. Hasil *Encode*

Pada gambar 8 menampilkan menu hasil, yaitu menampilkan list data yang sudah diproses steganografi. Hasil encode adalah hasil dari data yang sudah disisipkan kedalam cover image.



Gambar 8. Hasil Encode

3.4 Hasil Pengujian

Pada pengujian ini dilakukan pengujian untuk dapat mengetahui apakah metode pada penelitian ini terjadi *error* atau tidak. Tabel 1 adalah tabel hasil pengujian dari metode LSB pada aplikasi website yang sudah dibuat. Berikut adalah hasil pengujian menggunakan MSE(*mean square error*), dari masing-masing file yang sudah di proses steganografi memiliki nilai MSE.

Tabel 1. Hasil Pengujian

No	Nama *Image*	MSE
1	1_101234 PINANGRAJA	0.10353160770691773
2	2_104706 MAJALENGKA_MJL1_MT	0.1460770136310534
3	3_602410 SEIMPEREUM	0.058826157149033366
4	4_603410 PADABEUNGHARPASAWAHAN	0.04049981825225179
5	5_603428 PAJAJAR	0.029342054094179622

4. KESIMPULAN

Setelah melakukan pengujian dan evaluasi mengenai website aplikasi pengamanan dokumen steganografi menggunakan metode LSB didapatkan kesimpulan sebagai berikut: Steganografi dapat digunakan untuk mengamankan dokumen dan dapat mengembalikan dokumen seperti semula, dengan adanya Steganografi dengan metode LSB yang berbasis webite dapat mengamankan file dokumen laporan maupun file dokumen lainnya. penulis membuat website pada penelitian ini untuk digunakan sebagai salah satu cara mengamankan data atau file perusahaan yang penting. setelah adanya website ini, penulis berharap kepada pembaca dan masyarakat untuk meningkatkan kesadaran dalam menyimpan dan menjaga dokumen agar tidak hilang atau bocor

DAFTAR PUSTAKA

[1] A. Hafiz, "*Stegnografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant BIT (LSB),*" Jurnal Cendikia, XVII, pp. 194-198, 2019.
[2] K. Hani, "*Alogaritma Kriptografi dan Stegnografi untuk Pengamanan Pesan ke dalam Citra,"* Skripsi, pp. 8-20, 2020.
[3] G. Putra, K. Suhartana, K. Mogi, C. Pramatha, P. Suputra and G. Wibawa, *"Penerapan Stegnography Untuk Perlindungan Hak Cipta Menggunakan Metode Least Significant Bit (LSB),"* Jurnal Elektronik Ilmu Komputer Udayana, 10 (11), pp. 330-338, 2022.
[4] A. Padmanaba, E. Kumalasari and D. Andayati, *"Komparasi Penggunaan Framework Codeigniter Vs PHP Native Pada Sistem Informasi Manajemen Surat Sekretariat DPRD Pemalang,"* Jurnal SCRIPT, 8(1), pp. 1-4, 2020.

[5] D. Rosmala and A. Kusuma, *"Perbandingan Metode Most Significant Bit dan Least Significant Bit Pada Stegnografi untuk Keamanan Data Media Digital,"* MIND Journal, 3(2), pp. 36-46, 2018.
[6] K. D. R. Sianipar, L. C. Purba, S. W. Siahaan, I. Gunawan and S. , *"Pengamanan File Gambar Menggunakan Fungsi Algoritma Stegnografi LSB dari Serangan Brute Force,"* Jurnal TECHSI, 10(1), pp. 155-162, 2018
[7] . R. Kurniawan and S. Marhamelda, *"Sistem Pengolahan Data Peserta Didik Pada LKP Prima Tama Komputer Dumai Dengan Menggunakan Bahasa Pemrograman PHP,"* Jurnal Informatika, Manajemen, dan Komputer, 11(1), pp. 37-44, 2019.
[8] M. Tabrani, S. and H. Priyandaru, *"Sistem Informasi Managemen Berbasis Website pada UNL Studio dengan Menggunakan Framework Codeigniter,"* Jurnal M-Progress, 11(1), pp. 13-21, 2021.
[9] M. Laliha, S. and N. Ransi, *"Aplikasi Pengamanan File Bertipe *.PDF pada Video *.MP4 Menggunakan Kriptografi Vernam Cipher dan Stegnografi End of File,"* Jurnal semanTIK, 5(1), pp. 158-164, 2019.
[10] C. Jatmoko, B. Handoko, C. A. Sari, D. R. Ignatius and M. Setiadi, *"Performa Penyisipan Pesan dengan Metode LSB dan MSB pada Citra Digital untuk Keamanan Komunikasi,"* Jurnal Dinamika Rekayasa, 14)1), pp. 47-55, 2018.