ISSN cetak 2745-925X
ISSN online 2722-273X

JESSI Volume 05 Nomor 1 March 2024

DIGITAL PRIVACY PROTECTION: APPLYING STEGANOGRAPHY IN TEXT MESSAGES

Fadhlirrahman Baso[1]
[1]fadhlirrahman.baso@unm.ac.id
[1]Pendidikan Teknik Informatika dan Komputer, Universitas Negeri Makassar

Received : 15 December 2023
Accepted : 27 Februari 2024
Published : 19 Maret 2024

Abstract

Digital privacy protection has become a crucial priority in today's digital age, given the increasing risks of personal data leaks. Steganography, as a technique of concealing messages within other media, emerges as an innovative solution to safeguard text messages from unauthorized access. This article examines the implementation of steganography, specifically the Least Significant Bit (LSB) method, in protecting user's personal data. Through experiments conducted on the pelock.com website, this method successfully embedded text messages into images without compromising visual transparency. This success demonstrates the potential of steganography, especially LSB, as an effective tool in securing confidential information. Detailed implementation steps and test results indicate that steganography can serve as an additional layer in maintaining data confidentiality in the complex and evolving digital environment. The research also identifies potential avenues for further development, including the integration of artificial intelligence to enhance overall data security.
Keywords: Steganography, Least Significant Bit (LSB)

Abstrak

Perlindungan privasi digital menjadi prioritas penting di era digital saat ini, dengan risiko kebocoran data pribadi yang semakin meningkat. Steganografi, sebagai teknik penyembunyian pesan dalam media lain, muncul sebagai solusi inovatif untuk melindungi pesan teks dari akses yang tidak sah. Artikel ini mengkaji implementasi steganografi, khususnya metode Least Significant Bit (LSB), dalam melindungi data pribadi pengguna. Melalui uji coba pada website pelock.com, metode ini berhasil menyisipkan pesan teks pada gambar tanpa mengorbankan transparansi visual. Keberhasilan ini membuktikan potensi steganografi, terutama LSB, sebagai alat efektif dalam mengamankan informasi rahasia. Langkah-langkah implementasi yang terinci dan hasil uji coba menunjukkan bahwa steganografi dapat menjadi lapisan tambahan dalam menjaga kerahasiaan data di lingkungan digital yang kompleks dan terus berkembang. Penelitian ini juga mengidentifikasi potensi pengembangan lebih lanjut, termasuk integrasi kecerdasan buatan untuk meningkatkan keamanan data secara keseluruhan.
Kata kunci: Steganografi, Least Significant Bit (LSB)

ISSN cetak 2745-925X
ISSN online 2722-273X

JESSI Volume 05 Nomor 1 March 2024

1. Introduction

Digital Privacy Protection is an effort made to maintain the confidentiality of personal information in the ever-growing digital era. This confidentiality is related to the claims of individuals, groups or institutions regarding privacy through their privacy rights. Privacy itself can be defined as "the claim of individuals, groups, or institutions to determine when, how, and to what extent information about them is communicated to others." The right to privacy includes several aspects, such as humidity, confidentiality, and access restrictions [1].

In the era of information technology, protecting the right to privacy is very important to maintain political, spiritual and religious freedom. Therefore, understanding and protecting privacy rights is essential in the era of rapid technology and communication [2]. Even though in a legal context, privacy is not an absolute right and can be limited for certain reasons, such as protecting national security or public safety, the right to privacy must still be protected as a human right [3].

Protection of information system security is also a key factor in overcoming the risk of personal data leakage. According to Prof. Dr. Henri Subiakto, a Professor at FISIP Unair, "Protection of personal data requires complete, strong and firm regulations, as well as the readiness of intelligent, tough and adaptive human resources." With appropriate regulations and the readiness of human resources, the risk of personal data leakage can be minimized.

Not only does it threaten individuals, digital insecurity also harms business and government entities. In this case, digital privacy protection through steganography can help organizations keep their critical information confidential. Steganography, which comes from Greek which means disguise or concealment, reflects the essence of the art of hiding messages in other data without changing the data it contains. In this context, steganography is considered “closed writing” that allows hidden communication without being detected [4].

Thus, the origins of the word "steganography" and the meaning of the words in Greek, namely "steganos" and "graphein", clearly reflect the essence of steganography as the art of hiding messages in other data without changing the content or state of the data it contains.

Steganography in text messages provides a relevant solution to enhance digital privacy protection by effectively hiding messages in digital media without attracting the attention of unauthorized parties. Research conducted by the Sepuluh Nopember Institute of Technology (ITS) implemented steganography techniques using the Least Significant Bit (LSB) method to insert text messages into digital images. The research results show that steganography can be implemented effectively in digital media [5]. Apart from that, research conducted by the UNMUL Faculty of Mathematics and Natural Sciences also shows that steganography can be used to hide messages in digital images using the Least Significant Bit method [6]. In a digital era that is vulnerable to cybercrime and personal data leaks, steganography is becoming increasingly important as a way to protect digital privacy. With its ability to invisibly hide messages in digital media, steganography can provide an additional layer of protection against confidential messages, which is increasingly important in the face of increasingly complex digital data security challenges.

Steganography is the practice of hiding secret messages within normal messages or cover media with the aim of making the existence of the message difficult to detect by unauthorized parties [1]. One technique commonly used in steganography is the Least Significant Bit (LSB) method, where the least significant bit of the cover image is changed insignificantly by the bits of the secret message [7].

The LSB method has become popular in steganography because of its advantages in easy implementation and high level of transparency [7]. Steganography applications involve observing information, hiding private messages or codes, and sending secret messages [8]. For example, steganography can be used to hide sensitive information, such as email account data, by embedding it in digital images.

The benefits of this method are primarily felt by network administrators who need to transmit sensitive information to colleagues or network users. In addition, steganography can be used to hide messages or private code that requires high confidentiality (document). The existence of hidden messages is difficult to detect, making steganography effective for conveying secret messages [1].

Overall, steganography is an effective practice for hiding secret messages within normal messages or cover media. The LSB method, which changes the least significant bit, is the preferred choice due to its ease of implementation and high level of transparency. This strategy has a variety of applications, including protecting information, hiding private messages, and sending confidential messages effectively.

ISSN cetak 2745-925X
ISSN online 2722-273X

JESSI Volume 05 Nomor 1 March 2024

Least Significant Bit (LSB) is a technique used in steganography to hide secret information in cover media, such as digital images. This method works by changing the least significant bits of the cover image that are not significantly significant with the bits of the secret message [8]. LSB is a technique commonly used in encryption and decryption of confidential information [9]. This method is easy to implement and has high transparency [8].

However, this method also has disadvantages, such as being sensitive to filtering, scaling, rotation, adding noise to the image, and cropping which can damage the secret message [9]. LSB can be used for various applications, such as securing information, hiding private messages or codes, and conveying secret messages [10].

One example of the use of LSB is in archival filing, where confidential information is inserted on image media to provide security for archival filing data [8]. LSB can also be used to secure email account information at an agency. In addition, LSB can be used to hide secret messages in 24-bit color images by inserting messages in the most significant 2-bits of each image color (Red, Green, and Blue) [11].

Overall, LSB is a commonly used method in steganography to hide secret information within a cover medium. This method is easy to implement and has high transparency. LSB can be used for various applications, such as securing information, hiding private messages or codes, and conveying secret messages. Several studies have been carried out to develop the LSB method in steganography by combining it with other methods to increase data security.

2. Method

This research uses an experimental research method that designs an experimental framework that includes the use of the pelock.com website as the main platform for implementing steganography. By focusing on the Least Significant Bit (LSB) method, this research will systematically investigate the effectiveness of message hiding in digital images. This experiment will involve several stages, including preparation of experimental data, implementation of steganography using pelock.com features, and analysis of the results to evaluate the extent to which messages can be hidden without damaging the integrity of the image. With this experimental approach, the research aims to gain a deep understanding of steganography performance via the pelock.com platform.

3. Results and Discussion

Berikut ini adalah langkah-langkah untuk melakukan steganografi dengan metode LSB menggunakan website pelock.com.

3.1 Work Steps

This research aims to protect users' personal data using steganography techniques. The images used in this research are in .jpg format, and after carrying out steganography they are in .png format.

The steganography method used is the LSB method. This method provides small bits containing text in the image and will be inserted into the image that has gone through the steganography process. The image below shows a diagram of this research.

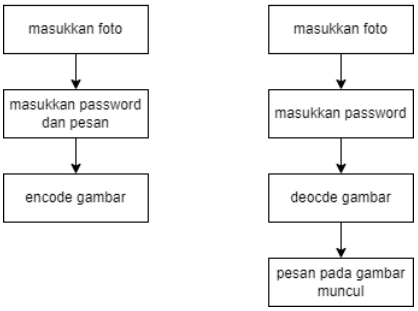

Figure 1. Steganography Step Diagram

3.2 Test Data

The image quality that we use has a size of 1280 X 720 pixels with a size of 187 KB. Meanwhile, the hidden message is in the form of email information and password with the encryption password "Halo123".

3.3 Test Results

Step 1: Open the pelock.com website page to perform steganography on the image. The image below shows the initial appearance of the pelock.com website.

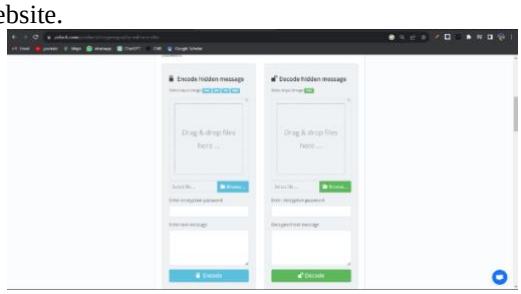

Figure 2. Pelock.com Home Screen

ISSN cetak 2745-925X
ISSN online 2722-273X

JESSI Volume 05 Nomor 1 March 2024

Step 2: Enter the image in which the message will be inserted into the image in the encode menu, then enter the encryption password and the message that will be encoded together with the image that has been entered.

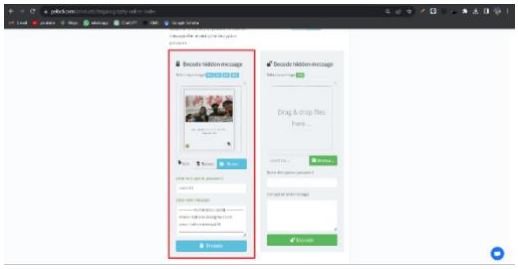

Figure 3. Image Encoding

Step 3: After the message has been entered, press encode to download the image that has gone through the steganography process, then to decode (open the information in the image), enter the image in the decode menu along with the encode password, then press decode to see the contents of the message in the image.

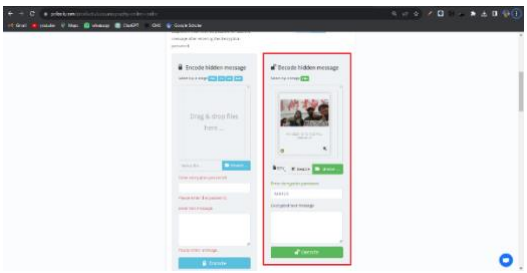

Figure 4. Image Decoding

Langkah 4: Apabila password yang dimasukkan tepat, maka akan tampil pesan seperti gambar di bawah.

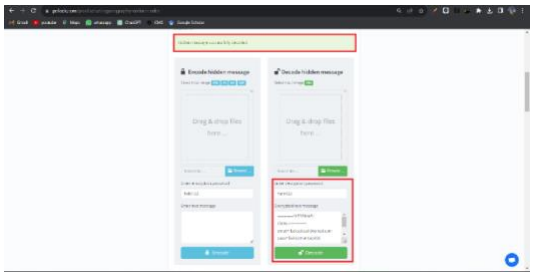

Figure 5. Image Decode Message Display

The image results before and after doing steganography are in the table below.

Tabel 1. Before and After Steganography

Before	After
	

As can be seen from the image above, we cannot distinguish which images have gone through the steganography process and which images have not gone through the steganography process. So basically steganography does not affect the quality and does not change any objects in the image, but in the image size there is a quite significant difference, the image before doing the steganography has a size of 187 KB while the image that has gone through steganography has a larger size, namely 1009 KB.

4. Conclusions and Recommendations

This research aims to protect users' personal data using steganography techniques, especially the LSB method. This method is effective in hiding information in an image without sacrificing transparency. The test results show that steganography does not affect the visual quality of the image, but can increase the file size significantly.

By using detailed steps, this research succeeded in implementing steganography on images by inserting text messages. The pelock.com website is an effective tool in carrying out the steganography process, making it easier for users to insert and retrieve secret messages. This success opens up the potential for developing LSB methods in steganography to improve data security better.

Based on the conclusions of this research, it is recommended to continue to explore and develop the Least Significant Bit (LSB) method in steganography as an effective strategy for protecting users' personal data. Although this method has been shown not to affect the visual quality of images, research can continue to explore ways to reduce the impact of significant increases in file size. In addition, further research should be carried out to measure and compare the level of security provided by the LSB method with other steganography methods. In future developments, it is necessary to consider the integration of artificial intelligence (AI) technology to increase resistance to steganography detection by image analysis algorithms. Further research can also explore the application of steganography to other file formats besides images,

such as videos or documents. The successful implementation of steganography via the pelock.com website shows the potential for further development in creating more user-friendly tools to protect digital privacy.

References

[1] O. N. Kadhim and Z. M. Hussain, "Information hiding using chaotic-address steganography," *J. Comput. Sci.*, vol. 14, no. 9, pp. 1247–1266, 2018, doi: 10.3844/jcssp.2018.1247.1266.

[2] H. P. Yuwinanto, "Privasi online dan keamanan data," *Palimpsest (Iowa. City).*, 2015, [Online]. Available: https://journal.unair.ac.id/download-fullpapers-palim0d249692cafull.pdf

[3] Marliana S, "Tinjauan Umum Tentang Perlindungan Hak Privasi Pengguna Simcard Terkait Registrasi Simcard Berdasarkan Permen Kominfo Nomor 14 Tahun 2017 Tentang Registrasi Pelanggan Jasa Telekomunikasi," pp. 26–54, 2019, [Online]. Available: http://repository.unpas.ac.id/41155/4/J. BAB II.pdf

[4] M. F. Syawal, D. C. Fikriansyah, and N. Agani, "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher Dan Metode LSB," *J. TICOM*, vol. 4, no. 3, pp. 91–99, 2016, [Online]. Available: https://media.neliti.com/media/publications/93707-ID-implementasi-teknik-steganografi-menggun.pdf

[5] M. Azlansyah and B. Setiyono, "Penyisipan Pesan pada Citra Digital Menggunakan Metode Least Significant Bit," *J. Sains dan Seni ITS*, vol. 8, no. 1, 2019, doi: 10.12962/j23373520.v8i1.37658.

[6] A. H. K. Darmayati, "Sistem Steganografi pada Citra Digital Menggunakan Least," *Semin. Sains dan Teknol. FMIPA Unmul*, vol. 1, no. 1, pp. 51–56, 2016.

[7] F. Yanti and K. Budayawan, "Implementasi Steganografi Menggunakan Metode Least Significant Bit (LSB) dalam Pengamanan Informasi pada Citra Digital," *Voteteknika (Vocational Tek. Elektron. dan Inform.*, vol. 11, no. 1, p. 63, 2023, doi: 10.24036/voteteknika.v11i1.121968.

[8] A. Lusia, "Implementasi Steganografi Citra Digital Pada Pemberkasan Arsip Menggunakan Metode Least Significantbit (Lsb) (Studi Kasus: Pt. Angkasa Pura I (Persero) Cabang Bandar Udara Internasioanal Juanda Surabaya)," Universitas Jember, 2020.

[9] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010, doi: 10.1016/j.sigpro.2009.08.010.

[10] E. S. Aisyah, R. Rosdiana, and M. R. Qodri, "Implementasi Steganografi Dengan Metode Lsb Untuk Mengamankan Informasi Akun Email Pada Suatu Instansi," *SENSI J.*, vol. 1, no. 1, pp. 24–30, 2015, doi: 10.33050/sensi.v1i1.722.

[11] E. R. Djuwitaningrum and M. Apriyani, "Teknik Steganografi Pesan Teks Menggunakan Metode Least Significant Bit Dan Algoritma Linear Congruential Generator," *Juita*, vol. IV, no. 2, pp. 79–85, 2016.