IMPLEMENTASI *LEAST SIGNIFICANT BIT* (LSB) DAN ALGORITMA *VIGENERE CIPHER* PADA AUDIO STEGANOGRAFI

Minarni[1)], Rasyid Redha[2)]
[12]Fakultas Teknik, Institut Teknologi Padang
email: minarni1706@gmail.com[1)], rasyidredhaa19@gmail.com[2)]

Abstrak

Abstrak: Penelitian ini membahas tentang implementasi metode *Least Significant Bit* (LSB) dan algoritma *Vigenere Cipher* untuk menjaga kerahasiaan informasi atau data dari pihak yang tidak berwenang dengan menyembunyikan pesan pada sebuah media berupa *file* audio. Metode LSB digunakan untuk menyisipkan pesan dengan cara mengganti bit terendah dalam sebuah *byte* media pembawa pesan. Algoritma kriptografi *Vigenere Cipher* untuk menambah keamanan pesan dengan melakukan penyandian teks alphabet menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci. Pengujian dilakukan berdasarkan kriteria steganografi yaitu perubahan ukuran *file*, *fidelity*, dan *robustness*. Berdasarkan pengujian yang dilakukan pada beberapa *file* audio mp3 yang telah disisipkan pesan dengan variasi 50 sampai dengan 1000 karakter, hasil yang diperoleh ukuran *file* tidak mengalami perubahan setelah disisipkan pesan dan dapat diekstrak kembali. Banyaknya karakter dalam pesan mempengaruhi waktu penguraian pesan. Dari sisi *fidelity*, penyisipan karakter tidak mengubah *bit rate* dari stega audio. Sedangkan dari sisi *robustness*, stega audio tidak tahan terhadap manipulasi. Hasil ini menunjukkan metode LSB dan algoritma *Vigenere Cipher* pada media audio dapat menyisipkan pesan dan menguraikan kembali pesan yang telah terenkrip dengan baik tanpa merusak komponen audio.

Kata kunci: Audio Steganografi, *Least Significant Bit*, *Algoritma Vigenere Cipher*

Abstract*: This study discusses the implementation of the Least Significant Bit (LSB) method and the Vigenere Cipher algorithm to maintain the confidentiality of information or data from unauthorized parties by hiding messages on media audio. LSB is used to insert messages by replacing the lowest bit in a byte of the carrier media. Vigenere Cipher cryptographic algorithm to increase message security by encoding the alphabetic text using a Caesar cipher based on the letters in the password. Testing based on steganographic criteria, namely changes in file size, fidelity, and robustness. Based on tests carried out on several mp3 audio files that have been inserted with messages with variations of 50 to 1000 characters, the results obtained that the file size does not change after the message is inserted and can be extracted again. The number of characters in a message affects the parsing time of the message. In terms of fidelity, character insertion does not change the bit rate of audio stega. Meanwhile, in terms of robustness, stega audio is not resistant to manipulation. These results indicate that the LSB method and the Vigenere Cipher algorithm on audio media can insert messages and decipher messages that have been encrypted properly without damaging the audio components.*

Keywords*: Audio Steganography, Least Significant Bit, Vigenere Cipher*

PENDAHULUAN

Seringkali seseorang yang hendak mengirim pesan kepada orang lain, tidak ingin orang yang tidak berwenang mengetahui pesan tersebut. Pesan yang berisi sesuatu bersifat rahasia yang ditujukan untuk kalangan terbatas. Salah satu upaya untuk mengantisipasi pesan agar tidak sampai kepada orang yang tidak berwenang dapat dilakukan dengan membuat sebuah aplikasi yang dapat menyembunyikan pesan tersebut pada suatu media yang dapat ditelusuri oleh setiap orang. Menurut (Munir, 2004) steganografi merupakan teknik penyembunyian data pada suatu media.

Data yang disembunyikan berupa data teks, gambar, audio, dan video. Menurut (Singh, 2015) salah satu media untuk menyembunyikan data yaitu *file* audio yang dikenal dengan Audio Steganografi.

Metode *Least Significant Bit* (LSB) merupakan metode steganografi yang bekerja menyisipkan pesan dengan mengganti bit terendah dalam sebuah *byte* media pembawa pesan. Dalam sebuah *byte* terdapat susunan bit, yang di dalamnya terdapat bit yang paling berarti (*Most Significant Bit*) dan bit yang paling kurang berarti (LSB). Bit yang sesuai untuk diganti adalah bit LSB, karena hanya mengganti nilai *byte* satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya (Mulyono, 2018). Untuk menambah keamanan dari steganografi digunakan algoritma kriptografi. Menurut (Munir, 2006) kriptografi adalah seni dan ilmu untuk menulis rahasia, yang memiliki tujuan untuk mengolah informasi dengan suatu algoritma sehingga pesan tidak dapat dibaca. Salah satu algoritma kriptografi klasik yaitu algoritma *Vigenere Cipher* dimana algoritma ini menyandikan teks alfabet menggunakan deretan sandi caesar berdasarkan huruf-huruf pada kata kunci. Dengan menggabungkan teknik steganografi dan kriptografi, dapat memberikan keamanan pada pesan rahasia. Pesan yang telah dikodekan menggunakan algoritma kriptografi tertentu, kemudian disembunyikan ke dalam suatu media pembawa pesan, agar tidak menimbulkan prasangka dan curiga terhadap orang lain yang melihatnya.

Beberapa penelitian tentang kombinasi steganografi dan kritografi telah dilakukan oleh beberapa peneliti, diantaranya Kuncoro (2019) melakukan penelitian mengamankan informasi berupa pesan teks dengan menyisipkan (menyembunyikan) ke dalam pesan lainnya pada citra digital menggunakan metode *Least Significant Bit* (LSB) dan algoritma kriptografi *Rivest Shamir Adleman* (RSA). Penelitian tentang penyisipan teks ke dalam video, lalu mengacak video sehingga video tersebut pun tidak dapat dilihat (Gunawan, 2018). Penelitian yang dilakukan oleh Kurniawan tentang pengamanan informasi berupa pesan teks dengan menyisipkan pesan kedalam media audio dengan format mp3 menggunakan metode *Parity Coding* dan algoritma *Caesar Cipher*. Hasil pengujian diperoleh bahwa setelah melakukan proses *embedding* (penyisipan pesan), terdapat penurunan kualitas dari *stegano file* dibandingkan dengan *file* mp3 yang asli, karena terjadi proses penggantian nilai bit terakhir dari setiap karakter *file* media dengan kemungkinan perubahan sebesar 50%. Hasil penelitian (Mustakmal, 2018) tentang perbandingan kualitas audio dengan menghitung dan membandingkan nilai PSNR antara *carrier* audio dengan *stego* audio. *File* yang digunakan berupa *file plain text* pantun berukuran 100 *bytes*. *Carrier* audio yang digunakan merupakan 5 *file* audio berformat WAV.

Penelitian ini mengimplementasikan metode steganografi *Least Significant Bit* (LSB) dan kriptografi Algoritma *Vinegere Cipher* dalam meningkatkan keamanan data atau informasi pada *file* audio berformat mp3.

METODE PENELITIAN

Penelitian ini dilaksanakan berdasarkan tahapan pengembangan sistem model *waterfall* merupakan model pengembangan sekuensial. Menurut (Pressman, 2012 model *waterfall* terdiri dari tahap analisis, desain, implementasi, dan pengujian.

Tahapan-tahapan tersebut diuraikan sebagai berikut.

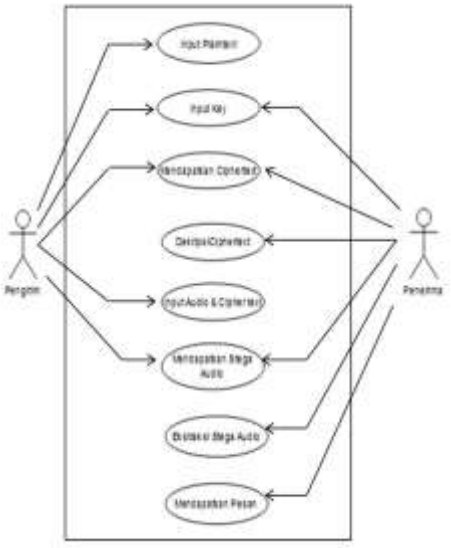
1. **Analisis Kebutuhan**

   Pada penelitian ini dibangun sebuah aplikasi yang berfungsi untuk menyisipkan pesan pada audio dengan menggabungkan metode *Least Significant Bit* (LSB) dengan algoritma kriptografi *Vigenere Cipher* untuk memberikan keamanan ganda pada pesan yang akan disembunyikan.

Aplikasi ini akan dibangun dengan menggunakan Matlab. Inti dari program ini yaitu menyisipkan informasi atau pesan pada nilai bit terendah dari sebuah *byte* pada audio sebelum disisipkan, informasi atau pesan tersebut dienkripsi menggunakan algoritma *Vigenere Cipher* terlebih dahulu. Penyisipan dilakukan setelah audio diubah kedalam bentuk bilangan desimal dan menyisipkannya pada nilai bit terendah pada sebuah *byte* dari audio tersebut. Analisa kebutuhan dalam penelitian ini meliputi alat dan bahan yang akan digunakan dalam penelitian. Bahan yang digunakan sebagai media penampung berupa *file* audio dengan format mp3, sedangkan pesan yang akan disisipkan berupa *text*. Fasilitas-fasilitas yang tersedia pada sistem yang akan memungkinkan pengguna untuk dapat menyisipkan pesan pada audio dan mengekstrak *file* audio tersebut untuk mendapatkan pesan kembali.

2. Desain

Pada tahapan ini dilakukan perancangan pembuatan aplikasi menggunakan pemodelan *use case diagram* yang merupakan gambaran aplikasi yang akan dibuat.

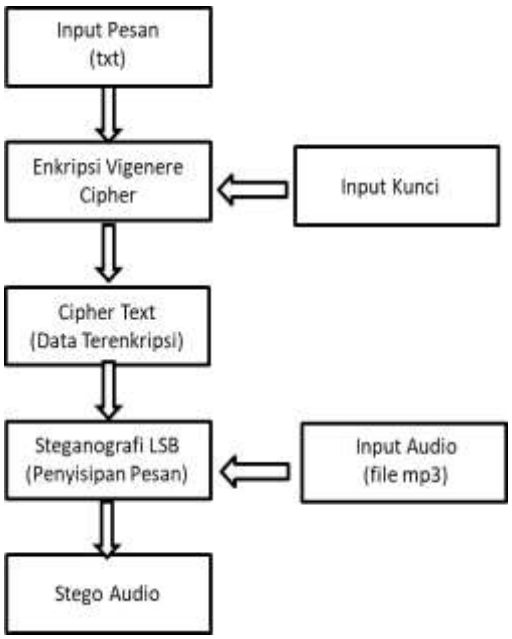


Gambar 1. Pemodelan Sistem Aplikasi Audio Steganografi Dengan *Use Case Diagram*

Pada gambar 1 dapat dijelaskan sebagai berikut pengirim menginputkan pesan atau *Plain Text* dan K*ey*, kemudian pengirim akan mendapatkan *Cipher Text*, lalu pengirim menginputkan audio beserta *Cipher Text* untuk keamanan pesan, kemudian pengirim akan mendapatkan stego audio yang akan dikirim kepada penerima pesan. Penerima menginputkan sebuah audio yang telah berisi sebuah pesan, lalu pesan yang sudah didapat kemudian didekripsi dengan algoritma *Vigenere Cipher* agar dapat dibaca.

3. Implementasi

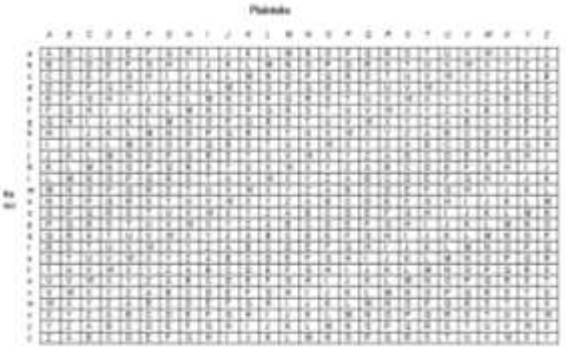
Pada tahapan ini terdapat dua proses yaitu, menyisipkan pesan ke dalam media audio yang dikenal dengan *encoding*, dan menguraikan (ekstraksi) pesan dari stego *audio* yang dikenal dengan *decoding*.



Gambar 2. Blok Diagram Proses *Encoding*

Gambar 2 menunjukkan proses *encoding*, diawali dengan menginput pesan teks yang akan dienkripsi menggunakan algoritma *Vigenere Cipher*. Menurut (Munir, 2006) algoritma ini menggunakan bujur

sangkar *Vigenere Cipher* seperti pada Gambar 3.



Gambar 3. Bujur Sangkar *Vigenere Cipher*

Setiap baris di dalam bujur sangkar menyatakan huruf-huruf *Cipher Text* yang diperoleh dengan *Caesar Cipher*. Enkripsi ditunjukkan pada persamaan 1.

$$C_i = (P_i + K_i) mod\ 26 \qquad (1)$$

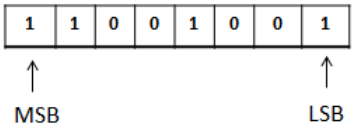
Dimana :
Ci : nilai desimal karakter *ciphertext* ke-i
Pi : nilai desimal karakter *plaintext* ke-i
Ki : nilai desimal karakter *key* ke-i
Nilai desimal karakter: A=0, B=1, C=2…Z=25

Berikut ilustrasi proses enkripsi sebagai berikut.
Pesan/*Plaintext* = **inirahasia**
Kunci = **audioaudio**

Enkripsi berdasarkan Gambar 3, maka:
huruf I dengan kunci a = (I + a) mod 26 = I
huruf N dengan kunci u = (N + u) mod 26 = H

Sehingga *Cipher text* = **IHLZOHUVRO**

Setelah pesan terenkripsi dan mendapatkan *Cipher Text*, selanjutnya dilakukan proses penyisipan pesan menggunakan metode LSB, di mana LSB merupakan bit paling kurang berarti pada susunan bit dalam satu *byte* (8 bit) seperti ditunjukkan pada Gambar 4. *File* audio diinputkan sebagai penampung atau *cover text*. (Mulyono, 2018).



Gambar 4. MSB dan LSB

Ilustrasi penyisipan pesan menggunakan LSB. Misalkan *byte file* audio yang telah dikonversikan menjadi biner seperti berikut

10001011 00101001 10101110 10101110 00010001
11001101 11001011 11001000 10101010 10101101

Pesan yang telah terenkrip menjadi *Cipher Text* dikonversikan menjadi biner 0101000101, kemudian setiap bit pesan akan menggantikan posisi LSB (bit yang diberi garis bawah pada contoh di atas), sehingga menjadi:

10001010 00101001 10101110 10101111 00010000
11001100 11001010 11001001 10101010 10101101

Rata-rata hanya setengah dari bit-bit dalam *file* audio yang akan dimodifikasi untuk menyembuyikan pesan menggunakan ukuran *cover* maksimum. Hasil berupa *file stego* audio yaitu *file* audio yang telah disisipkan pesan.

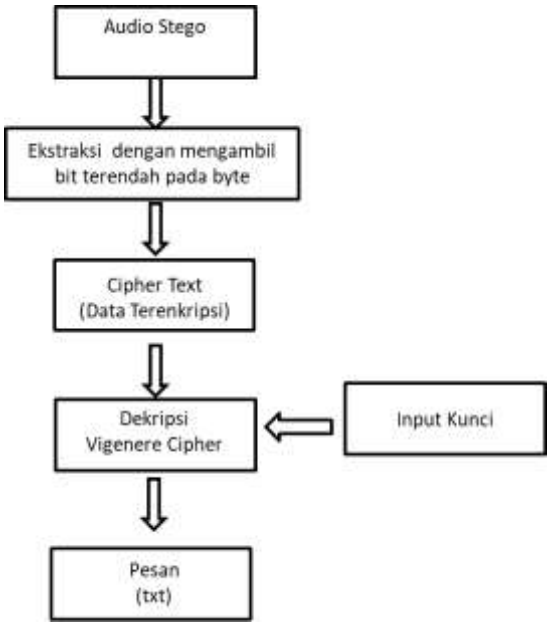
Pada gambar 5 menunjukkan proses *decoding* yaitu proses untuk membaca pesan yang ada di dalam *file* audio. Saat *stego* audio diinputkan, maka sistem akan membaca apakah terdapat pesan atau tidak. Sistem akan membaca panjang data yang disisipkan, kemudian melakukan proses ekstraksi atau penguraian pesan dengan mengambil bit terendah (LSB) pada *byte-byte file* audio sehingga menghasilkan *Cipher Text* (data yang terenkripsi). Selanjutnya dilakukan proses dekripsi algoritma *Vigenere Cipher* berdasarkan persamaan 2.

$$P_i = (C_i - K_i) mod\ 26 \qquad (2)$$

Ilustrasi proses dekripsi sebagai berikut.
Cipher text = IHLZOHUVRO
Kunci = audioaudio

Dekripsi berdasarkan Gambar 3, maka:
Huruf I dengan kunci a = (I – a) mod 26 = I
Huruf H dengan kunci u = (H – u) mod 26 = N
Sehingga *Plain text* = inirahasia

Plain text atau pesan yang diperoleh disimpan sebagai *file* baru.



Gambar 5. Blok Diagram Proses *Decoding*

4. Pengujian

Tahapan ini merupakan tahapan menguji aplikasi audio steganografi dengan berdasarkan ukuran *file* audio, *fidelity (bit rate),* dan *robustness.*

HASIL DAN PEMBAHASAN

Dalam melakukan pengujian pada aplikasi audio steganografi dengan LSB dan algoritma *Vigenere Cipher* ini menggunakan beberapa sampel audio berformat mp3 yang berukuran 3 MB sampai dengan 12 MB dan *bitrate* 192 kbps sebagai media penampung. Pesan yang disisipkan berupa *file* berformat txt dengan variasi jumlah karakter. Pengujian bertujuan untuk mengetahui kualitas audio berupa perubahan ukuran audio, waktu pengekstrakan, dan melakukan perubahan pada audio yang telah disisipkan pesan seperti pemotongan serta membuat audio menjadi lambat.

1. Pengujian Perubahan Ukuran Audio

Tabel 1. Pengujian Perubahan Ukuran Audio

Pesan (char)	Ukuran Audio (MB)				
	a.mp3 4,82515	b.mp3 6,96143	c.mp3 9,14315	d.mp3 9,36676	e.mp3 10,11533
50	4,82502	6,96130	9,14301	9,36663	10,11519
70	4,82502	6,96130	9,14301	9,36663	10,11519
100	4,82502	6,96130	9,14301	9,36663	10,11519
120	4,82502	6,96130	9,14301	9,36663	10,11519
150	4,82502	6,96130	9,14301	9,36663	10,11519
200	4,82502	6,96130	9,14301	9,36663	10,11519
300	4,82502	6,96130	9,14301	9,36663	10,11519
500	4,82502	6,96130	9,14301	9,36663	10,11519
1000	4,82502	6,96130	9,14301	9,36663	10,11519

Tabel 1 menunjukkan banyaknya karakter pesan yang disisipkan tidak berpengaruh ke ukuran *stego audio*. Berapapun jumlah karakter pesan dimasukkan ke audio, ukuran dari *stego audio* akan tetap sama. Ini disebabkan oleh bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya hanya sedikit bit signifikan yang diubah sehingga tidak berpengaruh dengan ukuran *file* setelah disisipkan.

2. Pengujian Waktu Ekstraksi

Tabel 2. Pengujian Waktu Ekstraksi

Pesan (char)	Waktu (s)				
	a.mp3 4,82515	b.mp3 6,96143	c.mp3 9,14315	d.mp3 9,36676	e.mp3 10,11533
50	2,97	3,89	4,78	4,83	5,14
70	3,01	3,93	4,43	4,85	5,17
100	3,09	3,98	4,47	4,88	5,19
120	3,15	4,03	4,50	4,90	5,21
150	3,20	4,09	4,53	4,93	5,20
200	3,27	4,15	4,59	4,96	5,25
300	3,34	4,23	4,65	4,99	5,27
500	3,41	4,27	4,76	5,10	5,29
1000	3,60	4,47	4,91	5,31	5,43

Waktu ekstraksi merupakan waktu yang diperlukan untuk mendapatkan pesan yang disisipkan. Tabel 2 menunjukan bahwa semakin banyak karakter yang disisipkan, maka waktu yang

dibutuhkan untuk pengekstrakannya pun semakin lama. Hal ini karena adanya dua proses yang terjadi pada saat ekstraksi yaitu mengambil bit terendah dari susunan pada *stega audio* hasil dari LSB yang menghasilkan *Cipher Text*. Kemudian *Cipher Text* didekripsi dengan algoritma *Vigenere Cipher* untuk mendapatkan pesan kembali.

3. Pengujian *Fidelity* Audio

Tabel 3. Pengujian *Fidelity* Audio

Karakter Pesan	*Stegoaudio*	*Bit Rate*
50	a.mp3	192kbps
70	a.mp3	192kbps
100	b.mp3	192kbps
120	b.mp3	192kbps
150	c.mp3	192kbps
200	c.mp3	192kbps
300	d.mp3	192kbps
500	d.mp3	192kbps
1000	e.mp3	192kbps

Dari hasil pengujian *fidelity* bahwa bit *rate* dari *stego audio* tidak mengalami perubahan atau tetap sama seperti audio aslinya. Tidak terjadinya perubahan pada komponen audio tersebut karena algoritma LSB hanya mengganti nilai bit terendah dari audio sehingga tidak merusak kualitas atau komponen dari audio tersebut, dan hasil pengujian *fidelity*-nya dapat dikatakan baik.

4.Pengujian *Robustness*

Pengujian *robustness* yang dilakukan berupa *cutting* dan *slow motion*, hasil yang diperoleh bahwa pesan tidak dapat di-*recovery* setelah dilakukan manipulasi pada *stego audio*. Hal ini disebabkan karena terjadinya perubahan pada bit audio, yang menyebabkan terjadinya perubahan tehadap pesan. Sehingga pesan tidak dapat dikenali. Dengan demikian steganografi dengan algoritma LSB tidak tahan terhadap *robustness*.

Dari hasil pengujian di atas menunjukkan metode LSB dan algoritma *Vigenere* dapat mengamankan data atau informasi secara berlapis algoritma *Vigenere Cipher* mengenkrip pesan atau informasi. Hasil enkripsi tersebut disisipkan atau disembunyikan menggunakan LSB dimana terjadi perubahan pada bit terendah pada *file* audio. Sehingga pesan tidak dapat dibaca oleh orang yang tidak berwenang. Dengan metode di atas, hasil pengujian menunjukkan pesan yang terenkrip dapat diuraikan atau dibaca kembali dengan baik tanpa merusak komponen audio.

KESIMPULAN

Implementasi teknik steganografi dan kriptografi pada audio mp3 menggunakan LSB dan algoritma *Vigenere Cipher* telah berhasil dilakukan. Penggabungan kedua metode ini dapat digunakan untuk mengamankan pesan yang disisipkan dalam *file* audio. Hasil pengujian menunjukkan pesan yang terenkrip dapat diuraikan atau dibaca kembali dengan baik tanpa merusak komponen audio.

DAFTAR PUSTAKA

Gunawan, I., Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video. *J-SAKTI (Jurnal Sains Komputer dan Informatika)*, *2*(1), 2018, pp.57-65.

Kuncoro, T.R. and Aditama, R., Analisis Kombinasi Algoritma Kriptografi Rsa Dan Algoritma Steganografi Least Significant Bit (Lsb) Dalam Pengamanan Pesan Digital. *Statmat: Jurnal Statistika Dan Matematika*, *1*(2), 2019.

Kurniawan, C. and Putranto, H.S., Perancangan Aplikasi Penyisipan

Pesan pada File Mp3 menggunakan Metode Parity Coding dan Enkripsi Caesar Cipher.

Mulyono IU, Susanto A, Anggraeny T, Sari CA. Encryption of Text Message on Audio Steganography Using Combination Vigenere Cipher and LSB (Least Significant Bit). *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*. 2018 Nov 10;4(1):63-74.

Munir, Rinaldi, Pengolahan Citra Digital Dengan Pendekatan Algoritmik, Informatika: Bandung, 2004.

Munir, R., Kriptografi. Penerbit Informatika, Bandung, 2006.

Mustakmal, M.E., Audio Steganografi Dengan Algoritma Lsb Untuk Pengamanan Data Digital, 2018.

Pressman, 2012, Rekayasa Perangkat Lunak Pendekatan Praktisi (Buku, Satu). Yogyakarta: Andi Offset, 2012.

Saragih, R.A., Metode Parity Coding Versus Metode Spread Spectrum Pada Audio Steganography. In *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, 2006.

Singh, A.K., Singh, J. and Singh, H.V., Steganography in Images Using LSB Technique. *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, 5(1), 2015, pp.426-430.