HANIF
Journal of Information Systems
https://journal.ilmubersama.com/index.php/hanif

Click here and write your Article Category

Implementation of the Least Significant Bit (LSB) Method for Data Security in a Mandailing Language Dictionary

Zulkifli Hasibuan [1], Mhd Zulfansyuri Siambaton [2], Heri Santoso[3]

[1 2] Department of Information Technology, Faculty of Engineering, Universitas Islam Sumatera Utara, Medan, 20217, North Sumatra, Indonesia
[3] Department of Information System, Faculty of Computer Science, Universitas Islam Negeri Medan, Medan, 20136, North Sumatra, Indonesia

ARTICLE INFORMATION

Received: February 00, 00
Revised: March 00, 00
Available Online: April 00, 00

KEYWORDS

Steganography; Least Significant Bit (LSB); Data Security; Mandailing Language Dictionary

CORRESPONDENCE

Phone: +62 852-7698-8902

E-mail: zulkiflihasibuan0202@gmail.com

A B S T R A C T

The development of information technology has encouraged the digitalization of various forms of information, including regional language dictionaries. The Mandailing Language Dictionary in digital form makes it easier for people to learn and preserve regional languages. However, digital data storage also poses risks to data security, such as theft, duplication, or modification of data by unauthorized parties. Therefore, a method is needed to improve data security in digital dictionary systems. This study aims to implement the Least Significant Bit (LSB) method as a steganographic technique to hide text data within digital images in the Mandailing Language Dictionary system.

The LSB method works by embedding text data into the least significant bit of digital image pixels so that the existence of the data is not easily detected visually. This research produces a web-based system capable of performing encoding (data embedding) and decoding (data extraction) processes on digital images. The encoding process is carried out by converting text into binary form and embedding it into the red color channel of each image pixel using the LSB method. In the decoding process, the system reads the LSB bits from the image to retrieve the embedded text data.

The testing results show that the embedded data can be accurately extracted without any changes, and the image quality before and after the embedding process does not show significant differences. Therefore, the LSB method can be used as a solution to improve data security in the Mandailing Language Dictionary system.

INTRODUCTION

The concept of data security encompasses three main aspects: confidentiality, integrity, and availability of data. Data confidentiality relates to the privacy and protection of data from unauthorized parties. Information classified as confidential includes personal data, health data, financial data, corporate confidential data, and government data [1].

Steganography is a technique as well as a field of study used to conceal messages using certain methods so that they are not easily detected by other parties [2]. The application of steganography aims to minimize suspicion, as the secret message is not displayed directly but is instead embedded into another medium as a carrier [3].

https://doi.org/10.12345/xxxxx

Steganography techniques include several methods for embedding hidden messages. One of them is the Least Significant Bit (LSB) method, which is used in the spatial domain [4].

A digital image is an electronic image obtained from various types of documents such as books, photographs, or segments of video and audio. The process used to convert an analog image into a digital image is called digitization [5].

Digitization is the process of converting images, text, or audio originating from physical objects into electronic data that can be stored and processed for other purposes. A digital image is a numerical representation (mostly in binary form) of a two-dimensional image. An image can be defined as a two-dimensional function f(x,y), where x and y are coordinates on a plane, and the value of the function f at each coordinate pair (x,y) is referred to as the intensity or gray level of the image. When the values of x, y, and the intensity function f are limited to discrete values, the image can be classified as a digital image.[6].

The Least Significant Bit (LSB) is a technique that replaces the rightmost bit with the bit of the data to be hidden. Each byte (1 byte) consists of 8 bits arranged in the order b7b6b5b4b3b2b1b0. The b0 bit has the smallest value or is the least significant (Least Significant Bit/LSB), while the b7 bit has the largest value or is the most significant (Most Significant Bit/MSB) [7].

METHOD

Steganogrphy

To ensure that the steganography process runs effectively, there are several key criteria that must be met, namely fidelity, imperceptibility, and recovery [8]. Fidelity refers to the ability of the cover media to maintain its original quality without significant changes after the message embedding process. Imperceptibility indicates that the stego media is difficult to distinguish from the original media, so the presence of the hidden message cannot be visually detected. Meanwhile, recovery refers to the system's ability to accurately extract the embedded message, ensuring that data accuracy and integrity are preserved [9].

Steganography techniques include various methods for embedding hidden messages. One of them is the Least Significant Bit (LSB) method, which is used in the spatial domain [4].

Least Significant Bit (LSB)

The steganography technique using the modified Least Significant Bit (LSB) method is one of the simplest approaches for embedding information into a digital image (cover medium) [10]. If an image that reconstructs the same message as the original (lossless compression) is converted into JPEG, which uses lossy compression, the hidden information within the LSB may be destroyed upon recompression. In a binary structure, there are the Most Significant Bit (MSB) and the Least Significant Bit (LSB).

Example: [1 1 0 1 0 0 1 0]

The first digit represents the MSB, while the last digit represents the LSB. The most suitable bit to modify is the LSB, since such a change only increases or decreases the byte value by one from its original value.

To hide an image using LSB, each byte in a 24-bit image can store 3 bytes in each pixel. An image with a resolution of 1,024 × 768 has the potential to hide up to 2,359,296 bits of information [11].

Encoding LSB

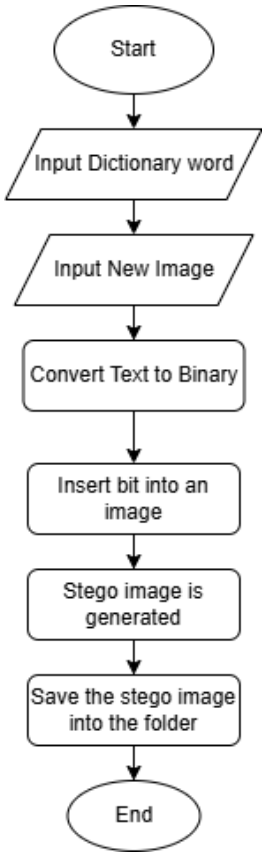

Figure 1. Encoding LSB

Explanation for figure 1:

1. Start
   The process begins.
2. Input Dictionary Word
   The user enters a word (and possibly its meaning) from the dictionary to be secured.
3. Input New Image
   The user uploads or selects a new image that will be used as the cover media for hiding the data.
4. Convert Text to Binary
   The input text is converted into binary format (e.g., ASCII 8-bit) so it can be embedded into the image.
5. Insert Bit into an Image
   The binary data is embedded into the image by modifying the Least Significant Bit (LSB) of the image pixels.
6. Stego Image is Generated
   After the embedding process, a new image (stego image) containing the hidden data is produced.
7. Save the Stego Image into the Folder
   The stego image is saved into a specified folder or storage location.
8. End
   The process is completed.

Fowchart LSB

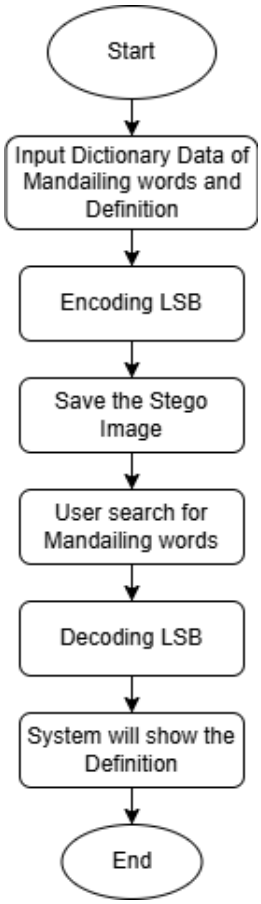

Figure 1. Flowchart LSB

Explanation for figure 1

1. Start
   The process begins.
2. Input Dictionary Data of Mandailing Words and Definition
   The system inputs data consisting of Mandailing words along with their meanings or definitions.
3. Encoding LSB
   The input data is embedded into a digital image using the Least Significant Bit (LSB) method.
4. Save the Stego Image
   The image that already contains the hidden data (stego image) is saved in the system.
5. User Search for Mandailing Words
   The user searches for a specific Mandailing word in the system.
6. Decoding LSB
   The system extracts the hidden data from the stego image using the LSB decoding process.
7. System Will Show the Definition
   The system displays the meaning or definition of the searched word to the user.
8. End
   The process is completed.

RESULTS AND DISCUSSION

This study produces a data security system for a Mandailing Language Dictionary by implementing the Least Significant Bit (LSB) steganography method. The developed system is capable of performing the embedding (encoding) and extraction (decoding) processes of dictionary text data into digital image media without causing significant visual changes to the cover image.

The data used in the testing process consists of Mandailing dictionary text, with the example word “horas”. The text is converted into 8-bit ASCII binary form, then embedded into the least significant bits (LSB) of the red channel values in each pixel of the digital image. To mark the end of the data, a special marker in the form of an EOF byte (00000000) is used.

Tables

Table 1. Data Table

Character	ASCII (Decimal)	ASCII (Biner-8 bit)
h	104	01101000
o	111	01101111
r	114	01110010
a	97	01100001
s	115	01110011
EOF	-	00000000

Table 2. Table of New R Values and Original R Values

Piksel	R asli	Biner R asli	Bit teks	R baru bin	R baru desimal
1	200	11001000	0	11001000	200
2	123	01111011	1	01111011	123
3	255	11111111	1	11111111	255
4	10	00001010	0	00001010	10
5	61	00111101	1	00111101	61
6	70	01000110	0	01000110	70
7	84	01010100	0	01010100	84
8	90	01011010	0	01011010	90
9	110	01101110	0	01101110	110
10	50	00110010	1	00110011	51
11	240	11110000	1	11110001	241
12	33	00100001	0	00100000	32
13	77	01001101	0	01001100	76
14	88	01011000	0	01011000	88
15	99	01100011	0	01100010	98
16	101	01100101	1	01100101	101
17	202	11001010	0	11001010	202
18	212	11010100	1	11010101	213
19	123	01111011	1	01111011	123

 https://doi.org/10.12345/xxxxx

20	134	10000110	0	10000110	134
21	56	00111000	0	00111000	56
22	67	01000011	0	01000010	66
23	89	01011001	1	01011001	89
24	90	01011010	0	01011010	90
25	100	01100100	0	01100100	100
26	101	01100101	1	01100101	101
27	102	01100110	1	01100111	103
28	103	01100111	1	01100111	103
29	104	01101000	0	01101000	104
30	105	01101001	0	01101000	104
31	106	01101010	1	01101011	107
32	107	01101011	0	01101010	106
33	108	01101100	0	01101100	108
34	109	01101101	1	01101101	109
35	110	01101110	1	01101111	111
36	111	01101111	0	01101110	110
37	112	01110000	0	01110000	112
38	113	01110001	0	01110000	112
39	114	01110010	0	01110010	114
40	115	01110011	1	01110011	115
41	116	01110100	0	01110100	116
42	117	01110101	0	01110100	116
43	118	01110110	0	01110110	118
44	119	01110111	0	01110110	118
45	120	01111000	0	01111000	120
46	121	01111001	0	01111000	120
47	122	01111010	0	01111010	122
48	123	01111011	0	01111010	122

Table 3.Encoding Result

Piksel	Bit teks	R baru bin	R baru desimal
1	0	11001000	200
2	1	01111011	123
3	1	11111111	255
4	0	00001010	10
5	1	00111100	60
6	0	01000110	70
7	0	01010100	84
8	0	01011010	90

Table 4. Decoding Result

No	Byte Biner (8 bit)	Desimal	Karakter
1	01101000	104	h
2	01101111	111	o
3	01110010	114	r
4	01100001	97	a
5	01110011	115	s
6	00000000	0	EOF

System Implementation

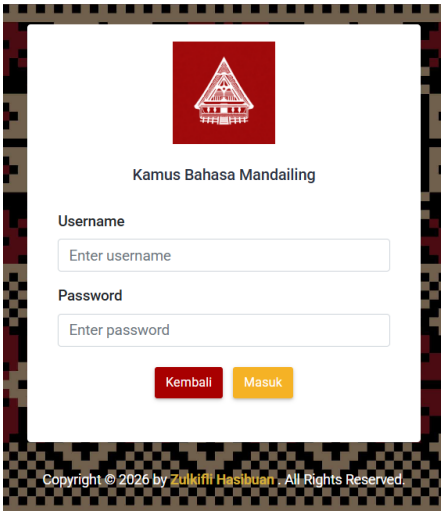

Figure 3. Login Page

Figure 3 is a displays the login page of the Mandailing Language Dictionary application, which functions as the initial gateway for users to access the system. At the top of the page, there is an application logo that represents the identity of the Mandailing Language Dictionary, followed by the application title clearly shown in the center to inform users about the system being accessed.

This page provides two input fields, namely Username and Password, which are used for user authentication. The username field is used to enter a registered username, while the password field is used to input a password as a form of access security.

Figure 4. Dashboard Page

Figure 4 is a displays the main page (dashboard) of the Mandailing Language Dictionary application after the user has successfully logged in.

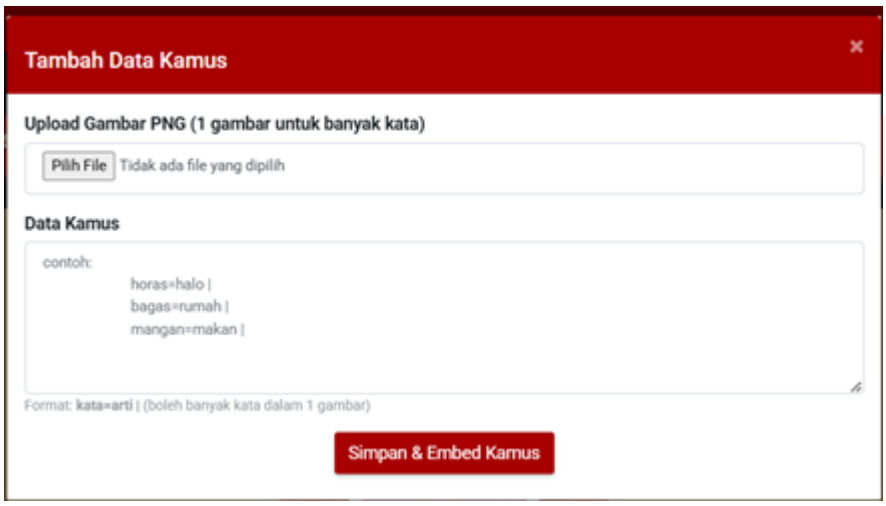

Figure 5. Dictionary Data Entry Page

Figure 5 shows the Add Dictionary Data page designed by the author as an interface for storing and securing Mandailing Language Dictionary data. On this page, the author provides a feature to upload images in PNG format, which function as a medium for storing data, where a single image file can be used to store multiple pairs of words and their meanings. This is in accordance with the concept of steganography using the Least Significant Bit (LSB) method applied in this study, which involves embedding text data into digital images.

Figure 5. User Page

Figure 5 displays the word search page of the Mandailing Language Dictionary application, which is designed by the author as the main interface for users to search for vocabulary translations.

CONCLUSION

Based on the results of the research, system design, and implementation, it can be concluded that the Least Significant Bit (LSB) method has been successfully implemented as a data security technique in the Mandailing Language Dictionary. Text data in the form of word meanings can be embedded into digital images by modifying the least significant bits (LSB) without causing significant visual changes to the image. The embedding (encoding) and extraction (decoding) processes run properly and systematically, where in the encoding stage the text data is converted into binary and embedded into image pixels, while in the decoding stage the data can be retrieved by reading the LSB bits and converted back into the original text accurately. Furthermore, the LSB method has proven effective in maintaining dictionary data security, as the data is not stored directly but hidden within the image, the extraction results are identical to the original data without any alteration, and the stego image does not show significant visual differences, thereby fulfilling security aspects such as confidentiality and data integrity.

REFERENCES

[1] Centre for Innovation Policy and Governance, “Big data, kecerdasan buatan, blockchain, dan teknologi finansial di Indonesia: Usulan desain, prinsip, dan rekomendasi kebijakan,” Direktorat Jenderal Aplikasi Informatika, 2018. [Online]. Available: https://aptika.kominfo.go.id/

[2] A. S. Fadel, R. D. Saputra, Y. Fatma, and R. N. Putra, “Analisis keamanan steganografi teks dengan metode LSB (Least Significant Bit) pada citra digital,” Jurnal CoSciTech (Computer Science and Information Technology), vol. 5, no. 1, pp. 36–41, 2024, doi: 10.37859/coscitech.v5i1.6759.

[3] F. Kurniawan, Z. Sitorus, and R. R. Putra, “Combination of cryptography and steganography in improving text data security using DES and LSB methods,” in Proceedings, pp. 352–362, 2023.

[4] E. R. Langi, A. M. Sambul, and F. D. Kambey, “Perbandingan metode Least Significant Bit dan Discrete Wavelet Transform dalam teknik steganografi pada citra batik bentenan,” Skripsi, Universitas Sam Ratulangi, 2021.

[5] H. Wijaya and K. Wilianti, “Penyisipan teks dengan metode low bit coding pada media audio menggunakan Matlab 7.7.0,” Jurnal TICOM, vol. 1, no. 3, pp. 28–35, 2013.

[6] C. Nugroho, “Steganografi pada pengiriman teks pesan gambar dengan metode Least Significant Bit dan Steghide,” Jurnal Ilmu Siber (JIS), vol. 1, no. 4, pp. 113–116, 2022.

[7] I. M. Yusup, C. Carudin, and I. Purnamasari, “Implementasi algoritma Caesar cipher dan steganografi Least Significant Bit untuk file dokumen,” Jurnal Teknik Informatika dan Sistem Informasi, vol. 6, no. 3, pp. 434–441, 2020, doi: 10.28932/jutisi.v6i3.2817.

[8] R. Fahmi, N. Imanudin, I. Kustiawan, and S. Elvyanti, “Steganografi citra digital menggunakan pendekatan Least Significant Bit dan Discrete Cosine Transform,” in Seminar Nasional Teknik Elektro, pp. 1–5, 2023. [Online]. Available: https://snte.fortei.org/list/index.php/snte/article/view/48

[9] I. U. W. Mulyono, Y. Kusumawati, and N. K. Ningrum, "Analisa visual citra hasil kombinasi steganografi dan kriptografi berbasis Least Significant Bit dalam cipher," Jurnal Masyarakat Informatika, vol. 14, no. 1, pp. 16–28, 2023, doi: 10.14710/jmasif.14.1.51484.

[10] I. G. N. B. P. Putra et al., "Penerapan steganography untuk perlindungan hak cipta menggunakan metode Least Significant Bit (LSB)," Jurnal Elektronik Ilmu Komputer Udayana, 2022.

[11] A. W. Laksono, S. Suhada, and A. Zakaria, "Implementasi metode Least Significant Bit (LSB) dalam teknik steganografi pada citra digital menggunakan MATLAB," Diffusion: Journal of System and Information Technology, vol. 4, no. 1, 2024.