Jurnal Informatika dan Rekayasa Perangkat Lunak ISSN 2656-2855
Vol. 6, No. 1, Maret 2024, Hal. 102-108 e-ISSN 2685-5518

Implementasi Steganografi Metode Least Significant Bit (LSB) untuk Menyembunyikan File Pesan dalam Gambar

Muhammad Na'im Al Jum'ah[1*], **Sarimuddin**[2]
[1] Program Studi Ilmu Komputer , Fakultas Teknologi Informasi,
Universitas Sembilanbelas November Kolaka
[*]Email: muhnaimaljumah@usn.ac.id, sarimuddin85@gmail.com

Abstrak

Kemudahan untuk melakukan manipulasi gambar bukanlah sesuatu hal yang sulit. Gambar menjadi media komunikasi yang lebih efektif bagi Masyarakat. Berkembangnya perangkat lunak untuk manipulasi gambar, meningkatnya tindak kejahatan seperti pishing, buliying di dunia maya. Metode Least Significant Bit merupakan salah satu metode steganografi yang dapat digunakan untuk enkripsi atau menyembunyikan pesan kedalam gambar. Menyembunyikan informasi dalam berbagai file media seperti gambar dilakukan untuk menjaga kerahasian dari pesan yang dikirimkan. Penelitian ini mengimplementasi metode Least Significant Bit (LSB) untuk menyembunyikan sebuah file pesan di dalam gambar. Penelitian ini melakukan enkrisi dan deskripsi terhadap pesan yang akan di kirimkan dengan melakukan penyisipan sebuah file terhadap gambar. Penelitian ini juga akan melakukan proses pengujian terhadap stego image. Dari hasil pengujian yang telah dilakukan dengan melakukan tiga proses pengiriman file image stego melalui copy file dengan flashdisk, email dan pengiriman melalui whatsapp dengan model dokumen, diperoleh hasil bahwa file image stego masih bisa dilakukan ekstraksi data untuk mendapatkan pesan yang telah di encripsi dalam gambar, namun ketika file image stego yang dikirimkan melalui whatsapps dengan medel pengiriman image, image stego tersebut tidak bisa dilakukan ekstraksi. Hal ini terjadi karena telah terjadi perubahan ekstensi file hasil download dari whatsapp tersebut. Hal ini juga dipengaruhi oleh perubahan data berupa kompresi file dari aplikasi whatsapp tersebut. Dimana setiap file yang dikirimakan melalui aplikasi whatsapp maka file tersebut akan mengalami kompresi file sehingga akan terjadi perubahan data

***Kata kunci**: Deteksi Gambar, Least Significant Bit, Steganografi, Kriptografi*

Abstract

Ease of image manipulation is not something difficult. Images become a more effective communication medium for society. The development of software for image manipulation, increasing crime such as phishing and bullying in cyberspace. The Least Significant Bit method is a steganography method that can be used to encrypt or hide messages in images. Hiding information in various media files such as images is done to maintain the confidentiality of the messages sent. This research implements the Least Significant Bit (LSB) method to hide a message file in an image. This research carries out encryption and description of the message to be sent by inserting a file into the image. This research will also carry out a testing process for the stego image. From the results of tests that have been carried out by carrying out three processes of sending stego image files via copying files with a flash disk, email and sending via WhatsApp with a document model, the results obtained are that stego image files can still be extracted data to get messages that have been encrypted in the image, However, when the stego image file is sent via WhatsApp using the image sending method, the stego image cannot be extracted. This happens because there has been a change in the extension of the file downloaded from WhatsApp. This is also influenced by data changes in the form of file compression from the WhatsApp application. Where every file sent via the WhatsApp application will experience file compression so that data changes will occur

***Keywords:** Image Detection, Least Significant Bit, Steganography, Cryptography*

PENDAHULUAN

Perkembangan media digital yang semakin modern, kemudahan untuk melakukan manipulasi gambar bukanlah sesuatu hal yang sulit. Gambar menjadi media komunikasi yang efektif bagi Masyarakat karena dapat dengan mudah di per oleh baik melalui kamera maupun telepon seluler(Xu et al., 2016). Dari perkembangan yang terjadi, ada kepercayaan pada integritas data visual, sehingga jika gambar di cetak di dalam media berupa surat kabar secara umum Masyarakat akan mempercayai itu

sebagai kebenaran informasi. Dengan cepatnya penyebaran informasi berupa data visual ini, dapat memungkinkan Masyarakat untuk menyimpan dan merekam data gambar yang ada(Piva, 2013).

Berkembangnya perangkat lunak untuk manipulasi gambar, meningkatnya tindak kejahatan seperti pishing, buliying di dunia maya, mendorong penanganan bukti digital yang semakin baik guna mengidentifikasi penyalahgunaan gambar di media digital (Abdul et al., 2015). Gambar merupakan media yang populer untuk menerbitkan data atau berita ataupun pesan yang bersifat rahasia. Hal ini menjadi poin penting untuk memastikan serta memverifikasi apakah jenis data ini nyata atau palsu (Babu et al., 2013).

Dalam informasi rahasia dibutuhkan pengamanan informasi. Kerahasiaan informasi akan menjamin informasi tersebut hanya dapat digunakan oleh pihak yang memiliki kewenangan(Faris et al., 2023). Menyembunyikan informasi dalam berbagai file media seperti gambar dilakukan untuk menjaga rahasia dari informasi pesan yang dikirimkan. Steganografi teknik yang bertujuan menyembunyikan pesan rahasia atau tulisan rahasia sehingga informasi yang sifatnya rahasia tersebut tidak dapat diidentifikasi oleh orang lain dalam artian yang dapat mengetahui informasi dari pesan tersebut hanya pengirim dan penerima. steganografi mempertahankan data aslinya dengan menyembunyikannya di media lain seperti teks, gambar, audio maupun video (Majeed et al., 2021).

Metode steganografi Least Significant Bit (LSB) dapat digunakan untuk enkripsi pesan. Dalam metode ini pesan akan disisipkan dengan cara mengganti bit terkecil yang terakhir dari pixel citra dengan bit pesan, karena tidak akan memberikan pengaruh atau perubahan yang signifikan terhadap citra digital. Penggantian bit-bit data dalam segmen citra gambar akan menyembunyikan pesan rahasia yang telah di sisipkan(Mani et al., 2016).

Untuk menyisipkan informasi dalam suatu file, atribut dari file tersebut harus diubah, seperti mengubah font ataupun ukuran dari file. Akan tetapi hal seperti ini mudah untuk di deteksi. Namun yang menjadi kendala adalah melakukan Analisa terhadap suatu file gambar, di mana dalam perubahan file tersebut tidak terlihat oleh dengan mata, namun tetap dapat didekodekan menggunakan komputer(Varol et al., 2019). Dengan menerapkan Least Significant Bit (LSB) file yang di kirim akan tersembunyi sehingga tidak dapat di akses oleh orang yang tidak berhak.

Pada penelitian ini akan melakukan implementasi metode Least Significant Bit (LSB) untuk enkripsi atau menyembunyikan sebuah file di dalam gambar. Penelitian ini melakukan enkripsi dan deskripsi terhadap pesan yang akan di kirimkan dengan melakukan penyisipan sebuah file terhadap gambar. Penelitian ini juga akan melakukan proses pengujian terhadap stego image. Proses pengujian meliputi tiga metode yaitu, mengirimkan file stego image melalui copy paste flash disk, email dan whatsapp. Pegujian ini bertujuan untuk melihat apakah file di sembunyikan di dalam file stego image masih bisa di ekstraksi setelah melewati proses pengiriman file

TINJAUAN PUSTAKA

Beberapa penelitian telah dilakukan terkait dengan metode Least Significant Bit (LSB) seperti yang dilakukan oleh (Yanti & Budayawan, 2023) tentang bagaimana melakukan implementasi steganografi dengan metode Least Significant Bit (LSB) untuk mengamankan informasi dalam citra digital. Dari penelitian yang dilakukan ditemukan bahwa citra yang di sisipkan dalam stego image tidak mengalami perubahan signifikan dari citra asli. Perubahan akan terjadi apabila informasi yang disisipkan dalam citra di ubah formatnya. Berbeda dengan yang dilakukan oleh(Wiryawan et al., 2019) dengan memanfaatkan teknik kompresi dalam mengimplementasikan pada metode Least Significant Bit (LSB). Dari penelitian ini diperoleh kesimpulan bahwa citra digital dengan format bmp dan jpg memiliki nilai yang identik dan perubahan karakteristik dari proses pengujian menggunakan Image Quality Assessment

Penelitian juga dilakukan oleh (Handoyo et al., 2018) dengan melakukan kombinasi metode Least Significant Bit (LSB) dan RSA untuk enkripsi citra digital. Dari penelitian ini diperoleh nilai imperceptibility yang masih terjaga dan terjadi peningkatan keamanan. Dapat dibuktikan dengan hasil PNSR serta kombinasi kedua metode ini tahan terhadap serangan salt dan pepper. Serupa dengan penelitian yang dilakukan oleh (Jatmoko et al., 2018) dengan melakukan uji peforma terhadap

pesan yang telah disisipkan dengan metode Least Significant Bit (LSB) dan Most Significant Bit (MSB). Dari hasil uji peforma yang dilakukan metode Least Significant Bit (LSB) terbukti kualitas lebih baik dari metode MSB. Namun dari segi ketahanan terhadap serangan metode MSB lebih unggul seperti pada jenis serangan salt dan pepper.

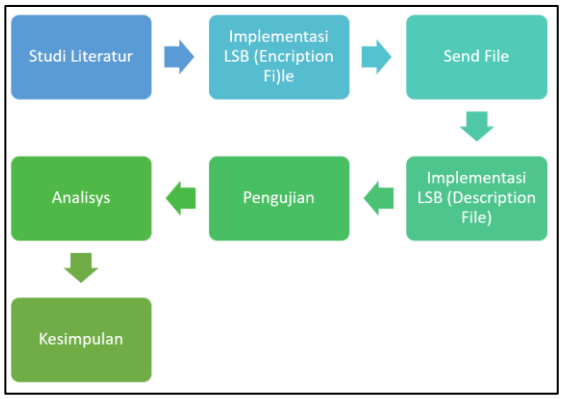
Penelitian lain juga dilakukan oleh (Utomo Wahyu Mulyono et al., 2023) dengan melakukan analisis visual citra dari hasil kombinasi antara steganografi dan kriptografi dengan metode Least Significant Bit (LSB) dalam nit chipper. Dari hasil analisis diperoleh hasil bahwa rata-rata nilai PNSR yang didapatkan lebih dari 30 dB dimana nilai kualitas gambar stego dengan nilai PSNR rata-rata 30 dB. Hal ini membuktikan kualitas sangat baik. Ukuran citra dari stego akan mengalami perubahan yang signifikan dari proses enkripsi dan embedding pesan.

Penelitian juga dilakukan oleh (Sina et al., 2022) tentang penggabungan metode Triple DES dan metode kompbinasi LSB dan BLUM-SHUB untuk aplikasi keamanan pesantxt. Dari penelitian ini diperoleh hasil ektraksi terhadap embedded message yang disembunyikan memiliki akurasi sampai 100%. stego-image yang memiliki rata-rata nilai peak signal to noise ratio (PSNR) sama dengan 88,61 yang berarti bahwa stego-image yang dihasilkan memiliki kualitas tinggi serta keberadaan pesan di dalam stego-image semakin sulit untuk diketahui.

Perbedaan penelitian ini dengan penelitian-penelitian sebelumnya yaitu pada penelitian ini, berfokus pada tiga jenis proses perpindahan atau pengiriman file yaitu flaskdisk, email dan whatsapp. Penelitian ini akan melakukan proses enkripsi dan deskripsi terhadap pesan yang akan di kirimkan dengan melakukan penyisipan sebuah file terhadap gambar. Penelitian ini juga akan melakukan proses pengujian terhadap stego image. Proses pengujian meliputi tiga metode yaitu, mengirimkan file stego image melalui copy paste flash disk, email dan whatsapp.Proses enkripsi dan deskripsi file dengan tiga proses tersebut, kemudian akan dilakukan analisis untuk melihat hasil yang ada dengan menerapkan Metode Least Significant Bit (LSB).

METODE PENELITIAN

Pada Gambar 1, terlihat metode penelitian yang digunakan dan akan menjelaskan proses penyelesaian permasalahan dari penelitian ini.



Gambar 1. Alur Metodologi Penelitian

Metode atau tahapan yang dilakukan di antaranya:

1. Studi Literatur.
   Tahapan pertama adalah studi literatur. Pada tahapan ini di kumpulkan referensi sejenis yang terkait dengan penelitian ini. Sumber informasi dan referensi dari penelitian ini berasal dari beberapa jurnal penelitian yang menjadi rujukan dalam penelitian.
2. Implementasi LSB (Encription File)
   Tahap yang kedua adalah melakukan proses enkripsi data. Pada tahapan ini file yang berupa pesan akan dilakukan proses enkripsi data dengan menyisipkan file tersebut pada cover image. Proses enkripsi file dilakukan dengan merode Least Significant Bit (LSB). Dengan menggunakan metode ini pesan akan disisipkan atau di enkripsi dengan cara mengganti bit terkecil (terakhir) dari pixel citra dengan bit pesan. Hal ini dilakukan untuk menyembunyikan file pesan yang akan di kirimkan.
3. Send File
   Tahapan selanjutnya adalah proses pengiriman file atau data. Pada tahapan ini dilakukan tiga pengujian data. Pertama akan mengirimkan file stego image melalui flasdisk untuk perpindahan data. Pengujian kedua dengan mengirimkan file stego image melalui alamat email dan proses pengujian yang ketiga akan mengirimkan

file stego image melalui media whatsapp. Proses pengiriman file melalui media whatsapp akan menggunakan dua metode. Metode pertama adalah mengirimkan file stego image melalui media photos dan yang kedua dengan media Document. Dari ketiga metode tersebut kemudian akan dilakukan Analisa perbandingan.

Gambar 2.Media pengujian file stego image

Dari ketiga metode yang digunakan seperti pada Gambar 2, kemudian dilakukan proses pengujian, apakah data yang telah di enkripsi masih dapat di temukan atau tidak.

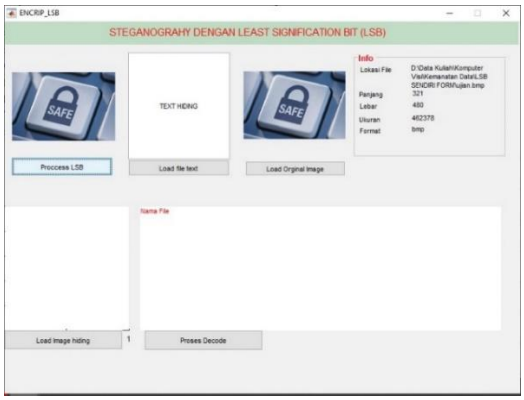
4. Implementasi LSB (Description File)
   Tahapan keempat adalah melakukan deskripsi data dari file stego image yang telah dikirim melalui tiga metode pengiriman data. Pada tahapan ini akan dilakukan pemeriksaan terhadap isi pesan yang telah dikirimkan
5. Analisis
   Tahapan selanjutnya adalah proses analisis. Pada tahapan ini akan dilakukan proses analisis perbandingan dari file stego image yang di kirimkan. Apakah terjadi perubahan data dari file stego image yang telah dikirimkan.
6. Kesimpulan
   Tahapan terakhir adalah kesimpulan. Pada tahapan ini akan dilakukan penarikan kesimpulan dari pengujian dan analisis yang telah dilakukan.

HASIL DAN PEMBAHASAN

Hasil penelitian akan dijelaskan secara rinci pada proses ini. Proses ini akan menjelaskan setiap langkah yang telah di terapkan dalam penelitian.

4.1 Implementasi LSB (Encription File)

Pada proses ini dilakukan proses enkripsi file di dalam gambar atau cover image. Pesan akan di simpan dalam file notepad dengan ekstensi file txt. File ini kemudian akan di enkripsi dalam cover image. Proses enkrisi file pesan dalam cover image dapat dilihat pada Gambar 3.

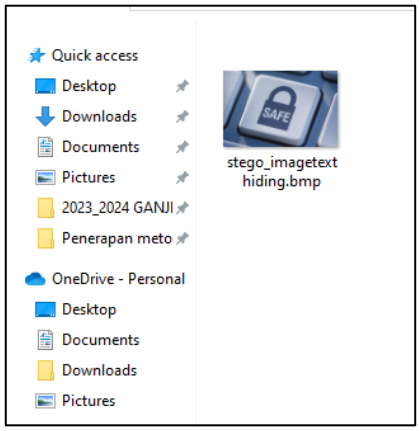


Gambar 3. Enkripsi file kedalam cover image

4.2 Proses Send File

Setelah dilakukan proses enkripsi file pesan di dalam cover image, kemudian dilakukan proses pengirim data. Dalam proses pengiriman file stego image, dilakukan tiga proses pengiriman data yaitu melalui copy ke flashdisk, email, dan yang terakhir dengan media whatsapp image dan dokumen. .

1. Pengujian pertama dilakukan pengiriman file stego image melalui flashdisk. Stego image yang berisi file pesan rahasia hasil enkripsi kemudian di copy ke dalam flashdisk.



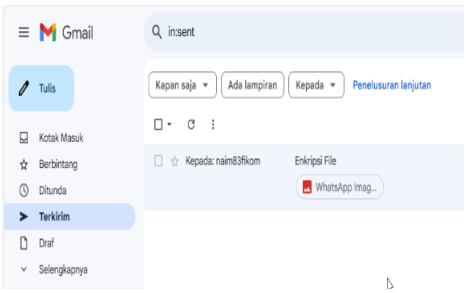
Gambar 4. Send stego image dengan flashdisk

2. Pengujian kedua adalah dengan melakukan pengiriman file stego image melalui Whatsapp. Stego image yang berisi file yang telah di enkripsi dikirim melalui whatsapp kepada penerima.

Gambar 5. Send stego image dengan whatsapp

Seperti pada gambar 5, file stego image yang dikirim menggunakan dua tipe pengiriman file. Pengiriman pertama adalah dengan model Image dan model kedua adalah dengan model Dokumen.

3. Pengujian ketiga dengan melakukan pengiriman file stego image melalui email. Stego image yang berisi file enkripsi akan dikirim melalui email kepada penerima file



Gambar 6. Send stego image dengan email

Seperti yang terlihat pada gambar 6, file hasil enkripsi di kirim melalui email kepada penerima file.

4.3 Implementasi LSB (Deskription File)

Pada tahapan ini, file yang telah diterima dari pengirim file akan dilakukan proses deskripsi file atau membuka file stego image yang telah di enkripsi dalam cover image yang ada.

4.3.1 Flashdisk

Pada pengujian pertama dilakukan proses deskripsi file stego image yang diterima melalui hasil copy file dari flashdisk.

Gambar 7. Deskripsi file stego image dari flaskdisk

Dari hasil pengujian yang dilakukan seperti pada gambar 7, file stego image yang di kirim meggunakan perantara flashdisk didapatkan isi dari pesan yang telah di enkripsi dalam file gambar.

4.3.2 Email

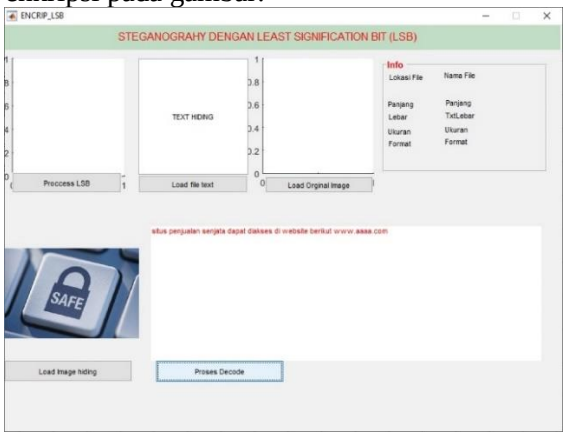
Proses pengujian pada tahap kedua ini dilakukan dengan melakukan deskripsi file stego image yang telah di terima melalui pengiriman email**.**

Gambar 8. Deskripsi file stego image dari email

Dari hasil pengujian yang dilakukan seperti pada gambar 8, file stego image yang di kirim meggunakan perantara email, didapatkan isi pesan yang telah di enkripsi dalam file gambar.

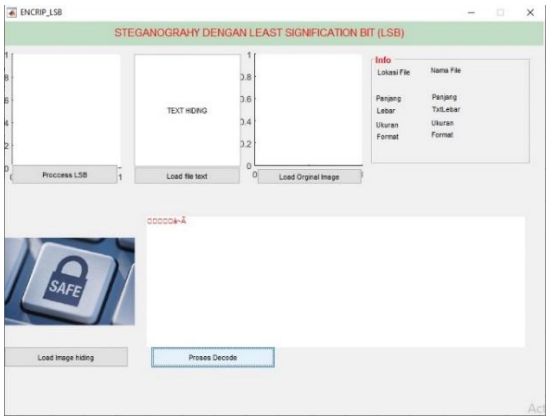
4.3.3 Whatsapp

Selanjutnya dilakukan proses deskripsi file stego image yang telah diterima melalui aplikasi whatsapp. Untuk deskripsi file yang telah dikirim melalui Whatsapp dengan metode Dokumen, berhasil ditemukan data yang telah di enkripsi pada gambar.



Gambar 7. Deskripsi file stego image dari whatsapp dokumen

Akan tetapi, ketika dilakukan deskripsi file terhadap file yang dikirim melalui model kirim gambar, tidak ditemukan data enkripsi yang telah disimpan pada gambar.



Gambar 8 Deskripsi file stego image dari whatsapp image

Proses ketiga adalah dilakukan proses deskripsi file yang telah di terima melalu email. Pada proses ini ditemukan pesan hasil enkripsi file.

4.4 Analisis

Tabel 1. Hasil Pengujian

No	Enkripsi	Image File	Media pengiriman file	Deskripsi	Hasil	
					Ditemukan	Tidak Ditemukan
1	✓	✓	Flashdisk	✓	✓	
2	✓	✓	Whatsapp	✓	✓	✗
3	✓	✓	Email	✓	✓	

Berdasarkan hasil pengujian yang telah di lakukan, ditemukan perbedaan dari tiga proses yang telah dilakukan. Pada proses pengujian untuk mendeskripsi image yang berisi file enkripsi, proses pengiriman file yang dilakukan menggunakan metode copy file dengan menggunakan flashdis dan pengiriman melalui email, berhasil di temukan isi dari pesan enkripsi yang telah diselipkan di dalam gambar. Namun untuk pengujian dengan metode pengiriman file dengan metode whatsapp. Proses pengiriman file image dengan whatsapp ini menggunakan dua metode, pengiriman file dengan meggunakan media photo dan media document. Untuk media dokumen, pesan hasil enkripsi berhasil di dapatkan, akan tetapi ketikan melakukan encripsi dengan pengiriman dengan media gambar, pesan hasil enkripsinya tidak di temukan. Hal ini disebabkan, terjadi perubahan ekstensi data dari file image yang di terima. File di kirim memiliki ekstensi file .bmt, namun setelah dilakukan proses pengiriman ekstensi file berubah menjadi file ekstensi .jepg.

SIMPULAN

Dari hasil pengujian yang telah dilakukan dengan melakukan tiga proses pengiriman file image stego melalui copy file dengan flashdisk, email dan pengiriman melalui whatsapp dengan model dokumen, diperoleh hasil bahwa file image stego masih bisa dilakukan ekstraksi data untuk mendapatkan pesan yang telah disembunyikan dalam gambar, namun ketika file image stego yang dikirimkan melalui whatsapps dengan model pengiriman image, image stego tersebut tidak bisa dilakukan ekstraksi. Hal ini terjadi karena telah terjadi perubahan ekstensi file hasil download dari whatsapp tersebut. Hal ini juga dipengaruhi oleh perubahan data berupa kompresi file dari aplikasi whatsapp tersebut. Di mana setiap file yang di kirimkan melalui aplikasi whatsapp

maka file tersebut akan mengalami kompresi file sehingga akan terjadi perubahan data.

Untuk pembanding dengan penelitian ini, pada penelitian selanjutnya dapat menerapkan metode steganografi lain untuk melihat hasil pengujian dengan tiga proses perpindahan data yang dilakukan.

DAFTAR PUSTAKA

Abdul, M., Almayyahi, M., Majeed, M. A., & Sulaiman, R. (2015). An Improved Lsb Image Steganography Technique Using Bit-Inverse In 24 Bit Colour Image. *Journal of Theoretical and Applied Information Technology*, *80*(2). https://www.researchgate.net/publication/285603382

Babu, L., John, J. S., D, P. B., & DivakaraMurthy, H. S. (2013). Steganographic Method for Data Hiding in Audio Signals with LSB & DCT. In *International Journal of Computer Science and Mobile Computing* (Vol. 2, Issue 8). www.ijcsmc.com

Faris, F. A. E. F., Febi, F. Y., Iwan, I. I., & Pizaini, P. (2023). Kombinasi algoritma kriptografi vigenere cipher dengan metode zig-zag dalam pengamanan pesan teks. *Jurnal CoSciTech (Computer Science and Information Technology)*, *4*(1), 182–192. https://doi.org/10.37859/coscitech.v4i1.4787

Handoyo, A. E., Setiadi, D. R. I. M., Rachmawanto, E. H., Sari, C. A., & Susanto, A. (2018). Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA. *Jurnal Teknologi Dan Sistem Komputer*, *6*(1), 37–43. https://doi.org/10.14710/jtsiskom.6.1.2018.37-43

Jatmoko, C., Handoko, L. B., Sari, C. A., Rosal, D., & Setiadi, I. M. (2018). *Uji Performa Penyisipan Pesan Dengan Metode Lsb Dan Msb Pada Citra Digital Untuk Keamanan Komunikasi*. http://dinarek.unsoed.ac.id

Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A review on text steganography techniques. In *Mathematics* (Vol. 9, Issue 21). MDPI. https://doi.org/10.3390/math9212829

Mani, R. G., Parthasarathy, R., Eswaran, S., & Honnavalli, P. (2016). *A Survey on Digital Image Forensics: Metadata and Image forgeries*.

Piva, A. (2013). An Overview on Image Forensics. *ISRN Signal Processing*, *2013*, 1–22. https://doi.org/10.1155/2013/496701

Sina, D. R., Kiu, G. A., Djahi, B. S., & Pandie, E. S. Y. (2022). Aplikasi Keamanan Pesan (.Txt) Menggunakan Metode Triple DES Dan Metode Kombinasi LSB Dan BLUM-BLUM-SHUB. *Jurnal Komputer Dan Informatika*, *10*(2), 204–209. https://doi.org/10.35508/jicon.v10i2.8465

Utomo Wahyu Mulyono, I., Kusumawati, Y., & Kurnia Ningrum, N. (2023). *Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher*. *14*(1), 2777–0648.

Varol, A., Institute of Electrical and Electronics Engineers. Portugal Section., & Institute of Electrical and Electronics Engineers. (2019). *Digital Forensics: Focusing on Image Forensics* (2019th ed.).

Wiryawan, I. G., Sariyasa, & Gunadi, I. G. A. (2019). Steganografi Berdasarkan Metode Least Significant Bit (Lsb) Pada Citra Digital Denga Teknik Kompresi Lossless. *Jurnal Ilmu Komputer Indonesia (JIKI)*, *4*(1). www.image-resource.com

Xu, B., Wang, X., Zhou, X., Xi, J., & Wang, S. (2016). Source camera identification from image texture features. *Neurocomputing*, *207*, 131–140. https://doi.org/10.1016/j.neucom.2016.05.012

Yanti, F., & Budayawan, K. (2023). Implementasi Steganografi Menggunakan Metode Least Significant Bit (Lsb) dalam Pengamanan Informasi pada Citra Digital. *Jurnal Vocational Teknik Elektronika Dan Informatika*, *11*(1), 63–70. http://ejournal.unp.ac.id/index.php/voteknika/index