Journal of Information System Research (JOSH)
Volume 6, No. 4, Juli 2025, pp 2218−2226
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i4.7900

Implementation of Digital Image Steganography Application Using The Least Significant Bit Method Based on Android Via Telegram

Abdullah Muhajir*, Muhamad Santoso, Bani

Ilmu Komputer, Teknik Informatika, Universitas Pamulang, Tangerang Selatan
Jl. Suryakencana No.1, Pamulang Bar., Kec. Pamulang, Kota Tangerang Selatan, Banten, Indonesia
Email: [1,*]dosen02602@unpam.ac.id, [2]dosen02593@unpam.ac.id, [3]dosen02381@unpam.ac.id
Corresponding Author Email: dosen02602@unpam.ac.id
Submitted: **07/07/2025;** Accepted: **31/07/2025;** Published: **31/07/2025**

Abstract−Confidentiality and security of information on globalization is increasingly becoming a vital needs in various aspects of life. Any information would have a higher value if the concerning aspects of business decisions, security, or public interest. Where information-such information surely will be much sought after by various parties also have an interest in it. How to implement a data security system so that the data can be hidden in addition, can also be maintained in strict confidence from unauthorized parties. Designing applications Android-based steganography to hide documents by using the method of Least Significant Bit (LSB). This application can be expected to add to the knowledge of how to insert the document doc, xls, ppt, pdf and how to create application programs that can hide the document in the image, as well as developing the ability of the author to design the program mobile applications. The process of document confidentiality can be maintained this is due to the existence of the document is stored in a format that is different from the results of the prior encryption or already in the pasted file encryption is still the same.

Keywords: Steganography; The Least Significant Bit (LSB); Images; Files; Android

1. INTRODUCTION

Steganography is the art of hiding information or embedded messages in a cover object which can be in the form of text, images, audio, video and others)[1]. This is closely related to data security. In information and communication technology, steganography is a technique and art of concealment that utilizes digital formats meaning that digital information is hidden behind other digital information so that the actual digital information is not visible[2].

The purpose of steganography is a technique of hiding information into a container (media) so that the hidden data is difficult to recognize by the human senses[3]. This technique makes others unaware that there is important information that we send hidden in other media, such as images, audio, and video. If the information that has been hidden in a media is stolen, the thief will not necessarily be able to know the information contained in it, because there is a password (key) to be able to open the information contained in the information media[4]. The password is only known to the sender and receiver. One of the steganography methods is Spread Spectrum. The spread spectrum method transmits a narrow-band information signal into a wideband channel with frequency spread[5]. The frequency spread itself serves to increase the level of redundancy. By increasing the level of redundancy, the code is not easy to crack[6]. There are four main components of steganography, namely: (1) embedded message (hiddentext), which is a hidden message; (2) cover-object (covertext), which is a message used to hide embedded messages; (3) stego-object (stegotext), which is a message that already contains an embedded message; (4) stego-key, which is the key used to insert messages and extract messages from stegotext[7].

Some examples of international journals and published research include: Kriti Saroha and Pradeep Kumar Singh researched special steganography of audio files using LSB, Sujay Narayana and Gaurav Prasad researched steganography with LSB on image files only, Pradeep Kumar Singh and R.K.Aggrawal used LSB on image to audio files, Dian Dwi Hapsari and Lintang Yuniar Banowosari used LSB on images, Saurabh Singh and Gaurav Agarwal used LSB in videos, Rahul Rishi et al steganography in images using the Mode and Multiple Technique method that is still being developed from LSB, and many other journals and research are still using LSB in steganography research[8].

In theory, all digital files in general that exist in a computer can be used as embedded messages or hidden ones, such as image files, audio, text, video and so on. The file has redundant bits of data as a characteristic of a digital file that can be modified[9].

Various studies on steganography have actually been carried out and continue to be developed by researchers using various steganography methods[10]. The most widely used and encountered method is the Least Significant Bit (LSB) method[11]. This is because LSB is a method that has advantages such as, easy and fast algorithmically, all types of digital files can be used as sampling and messages that can be hidden are messages that are relatively large in size that can be inserted into all types of digital files[12]. However, most of the research that is generally conducted is still separate or limited to one type of digital file only, even to only one type of digital file format, although research on file types and other digital file formats is still conducted. This will certainly be troublesome for users who want to insert information or messages with different files or file formats[13].

Journal of Information System Research (JOSH)
Volume 6, No. 4, Juli 2025, pp 2218−2226
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i4.7900

When looking at applications from modern devices or mobile devices, it is not uncommon for people to see the features or technology offered from an application[14]. In this case, Telegram and WhatsApp, which are social media and communication applications, both offer advanced features in modern communication technology[15].

The difference regarding the app features on Telegram is that it allows users to use multi-devices independently without the mobile app running on iOS, Android, Windows, and Linux. Unlike WhatsApp which requires a mobile application that runs using multi-devices on other devices[16].

With some of the information above, security and confidentiality issues are one of the important aspects of sending messages or information. Therefore, a data security is needed, which is able to maintain the security of the data content to cover security gaps[17]. To facilitate the process of hiding document messages into images, a steganography application was designed with the Least Significant Bit (LSB) method. The application is designed with three processes, namely encode, decode and sendimage[18]. The encoding process goes through several stages, namely selecting documents in .doc, .xls, .ppt, .pdf formats and then inserting them into the image. To open the file, a decoding process is required which is carried out through several stages, namely looking for images that have been inserted into the file or document and then the file can only be opened[19].

2. RESEARCH METHODOLOGY

2.1 System Analysis

This stage is carried out by gathering the requirements for the steganography application. Data collection was obtained through literature review and observation. This research used a software engineering method with a waterfall model approach, which has several stages in the software development process, namely:

a. Prosedure Encode Form

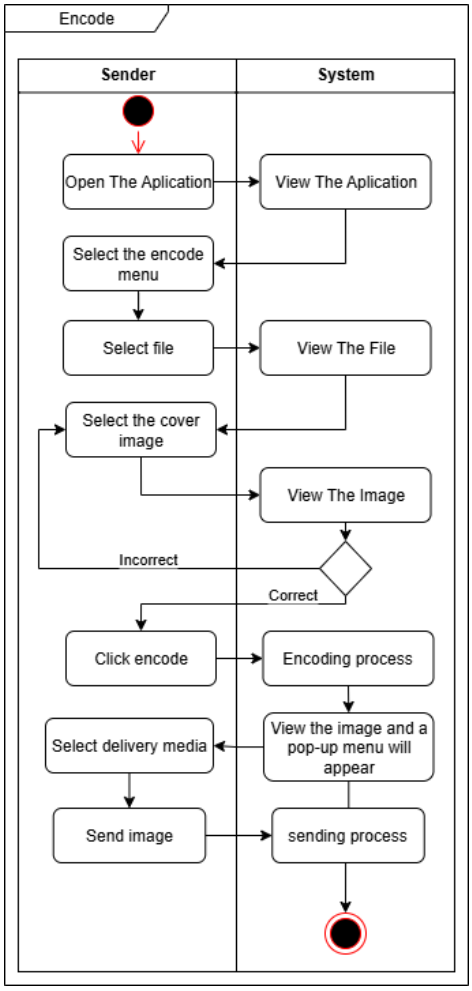

Figure 1. Encode

Figure 1, the user or sender opens the application then the system views the application Flow from the proposed application in order to maintain communication security, starting from the user or sender opening the application then selecting the encode form menu, then selecting the file contained in the storage media, after that selecting the image file storage that will be inserted in the image media if the size is small, it will choose

Journal of Information System Research (JOSH)
Volume 6, No. 4, Juli 2025, pp 2218−2226
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i4.7900

a larger image, Followed by clicking the encode button then the application will process it, after which a popup menu will appear for sending files that have been encoded[20].

b. Prosedure Decode Form
The user opens the LSB application and then selects the menu, then selects the home menu and then selects the decode tab, after that select/browse the encoded file in the storage media, after selecting the encoded file then click decode file, wait until the decode is complete[21].

c. Prosedure About
The user opens the LSB alias and then selects the about menu, then it appears about the LSB application.

d. Procedure Help
The user selects the LSB application and then opens the help menu, then it will appear what applications can be used.

e. Procedure Exit
The user selects the application lsb and then the exit menu to exit the application

2.2 Enkripsi Least Significant Bit Algorithm

Figure 2, Stages of the encryption algorithm with the Least Significant Bit:

```
1. Tampilkan Layar Encode
2. Input Pilih
3. If Pilih = "Telusur" Then
   4. Tampil Layar Telusur
   5. Ambil File/document
6. Else
   8. Kembali ke baris 2
8. Ind If
9. Input Pilih
10. If Pilih = "Telusur" Then
   11. Tampil Layar Browser
   12. Ambil Gambar/Image
14. Ind If
15. Input Pilih
16. If Pilih = "Encode" Then
   16. Tampil Gambar Asli dan HasilEncoding
17. End If
18. Input Pilih
   19. Pilih = "Tutup" Then
   20. Unload Layar Encode
   21. Kembali Ke Layar Menu Utama
22. Else
23. 23. Kembali ke baris 17
24. End If
```

Figure 2. Stages of encryption algorithms with Least Significant Bit

2.3 Algoritma Deskripsi Least Significant Bit

Figure 3, Stages of the description algorithm with the Least Significant Bit:

Process:

```
1.  Tampilkan Layar Decode
2.  Input Pilih
3.  If Pilih = "Telusur" then
4.  Tampil Layar Browser
5.  Ambil gambar stego image
6.  Else
7.  Kembali ke baris 2
8.  End If
9.  Input Pilih
10. If Pilih = "Decode" Then
11.     Tampil Lokasi Dimana File Decode Disimpan
12. Else
13. Kembali Ke baris 9
14. End If
15. Input Pilih
16. If Pilih = "Back" Then
17.     Unload Layar Decode
18.     Kembali Ke Layar Menu Utama
19. End if
```

Figure 2. Stages of Description Algorithm

2.4 Algoritma Deskripsi Least Significant Bit

Figure 4, The Least Significant Bit (LSB) process in this thesis is as follows. The first step is to select the image file to use as the medium for the insertion. In this thesis, the file format used is an image file with the *TIFF extension. Place the file to be used as the media in one folder along with the m-file matlab LSB[22].

Journal of Information System Research (JOSH)
Volume 6, No. 4, Juli 2025, pp 2218−2226
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i4.7900

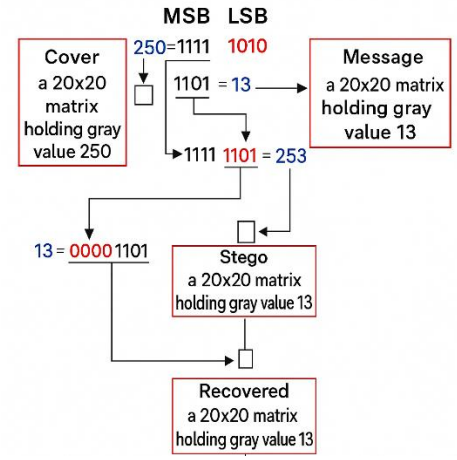

Figure 3. LSB Method Process

3. RESULT AND DISCUSSION

3.1 Running System

The system that is running as a whole is very necessary for the author to be able to know the weaknesses of the system that is running, both from the way the system works and the implementation and everything involved in the system. For the creation of a new information system, it must be more programmatic and structured[23].

3.1.1 Activity Diagram Running System

Activity is a description of the various flows of activity in the system that are being designed, how each flow starts, decisions that may occur, and how they end. Here is the activity diagram that is running.

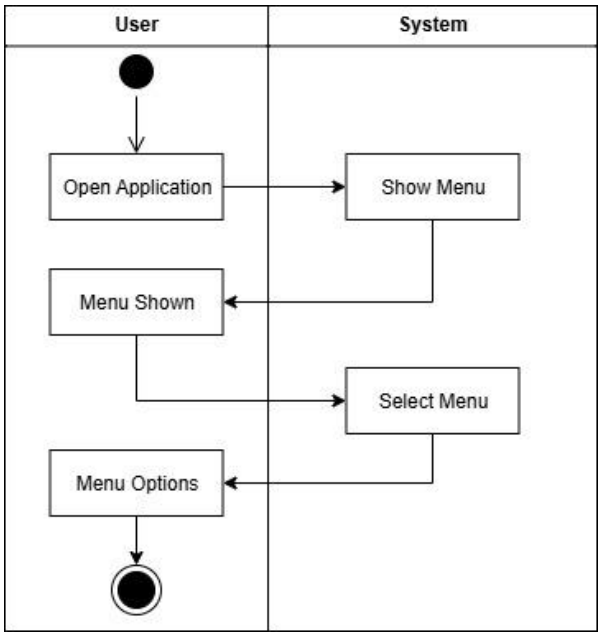

Figure 4. Activity Diagram running system

Figure 5, explains the activity diagram of the system that was running before this study was conducted.

3.2 Analysis of the proposed system

The proposed system analysis will be explained with the UML design as a system design tool. UML is a set of structures and techniques for modeling object-oriented program (OOP) design and its applications. UML is a combination of modeling languages developed by Booch, Object Modeling Technique (OMT) and Object Oriented Software Engineering (OOSE) .

The Booch method from Grady Booch is very well known as the Design Object Oriented method. This method makes the process of analysis and design into four interactive stages, namely: identification of classes and objects, semantic identification of the relationship between objects and classes.

Journal of Information System Research (JOSH)
Volume 6, No. 4, Juli 2025, pp 2218−2226
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i4.7900

The advantage of this method is in the notation that supports all OOP concepts. Jacobson's OOSE method places more emphasis on use cases. OOSE has three stages, namely creating a requirement and analysis model, design and implementation, and a test model. (Antonio, 2019)
Contains the results of application implementation or program results (which are important only), or results from method testing.

3.2.1 Proposed System Procedure

1. Prosedure Encode Form
   The user will open the LSB application, then select the pili home application menu and the user select the Encode tab menu, then select the document file if it has, then select the image file for the media, if the image file is to be inserted then click the encode button then the file will appear
2. Prosedure Decode Form
   User opens the LSB application and then selects the menu, then selects the home menu and then selects the decode tab, after that select/browse the encoded file in the storage media, after selecting the encoded file then click decode file, wait until the decode is finished
3. Prosedure About
   The user opens the LSB alias and then selects the about menu, then it appears about the LSB application.
4. Prosedure Help
   The user selects the LSB application and then opens the help menu, then it will appear what applications can be used
5. Prosedure Exit
   The user selects the application lsb and then the exit menu to exit the application

3.2.2 Use Case

A use case diagram is an abstraction of the interaction between the system and the actor. The use case works by describing the type of interaction between the user of a system and the system itself through a story of how a system is used. The proposed use cases are as follows:

Table 1. Specification of Use Case Diagram

Actor	Description
Sender or receiver	Encode Form The sender encodes the file to be sent to the recipient Decode Form The recipient decodes the file received from the sender and obtains the result of the encryption file About Contains only About the Application Help This menu contains files that can be used and how to Exit Exit menu

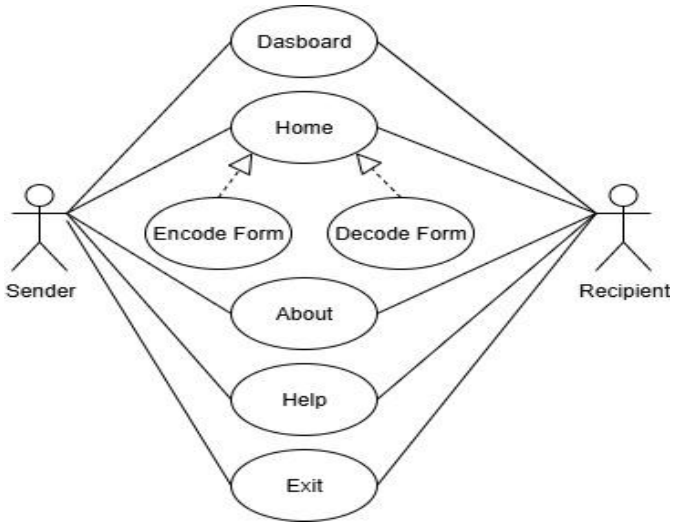

Figure 5. Use Case Diagram Proposal

Figure 6, is a use case diagram in this study.

Journal of Information System Research (JOSH)
Volume 6, No. 4, Juli 2025, pp 2218−2226
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i4.7900

3.3 Implementation

The implementation of system applications is useful to find out whether the program that has been created can run optimally, for that the program must be tested first. The way to use this application and the appearance that will appear when the application is run will be explained as follows :

1. Home screen display

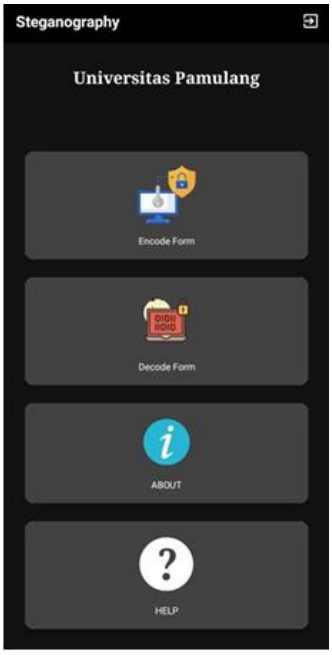

Figure 6. Main menu screen display

Figure 7, this screen will appear after the home screen and splashscreen process runs, on this screen users can choose from five menu options available. Among them are:

a. Home menu, this menu is used to go to the Encode Form and Decode Form screens, where the Encode Form is used for the insertion of steganography files and Decode Form is used to return the filr that has been inserted into the stegano file.
b. About Application, this menu is used to show information about the application creator
c. Help, this menu is used to show information about the steganography application usage guide. and
d. Exit, this menu is used to exit the running steganography application.

2. Display of the encode form screen

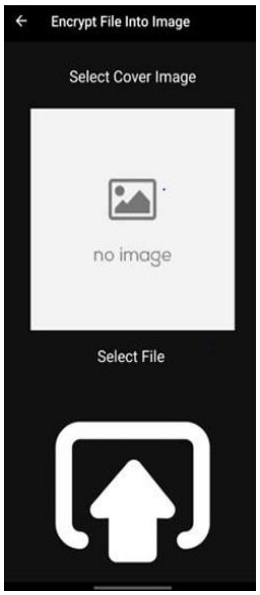

Figure 7. Encode Form Screen Display

Figure 8 is encoded screen display image. On this screen, there are 3 (three) columns consisting of:

a. File Column: This column is used to indicate the file name of the selected document after the browser process has been performed.

Journal of Information System Research (JOSH)
Volume 6, No. 4, Juli 2025, pp 2218−2226
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i4.7900

b. Cover Image Column, This column is used to indicate the name of the image file that will be used as a stegano cover image after the image browsing process is carried out.
c. Save to Column : This column is used to name the stego image file into the Embed folder.
d. Encode Button, This button is used to start the process of inserting a document or file into an image and the original image and its encoding image appear.
e. Close Button, This button is used to close the Form Encode.

3. **Form decode screen display**

Figure 8. Form Decode Screen Display

Figure 9 is Screenshot of the decode form screen display. This screen is used to extract stegano image files that have gone through the previous encoding process . On this screen, there is a Load Image column that indicates the name of the stego image file that has been selected from the browsing process. After that, the decode button is used to retrieve messages hidden in the cover image into the Retrieve folder.

4. About App screen view

Figure 9. Screen Display About App

Figure 10 is the About App screen display contains information about the name of this application, the year of creation, the name of the creator and the information of the faculty of the creator.

Journal of Information System Research (JOSH)
Volume 6, No. 4, Juli 2025, pp 2218−2226
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i4.7900

5. Help screen display

Figure 10. Help Screen Display

Figure 11 is screen contains a guide on how to Encode, Decode, Advantages and disadvantages of this steganography application.

6. Exit screen display

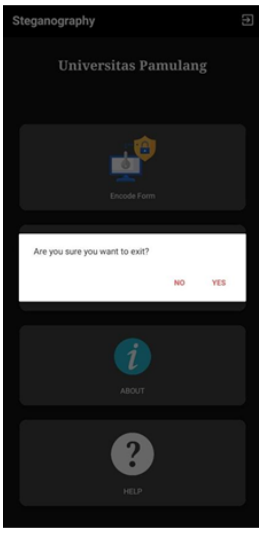

Figure 11. Exit Screen Display (This screen contains the exit of the app)

Figure 12 is screenshot of the decode form screen display.

4. CONCLUSION

Based on the conclusions obtained from the design, manufacture, testing, and analysis of this steganography application program, it can be concluded that by using the LSB (Least Significant Bit) method, data or files can be securely hidden so that unauthorized parties cannot breach the security or intercept the message, especially in internet-based communications, as others will only see an ordinary image file. Additionally, the encoded image file becomes larger in size compared to the original due to the insertion of hidden data; if someone is familiar with image file structures, they may notice irregularities in the file.

REFERENCES

[1] M. O. Abdillah, O. A. Pane, and F. R. A. Lubis, “Implementasi Keamanan Aset Informasi Steganografi Menggunakan Metode Least Significant Bit (LSB),” J. Sains dan Teknol., vol. 3, no. 1, pp. 40–46, Jan. 2023, doi: 10.47233/jsit.v3i1.482.
[2] F. Yanti and K. Budayawan, “Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) dalam

Journal of Information System Research (JOSH)
Volume 6, No. 4, Juli 2025, pp 2218−2226
ISSN 2686-228X (media online)
https://ejurnal.seminar-id.com/index.php/josh/
DOI 10.47065/josh.v6i4.7900

Pengamanan Informasi pada Citra Digital," Voteteknika (Vocational Tek. Elektron. dan Inform., vol. 11, no. 1, p. 63, Mar. 2023, doi: 10.24036/voteteknika.v11i1.121968.
[3] I. R. Lie and D. Alamsyah, "Pernerapan Algortima Diffie-Hellman pada Steganografi Least Significant Bit," MDP Student Conf., vol. 2, no. 1, pp. 234–243, 2023, doi: 10.35957/mdp-sc.v2i1.4107.
[4] S. Sandfreni, M. B. Ulum, and A. H. Azizah, "Analisis Perancangan Sistem Informasi Pusat Studi Pada Fakultas Ilmu Komputer Universitas Esa Unggul," Sebatik, vol. 25, no. 2, pp. 345–356, Dec. 2021, doi: 10.46984/sebatik.v25i2.1587.
[5] Sondang Sibuea, Mohammad Ikhsan Saputro, Agie Annan, and Yohanes Bowo Widodo, "Aplikasi Mobile Collection Berbasis Android Pada Pt. Suzuki Finance Indonesia," J. Inform. Dan Tekonologi Komput., vol. 2, no. 1, pp. 31–42, Mar. 2022, doi: 10.55606/jitek.v2i1.185.
[6] K. Wijaya, B. Lansky, C. A. Dewi, Rojali, and G. Z. Nabiilah, "Time-Based Steganography Image with Dynamic Encryption Key Generation," Procedia Comput. Sci., vol. 227, pp. 233–242, 2023, doi: 10.1016/j.procs.2023.10.521.
[7] A. A. Permana and H. Amna, "Implementasi Steganografi File Citra Digital Menggunakan Metode Least Significant Bit," J. Tek., vol. 11, no. 1, pp. 62–72, 2022, doi: 10.31000/jt.v11i1.6161.
[8] V. Wati, H. Sa'diyah, and D. Ariyus, "Pendekatan Stego-Kripto Mode Cipher Block Chaining Untuk Pengamanan Informasi Pada Citra Digital," JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer), vol. 5, no. 2, pp. 197–204, Feb. 2020, doi: 10.33480/jitk.v5i2.1160.
[9] Y. Bagus Pratama and F. Fachri, "Analisis Keamanan Steganografi Pada Gambar Yang Diunggah Ke Media Sosial Menggunakan Least Significant Bit (Lsb)," JATI (Jurnal Mhs. Tek. Inform., vol. 9, no. 1, pp. 725–732, 2024, doi: 10.36040/jati.v9i1.12370.
[10] Y. D. Wijaya and M. W. Astuti, "Pengujian Blackbox Sistem Informasi Penilaian Kinerja Karyawan Pt Inka (Persero) Berbasis Equivalence Partitions," J. Digit. Teknol. Inf., vol. 4, no. 1, p. 22, Mar. 2021, doi: 10.32502/digital.v4i1.3163.
[11] S. Lutfi and R. Rosihan, "Perbandingan Metode Steganografi Lsb (Least Significant Bit) Dan Msb (Most Significant Bit) Untuk Menyembunyikan Informasi Rahasia Kedalam Citra Digital," JIKO (Jurnal Inform. dan Komputer), vol. 1, no. 1, pp. 34–42, Apr. 2018, doi: 10.33387/jiko.v1i1.1169.
[12] I. Kurniawan, M. R. Maulana, and C. Yulianto Rusli, "Analisis Pesan Steganograph Pada Setelah Pengiriman File Pada Platform Social Media," IC-Tech, vol. 18, no. 2, pp. 41–48, Oct. 2023, doi: 10.47775/ictech.v18i2.278.
[13] A. Olawale, A. Adebayo, and G. Arome, "Embedding Text in Audio Steganography System using Advanced Encryption Standard, Text Compression and Spread Spectrum Techniques in Mp3 and Mp4 File Formats," Int. J. Comput. Appl., vol. 177, no. 41, pp. 46–51, Mar. 2020, doi: 10.5120/ijca2020919914.
[14] I. F. Ashari, L. R. Siwi, H. Londata, and I. Wicaksono, "Analisis Dan Perbandingan Steganografi Pada Media Audio Dan Gambar Menggunakan Lsb Dan Rc4," J. ELTIKOM, vol. 7, no. 1, pp. 67–78, Jun. 2023, doi: 10.31961/eltikom.v7i1.583.
[15] S. F. R. Salsabila, A. I. Hadiana, and F. R. Umbara, "Penerapan Kriptografi Advanced Encryption Standard (AES) dan Steganografi Spread Spectrum Untuk Mengamankan Pesan Dalam Gambar," J. Informatics Commun. Technol., vol. 5, no. 2, pp. 196–209, Dec. 2023, doi: 10.52661/j_ict.v5i2.216.
[16] Aqilah Syaima' Fadel, Rianto David Saputra, Y. Fatma, and Risky Nanda Putra, "Analisis keamanan steganografi teks dengan metode lsb (least significant bit) pada citra digital," J. CoSciTech (Computer Sci. Inf. Technol., vol. 5, no. 1, pp. 36–41, Apr. 2024, doi: 10.37859/coscitech.v5i1.6759.
[17] A. Prameshwari and N. P. Sastra, "Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen," Eksplora Inform., vol. 8, no. 1, p. 52, Sep. 2018, doi: 10.30864/eksplora.v8i1.139.
[18] N. Subramanian, O. Elharrouss, S. Al-Maadeed, and A. Bouridane, "Image Steganography: A Review of the Recent Advances," IEEE Access, vol. 9, pp. 23409–23423, 2021, doi: 10.1109/ACCESS.2021.3053998.
[19] E. Nirmala, "Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android," J. Inform. Univ. Pamulang, vol. 5, no. 1, p. 36, Mar. 2020, doi: 10.32493/informatika.v5i1.4646.
[20] A. Z. Agung Wahyu Laksono, Sitti Suhada, "Implementasi Metode Least Significant Bit (Lsb) Dalam Teknik Steganografi Pada Citra Digital Menggunakan Matlab," Diffus. J. Syst. Inf. Technol., vol. 4, no. 1, pp. 1–14, Jul. 2024, doi: https://doi.org/10.37031/diffusion.v4i1.24194.
[21] M. K. Ridwan, W. F. Pattipeilohy, and S. Sanwani, "Aplikasi Keamanan Document Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (Dct) Pada Perusahan Alat Berat," JITK (Jurnal Ilmu Pengetah. dan Teknol. Komputer), vol. 5, no. 2, pp. 177–182, Feb. 2020, doi: 10.33480/jitk.v5i2.1033.
[22] I. Riadi, S. Sunardi, and D. Aryanto, "Steganografi Video Digital dengan Algoritma LSB (Least Significant Bit) dan Rijndael," J. Innov. Inf. Technol. Appl., vol. 2, no. 02, pp. 127–134, Dec. 2020, doi: 10.35970/jinita.v2i02.361.
[23] I. U. W. Mulyono, Y. Kusumawati, and N. K. Ningrum, "Analisa Visual Citra Hasil Kombinasi Steganografi dan Kriptografi Berbasis Least Significant Bit Dalam Cipher," J. Masy. Inform., vol. 14, no. 1, pp. 16–28, Jun. 2023, doi: 10.14710/jmasif.14.1.51484.