

# Perancangan Integrasi Sistem Enkripsi dan Steganografi untuk Pengamanan Data Suara Manusia Berbasis Web

A.A Putu Priyamdeva Arya Maheswara<sup>a1</sup>, Gusti Made Arya Sasmita<sup>a2</sup>, A.A Ketut Agung Cahyawan Wiranatha<sup>a3</sup>

<sup>a</sup>Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana  
Bukit Jimbaran, Bali, Indonesia Telp. (0361) 701806

e-mail: <sup>1</sup>[priyamdeva.arya@gmail.com](mailto:priyamdeva.arya@gmail.com), <sup>2</sup>[aryasasmita@unud.ac.id](mailto:aryasasmita@unud.ac.id),  
<sup>3</sup>[agung.cahyawan@unud.ac.id](mailto:agung.cahyawan@unud.ac.id)

## Abstrak

*Steganografi audio pada gambar ialah metode yang digunakan buat menyembunyikan pesan audio secara rahasia dalam gambar. Metode Least Significant Bit (LSB) ini pula dipadukan dengan Advanced Encryption Standard (AES) dalam meningkatkan keamanan pesan yang dirahasiakan. Pesan audio yang hendak dirahasiakan, bisa dienkripsi menggunakan Advanced Encryption Standard (AES) saat sebelum disisipkan ke dalam gambar. Advanced Encryption Standard (AES) bisa dipadukan dengan pemakaian Rivest Shamir Adleman (RSA) pada kunci Advanced Encryption Standard (AES). Rivest Shamir Adleman (RSA) digunakan dalam meningkatkan keamanan pada kunci Advanced Encryption Standard (AES). Kunci Advanced Encryption Standard (AES) bisa dienkripsi menggunakan Rivest Shamir Adleman (RSA) saat sebelum disematkan dalam gambar menggunakan Metode Least Significant Bit (LSB), sehingga hanya penerima yang mempunyai kunci Rivest Shamir Adleman (RSA) yang cocok untuk mengakses pesan audio yang dirahasiakan. Hasil dari pengolahan tersebut bisa dinilai dari angka PSNR (Peak-Signal-to-Noise Ratio).*

**Kata kunci:** *Steganografi, Least Significant Bit, Advanced Encryption Standard, Rivest-Shamir-Adleman, Peak Signal to Noise Ratio*

## Abstract

*Audio steganography on images is a method used to secretly hide audio messages in images. The Least Significant Bit (LSB) method is also combined with Advanced Encryption Standard (AES) to increase the security of confidential messages. Audio messages that you want to keep secret can be encrypted using Advanced Encryption Standard (AES) before being inserted into the image. Advanced Encryption Standard (AES) can be combined with the use of Rivest Shamir Adleman (RSA) on Advanced Encryption Standard (AES) keys. Rivest Shamir Adleman (RSA) is used to increase the security of Advanced Encryption Standard (AES) keys. The Advanced Encryption Standard (AES) key can be encrypted using Rivest Shamir Adleman (RSA) before being inserted into the image using the Least Significant Bit (LSB) Method, so that only recipients who have the Rivest Shamir Adleman (RSA) key are suitable for accessing the audio message. kept secret. The results of this processing can be measured from the PSNR (Peak-Signal-to-Noise Ratio) figure.*

**Keywords :** *Steganography, Least Significant Bit, Advanced Encryption Standard, Rivest-Shamir-Adleman, Peak Signal to Noise Ratio*

## 1. Introduction

Pesatnya kemajuan teknologi menjadikan keamanan komunikasi internet menjadi perhatian penting. Berbagai bentuk komunikasi, seperti telepon, pesan, dan panggilan video, rentan terhadap penyadapan. Upaya mengamankan data suara semakin penting seiring dengan meningkatnya teknologi pengenalan suara, aplikasi suara digital, dan layanan berbasis suara. Privasi, keamanan komunikasi, pengenalan dan autentikasi suara, pencegahan penipuan, dan sistem suara yang aman merupakan aspek utama perlindungan data suara [1].

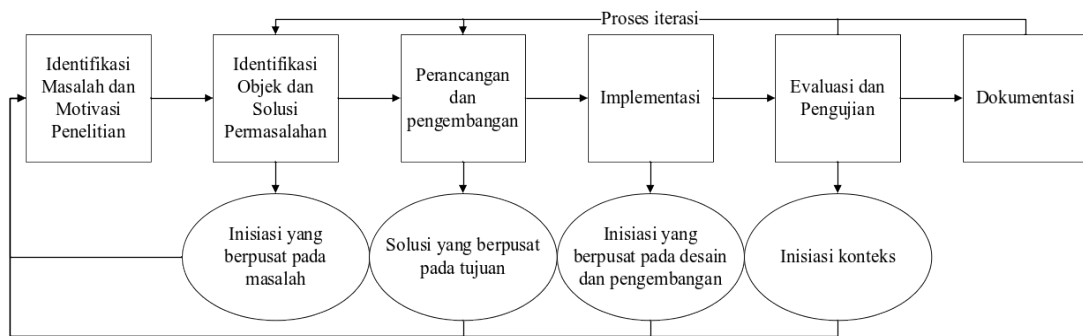
Untuk mengatasi tantangan ini, enkripsi data, protokol keamanan komunikasi, dan praktik keamanan informasi sangatlah penting. Organisasi dan pengembang teknologi suara harus

mematuhi peraturan keamanan dan privasi yang berlaku dan terus meningkatkan teknologi keamanan suara [2].

Pemecahan utama untuk mengamankan informasi suara yaitu dengan penelitian ini. Steganografi menyembunyikan pesan di dalam media lain, sehingga tidak ditemukan. Riset ini berfokus pada keamanan informasi dalam integrasi sistem enkripsi serta steganografi, khususnya penyisipan pesan dalam *format audio* MP3 ke dalam file gambar PNG dengan tata cara *Least Significant Bit* (LSB), *hash*, kompresi, *Advanced Encryption Standard* (AES), serta *Rivest Shamir Adleman* (RSA). Tujuannya merupakan buat membuat aplikasi secara *open source* untuk pengguna semacam detektif swasta ataupun petugas intelijen yang tidak sanggup membeli aplikasi handal. Riset ini bertujuan buat membagikan pemecahan yang bisa diterapkan secara luas, tercantum pada pengajuan pinjaman *online* memakai verifikasi suara.

## 2. Research Method

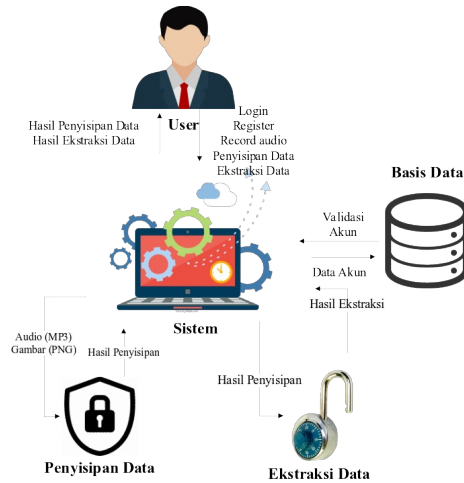
Metodologi riset ialah tahapan bawah yang dicoba dalam sesuatu riset dengan tujuan agar proses riset bisa terlaksana dengan lebih tertib, sistematis, terkontrol serta terencana. Metodologi ini mempunyai 6 tahapan yang bisa dilihat pada Gambar 1.



Gambar 1 Metodologi Riset

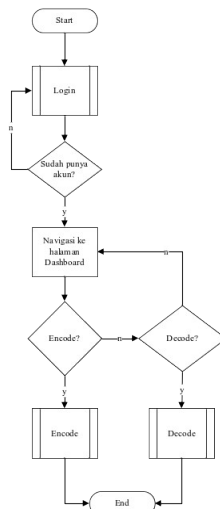
Gambar 1 menguraikan tahapan dari metodologi riset. Tahapan ini digunakan untuk memperbaiki atau mengembangkan sistem baru.

1. Identifikasi Permasalahan: Langkah ini bertujuan untuk mengidentifikasi masalah komunikasi pesan suara yang disadap oleh orang lain, yang dapat mengakibatkan penyalahgunaan informasi penting.
2. Identifikasi Objek dan Solusi Masalah: Tahap ini meliputi analisis studi literatur untuk menentukan tujuan dan arah penelitian, serta menemukan solusi baru.
3. Perancangan dan Pengembangan: Perancangan sistem dilakukan untuk membuat model sementara dari sistem yang akan dirancang, meliputi gambaran umum, perancangan basis data, dan perancangan antarmuka.
4. Demonstrasi (Implementasi): Hasil sistem didemonstrasikan untuk mendapatkan saran perbaikan.
5. Evaluasi dan Pengujian: Tahap ini bertujuan untuk mengetahui fungsionalitas sistem dan kemampuan pemecahan masalah, serta mengukur kemampuannya dalam memenuhi keinginan pengguna. Pengujian dilakukan dengan menggunakan pengujian *black box*.
6. Komunikasi: Hasil penelitian yang telah selesai didokumentasikan melalui laporan atau publikasi di jurnal [3].



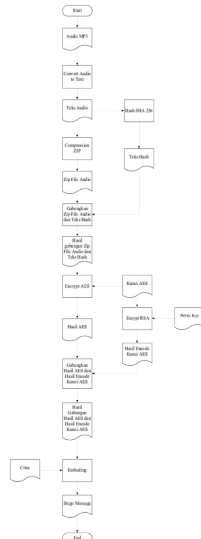
Gambar 2 Gambaran Umum

Gambar 2 merupakan gambaran umum dari Perancangan Integrasi Sistem Enkripsi dan Steganografi untuk Pengamanan Data Suara Manusia Berbasis Web. Pengguna dapat mendaftar untuk sebuah akun, atau masuk jika sudah memilikinya. Sistem memeriksa keberadaan akun di *database*, setelah login, pengguna dapat melakukan *encode* dan *decode* data, untuk memasukkan data *audio* ke dalam gambar, pengguna harus *input file audio* MP3 dan gambar PNG, jika tidak ada data *audio*, pengguna dapat merekam *audio*. Hasil proses penyisipan dapat disimpan. Pengguna yang ingin mengekstrak data *audio*, pengguna harus memasukkan *file* sisipan yang telah disisipkan sebelumnya. Hasil proses ekstraksi juga bisa disimpan.



Gambar 3 Diagram Alur Sistem

Gambar 3 merupakan diagram alur utama Perancangan Integrasi Sistem Enkripsi dan Steganografi untuk Pengamanan Data Suara Manusia Berbasis Web. Prosesnya dimulai dengan pengguna diminta untuk login, jika pengguna tidak memiliki akun, mereka akan diminta untuk mendaftar, yang tersedia saat login. Pengguna setelah login berhasil, pengguna akan diarahkan ke Halaman Dashboard. Pengguna dapat memilih untuk *Encode* atau *Decode* data. Pengguna yang memilih opsi *encode*, mereka akan diminta untuk memilih menu *encode*, sebaliknya, jika pengguna ingin melakukan *decode*, maka pengguna akan diminta untuk memilih menu *decode*.



Gambar 4 Diagram Alur Proses Encode

Gambar 4 merupakan diagram alur proses *encode* dari Perancangan Integrasi Sistem Enkripsi dan Steganografi untuk Pengamanan Data Suara Manusia Berbasis Web. Proses diawali dari pengguna yang berhasil login. Pengguna dapat memasukkan data dengan memilih menu *encode*, dan memasukkan pesan *audio* rahasia dalam bentuk MP3 dan gambar PNG sebagai *cover*. Sistem mengubah pesan *audio* menjadi teks, mengompresnya melalui ZIP, dan melakukan *hashing* menggunakan SHA256. Hasil kompresi dan *hashing* digabungkan dan dienkripsi menggunakan *Advanced Encryption Standard* (AES). Kunci AES diamankan menggunakan *Rivest-Shamir-Adleman* (RSA) dan dilakukan kombinasi menjadi hasil enkripsi AES. Hasil ini melanjutkan proses penyisipan. Data pesan dilakukan *embedding* ke dalam gambar menggunakan Metode *Least Significant Bit* (LSB). Sistem menghasilkan *file* yang sudah diproses dan diberikan kepada pengguna dalam bentuk gambar PNG, yang menunjukkan proses penyisipan berhasil.



Gambar 5 Diagram Alur Proses Decode

Gambar 5 merupakan diagram alur proses *decode* dari Perancangan Integrasi Sistem Enkripsi dan Steganografi Untuk Pengamanan Data Suara Manusia Berbasis Web. Proses diawali dari pengguna yang berhasil login. Pengguna yang ingin ekstrak data dapat memilih menu *decode* lalu menginput *file* berisi pesan rahasia berupa *audio* dalam format gambar PNG. Proses *decoding* dimulai dengan ekstraksi data menggunakan Metode *Least Significant Bit* (LSB) sebagai menghilangkan *audio* rahasia dari citra, jika ada pesan, sistem akan memverifikasi kuncinya, jika dekripsi *Rivest-Shamir-Adleman* (RSA) berhasil, sistem akan melakukan *decrypt* kunci *Advanced Encryption Standard* (AES), menghasilkan kunci AES. Proses jika *decrypt* RSA gagal, maka hasil enkripsi AES tidak dapat di *decode*. *Decode* AES menghasilkan serangkaian gabungan *file* ZIP, termasuk *hashing* dan teks *audio*. *File* tersebut dipisah sehingga ekstraksi *file* dapat terjadi dan menghasilkan teks *audio*. Teks audio ini kemudian diubah menjadi *file audio* dengan mengubah teks menjadi *audio*.

### 3. Result and Discussion

Sistem yang telah dirancang perlu diuji. Pengujian merupakan tahapan yang penting karena dengan melakukan pengujian maka perancang sistem akan mengetahui letak kesalahan pada proses *input*, proses data, *output*, dan lain-lain. Pengujian sistem mencakup bagaimana sistem melakukan fungsi-fungsi yang dirancang sebelumnya [4].

#### 3.1. Steganography System Testing

Pengujian sistem steganografi digunakan untuk melihat keberhasilan aplikasi dalam menyisipkan pesan *file audio* ke dalam *cover image* dan mengekstrak pesan *file audio* dari *stego-image*. Pengujian *encoding* merupakan aspek kualitas gambar hasil steganografi dengan mencari kualitas gambar pada PSNR (*Peak-Signal-to-Noise-Ratio*). Pengujian pertama yang dilakukan adalah pengolahan pesan *stego* berupa *file audio* yang dilakukan menggunakan *voice note* dengan *default sample rate* 11025 Hz, 22050 Hz dan 44100 Hz [5].

Tabel 1 Encode Audio

Nama File Audio	Frekuensi (Hz)	Size	Ukuran Audio Setelah Melalui Covert Teks, Hash, dan ZIP	Ukuran Audio Setelah Encrypt AES dan RSA
Audio_1.MP3	11025 Hz	127 KB	124 KB	221 KB
Audio_2.MP3	22050 Hz	213 KB	209 KB	372 KB
Audio_3.MP3	44100 Hz	245 KB	243 KB	431 KB

Tabel 1 merupakan hasil pengujian *encode audio*, dimana pengujian ini menggunakan total 3 *audio* dengan 3 jenis frekuensi (Hz), antara lain frekuensi 11025 Hz, frekuensi 22050 Hz, dan frekuensi 44100 Hz. Pengujian yang dilakukan adalah mengukur ukuran *audio* setelah *hashing* dan kompresi serta setelah *Advanced Encryption Standard* (AES) dan *Rivest Shamir Adleman* (RSA).

Tabel 2 Encode Audio ke Gambar

Gambar dengan Resolusi 1920 X 1080	Ukuran (KB)	Pesan <i>Audio</i>	Ukuran Pesan <i>Audio</i> Sebelum <i>Encoding</i> (KB)	Ukuran Pesan <i>Audio</i> Setelah <i>Encoding</i> (KB)	Ukuran <i>Stego-Image</i> (MB)	PSNR
	2,29 MB	Audio_1.MP3	127 KB	221 KB	2,63 MB	56 dB
	2,29 MB	Audio_2.MP3	213 KB	372 KB	2,69 MB	53 dB
	2,29 MB	Audio_3.MP3	245 KB	431 KB	2,72 MB	53 dB

Tabel 2 merupakan hasil pengujian untuk *encode audio* ke gambar, dimana pengujian ini menggunakan *audio* yang telah di *encode* sebelumnya. Pengujian yang dilakukan adalah *encode audio* ke dalam gambar. Hal yang diukur adalah perbandingan ukuran *file stego image* dan *cover*

*image* serta mengukur nilai *Peak Signal to Noise Rasio*. *Stego image* juga dapat dilakukan *decode* sehingga menghasilkan *audio*. *Audio* yang dihasilkan sama persis dengan *audio* yang dimasukkan sebelumnya [6].

Tabel 3 Pengujian Steganografi di Sosial Media

<b>Fungsional</b>	<b>Skenario</b>	<b>Hasil</b>	<b>Keterangan</b>
<i>Decode</i> menggunakan gambar yang dikirim melalui aplikasi Messenger	Citra yang sudah di <i>embedding</i> kemudian dikirim melalui aplikasi Messenger ke penerima. Penerima melakukan perubahan nama <i>file</i> kemudian mengirim ke pengirim	Citra yang sudah dilakukan perubahan nama <i>file</i> oleh penerima bisa dilakukan <i>decode</i> oleh pengirim	Sukses <i>decode</i>
<i>Decode</i> menggunakan gambar yang dikirim melalui aplikasi Whatsapp	Citra yang sudah di <i>embedding</i> kemudian dikirim melalui aplikasi Whatsapp ke penerima. Penerima melakukan perubahan nama <i>file</i> kemudian mengirim ke pengirim	Citra yang sudah dilakukan perubahan nama <i>file</i> oleh penerima tidak bisa dilakukan <i>decode</i> oleh pengirim	Gagal <i>Decode</i>
<i>Decode</i> menggunakan gambar yang dikirim melalui aplikasi Telegram	Citra yang sudah di <i>embedding</i> kemudian dikirim melalui aplikasi Telegram ke penerima. Pengirim mengirim citra tersebut melalui Telegram dengan pilihan " <i>Send in a quick away</i> ". Penerima melakukan perubahan nama <i>file</i> kemudian mengirim ke pengirim	Citra yang sudah dilakukan perubahan nama <i>file</i> oleh penerima tidak bisa dilakukan <i>decode</i> oleh pengirim	Gagal <i>Decode</i>
<i>Decode</i> menggunakan gambar yang dikirim melalui aplikasi Telegram	Citra yang sudah di <i>embedding</i> kemudian dikirim melalui aplikasi Telegram ke penerima. Pengirim mengirim citra tersebut melalui aplikasi Telegram dengan pilihan " <i>Send without compression</i> ". Penerima melakukan perubahan nama <i>file</i> kemudian mengirim ke pengirim	Citra yang sudah dilakukan perubahan nama <i>file</i> oleh penerima bisa dilakukan <i>decode</i> oleh pengirim	Sukses <i>decode</i>
<i>Decode</i> menggunakan gambar yang dikirim melalui aplikasi Gmail	Citra yang sudah di <i>embedding</i> kemudian dikirim melalui aplikasi Gmail ke penerima. Penerima melakukan	Citra yang sudah dilakukan perubahan nama <i>file</i> oleh penerima bisa dilakukan <i>decode</i> oleh pengirim	Sukses <i>decode</i>


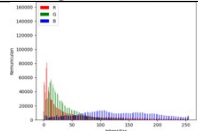
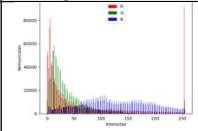
	perubahan nama <i>file</i> kemudian mengirim ke pengirim		
<i>Decode</i> menggunakan gambar yang dikirim melalui aplikasi Line	Citra yang sudah di <i>embedding</i> kemudian dikirim melalui aplikasi Line ke penerima. Pengirim mengirim citra tersebut melalui aplikasi Line tanpa menggunakan opsi <i>original</i> . Penerima melakukan perubahan nama <i>file</i> kemudian mengirim ke pengirim	Citra yang sudah dilakukan perubahan nama <i>file</i> oleh penerima tidak bisa dilakukan <i>decode</i> oleh pengirim	Gagal <i>decode</i>
<i>Decode</i> menggunakan gambar yang dikirim melalui aplikasi Line	Citra yang sudah di <i>embedding</i> kemudian dikirim melalui aplikasi Line ke penerima. Pengirim mengirim citra tersebut melalui aplikasi Line dengan menggunakan opsi <i>original</i> . Penerima melakukan perubahan nama <i>file</i> kemudian mengirim ke pengirim	Citra yang sudah dilakukan perubahan nama <i>file</i> oleh penerima bisa dilakukan <i>decode</i> oleh pengirim	Sukses <i>decode</i>


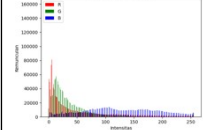
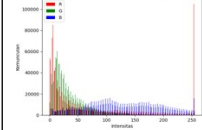

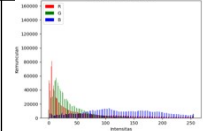
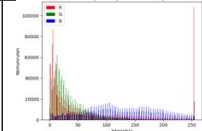
Tabel 3 merupakan tabel proses pengujian steganografi pada Perancangan Integrasi Sistem Enkripsi dan Steganografi Untuk Pengamanan Data Suara Manusia Berbasis Web. Pengujian ini dilakukan dengan mengirimkan hasil *encode* ke aplikasi sosial media seperti Messenger, Gmail, Line, Whatsapp dan Telegram. Pengujian ini dilakukan dengan mengirimkan hasil *encode* kepada penerima, kemudian penerima mengubah nama *file*, kemudian mengirimkannya kembali menggunakan aplikasi dan opsi yang sama. Hasil pengujian ini menunjukkan *decoding* berhasil dan *decoding* gagal. Aplikasi yang berhasil melakukan *decode* antara lain Gmail, Messenger, Telegram, dan Line dengan opsi tanpa kompresi/file asli. Aplikasi yang gagal *decode* adalah WhatsApp, Telegram, Line dengan opsi *send in a quick away* [7].

### 3.2. Analysis

Histogram merupakan grafik yang menampilkan jumlah piksel pada sesuatu gambar pada tiap nilai keseriusan berbeda yang ada pada foto tersebut. Analisis histogram ini menggunakan perbedaan histogram piksel (PHD). PHD merupakan salah satu teknik evaluasi parameter citra, tekniknya dengan mengambil perbedaan antara gambar lama dan gambar sisipan.

Tabel 4 Histogram

Gambar 1920X1080	PNG	Audio MP3	Histogram Cover Image	Histogram Stego- Image
		Audio_1.MP3		

	Audio_2.MP3		
	Audio_3.MP3		

Tabel 4 merupakan hasil analisis histogram. Hasil analisis ini menunjukkan perbandingan histogram setiap gambar sebelum dan sesudah dilakukan *encode audio*. Terlihat pada tabel diatas bahwa histogram *stego image* jika dilihat secara detail menunjukkan perubahan bentuk grafik. Perbedaan ini dipicu oleh proses penyisipan karakter pesan ke dalam bit yang menyebabkan pikselnya berubah, semakin banyak karakter yang dimasukkan, grafik histogram akan semakin berubah [8].

Pengujian yang telah dilakukan melalui *encode* dan *decode* memperoleh hasil yang bervariasi untuk setiap *file*. Hasil yang telah diperoleh pada pengujian steganografi dapat dianalisis lebih lanjut menunjukkan bahwa ukuran *file stego image* bertambah karena penggunaan penyisipan *Least Significant Bit* (LSB) pada setiap piksel gambar memerlukan penghilangan bitmap mentah dari *file* gambar PNG, lalu memodifikasinya dan membuat *file* baru dengan data bitmap yang baru dan memungkinkan tidak semua bitmap dikompresi semudah gambar lama (*cover image*) [9]. Resolusi gambar hasil proses *encode* tidak mengalami perubahan, namun ukuran gambar jika dilihat dari gambar lama (*cover image*) dan gambar hasil *encode* (*stego image*) mempunyai ukuran yang berbeda. Hal ini juga mempengaruhi perbedaan ukuran *audio* saat diekstraksi.

Pengujian yang dilakukan melalui skenario steganografi memperoleh hasil yang beragam. Hasil yang diperoleh pada skenario steganografi dapat dianalisis lebih lanjut untuk menunjukkan bahwa kompresi sangat berpengaruh ketika bertukar pesan melalui media sosial.

Tabel 5 Imperceptibility

Apakah kedua gambar berikut sama?		Iya	Tidak
		11	
		11	

Tabel 5 merupakan pengujian *imperceptibility* yang artinya tidak terdeteksi pesan pada *stego image*. Terlihat dari kuesioner membuktikan bahwa gambar *stego* tidak terdeteksi oleh mata manusia.

#### 4. Conclusion

1. Perancangan Sistem Integrasi Enkripsi dan Steganografi untuk Pengamanan Data Suara Manusia Berbasis Web telah berhasil diterapkan pada penelitian ini. Proses perancangan



meliputi pembuatan *database* sistem dan diagram alur, dilanjutkan dengan pembuatan sistem berbasis *web* sesuai desain yang dibuat.

2. Hasil pengujian menghasilkan aplikasi yang mampu melakukan penyisipan dan ekstraksi data, dilengkapi dengan fitur *login*, *register*, dan *record*. Gambar yang digunakan untuk menyisipkan *audio* mempunyai nilai PSNR (*Peak-Signal-to-Noise- Ratio*) yang tinggi, yang menunjukkan kemiripan yang erat antara hasil rekonstruksi dengan gambar aslinya, yaitu tidak kurang dari 30 dB. Hal ini membuatnya tidak mungkin menimbulkan kecurigaan dari orang lain.

## References

- [1] Alifi, M. B., & Suartana, I. M. (2020). *Implementasi Teknik Steganografi pada Gambar JPEG dan PNG dengan menggunakan Metode Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR)*. 02, 113–119.
- [2] Darnita, Y., Khairunnisyah, K., & Mubarak, H. (2019). Kompresi Data Teks Dengan Menggunakan Algoritma Sequitur. *Sistemasi*, 8(1), 104. <https://doi.org/10.32520/stmsi.v8i1.429>
- [3] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3), 45–77. <https://doi.org/10.2753/MIS0742-122240302>
- [4] Giovani, A. C., Wahyu Utami, Y. R., & Susyanto, T. (2019). STEGANOGRAFI PADA CITRA BITMAP MENGGUNAKAN METODE LEAST SIGNIFICANT BIT BERSILANG UNTUK TEKS TERENKRIPSI BASE64. *Jurnal Ilmiah SINUS*, 17(1), 73. <https://doi.org/10.30646/sinus.v17i1.384>
- [5] Hutapea, D. Y., & Hutapea, O. (2018). Watermarking Method of Remote Sensing Data Using Steganography Technique Based on Least Significant Bit Hiding. *International Journal of Remote Sensing and Earth Sciences (IJReSES)*, 15(1), 63. <https://doi.org/10.30536/j.ijreses.2018.v15.a2824>
- [6] Darwis, D., & Kisworo. (2017). TEKNIK STEGANOGRAFI UNTUK PENYEMBUNYIAN PESAN TEKS MENGGUNAKAN ALGORITMA END OF FILE. *Jurnal Sistem Informasi Dan Telematika*, 8(2).
- [7] Kaspari, A. (2021). ANALISIS KEAMANAN PESAN MENGGUNAKAN METODE STEGANOGRAFI LEAST SIGNIFICANT BIT (LSB). In | *Analisis Keamanan Pesan Menggunakan Metode... | Andrian Kaspari* (Vol. 4, Issue 1).
- [8] Tulloh, A. R., Permanasari, Y., & Harahap, E. (2016). Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen. *Jurnal Matematika UNISBA*, 15(1). <http://ejournal.unisba.ac.id>
- [9] Wisnu Arimurti, I. G. N. A., & Arta Wibawa, I. G. (2017). *Aplikasi Steganografi Untuk Menyembunyikan Pesan Teks Pada Gambar Dengan Metode Least Significant Bit (LSB)*.