E-ISSN: 2962-6110
P-ISSN: 2964-7843
JSRET
Journal of Scientific Research, Education, and Technology
jsret.knpub.com

Implementation of Least Significant Bit Steganography for Securing Electronic Land Certificates

M. Fadhil Lutfi, Moh. Ali Romli
Universitas Teknologi Yogyakarta, Yogyakarta, Indonesia

ABSTRACT

The government's transition from physical to electronic land certificates raises significant concerns regarding document security and authenticity. This study implements the Least Significant Bit (LSB) steganography technique to secure electronic land certificates by embedding user identification and metadata into a digital image. The LSB method hides information within the least significant bits of image pixels, ensuring that the visual appearance of the image remains unchanged to the human eye. This approach enables the secure storage of sensitive data, allowing only authorized users to extract the hidden information for document verification. Experimental results demonstrate that the embedded image maintains high visual quality, as indicated by low Mean Squared Error (MSE) and high Peak Signal-to-Noise Ratio (PSNR) values. The LSB steganography technique thus provides an effective and imperceptible method for enhancing the confidentiality and integrity of electronic land certificates.

Keywords: *Steganography, Least Significant Bit (LSB) , Electronic Land Certificate, Access Security*

Corresponding author
Name: M. Fadhil Lutfi
Email: lutfi.mfl7@gmail.com

INTRODUCTION

The transition from physical to electronic documents has become an inevitable aspect of modern digital transformation, particularly within government institutions. One of the most significant implementations of this transformation is the digitization of land ownership certificates into electronic land certificates (e-certificates). This initiative aims to improve efficiency, accessibility, and data management in the land administration process. However, as digital documents replace physical ones, the issue of data security, authenticity, and protection against unauthorized access has become increasingly crucial (Aminullah, Bakti, Hayat, & Lukman, 2022; Paramita, Muchbarak, Sulistyohati, & Primawati, 2023).

Digital data, while efficient for storage and transmission, remains vulnerable to duplication, interception, and modification. Conventional cryptographic techniques such as AES and RSA provide data encryption but can also expose the presence of sensitive information, making the system a potential target for attackers (Sidiq, Rahayu, & Supriatna,

2023; Sellyana & Nugraha, 2023). In contrast, steganography offers a different layer of security by concealing information within a non-suspicious medium such as an image, sound, or video file (Abdulla, 2024; Bahtiar & Chandra, 2024). Through steganography, the existence of confidential data remains hidden, which enhances security by reducing the likelihood of detection.

Among the various steganographic techniques, the Least Significant Bit (LSB) method has become the most widely used approach for image-based data hiding. This technique modifies the least significant bits of image pixels to store secret data without causing significant visual distortion, making the stego image nearly identical to the original (Filzasavitra, Purboyo, & Saputra, 2019; Herviana & Djuniadi, 2024). Previous studies have shown that LSB is capable of embedding various forms of data text, images, and encrypted content while maintaining high image quality as measured by Peak Signal-to-Noise Ratio (PSNR) and Mean Square Error (MSE) metrics (Sabilla, Meirisdiana, Sunaryono, & Husni, 2021; Punia, Malik, & Singh, 2023).

Research by Abiyu, Imelda, Hardjianto, and Waluyo (2023) demonstrated the practical implementation of LSB steganography in a corporate context, while Maulidina, Idris, and Djumhadi (2024) focused on applying LSB for forensic data concealment. However, the majority of existing research has centered around concealing text or small binary messages rather than large, sensitive documents such as land ownership certificates. This limitation opens an opportunity for further exploration into how LSB steganography can be used for document-level security, particularly in safeguarding electronic land certificates from duplication, forgery, and unauthorized access.

This research focuses on the implementation of Least Significant Bit (LSB) steganography as a method for embedding an entire electronic land certificate file into a digital image. Unlike traditional encryption, this approach conceals the existence of the file itself, making the stored data indistinguishable from regular image content. The study experimentally evaluates the embedding and extraction processes to ensure that the hidden certificate can be perfectly retrieved without data loss while preserving image quality. The results are assessed using quantitative image quality metrics such as PSNR and MSE, as these parameters determine how well the stego image retains its original appearance after data insertion (Ashwini, Ramesh, & Tejaswini, 2022; Tinambunan & Mulyati, 2024).

By implementing the LSB method for digital land certificate protection, this research contributes to the development of a secure, covert, and reliable approach to digital document preservation. The findings are expected to strengthen the foundation for secure electronic document management systems in the context of Indonesia's ongoing digital land certificate transformation.

METHOD

This study employs a quantitative experimental approach to evaluate the effectiveness of the Least Significant Bit (LSB) steganography technique in embedding and extracting complete electronic land certificate files within digital images. The main objective

is to analyze how the LSB method maintains image quality and data integrity after the embedding process. The experiment was conducted in a controlled environment, where a set of cover images served as the embedding medium, and several certificate files in PDF format were used as the secret data to be hidden.

The research procedure consists of several sequential stages: data preparation, embedding, extraction, and evaluation. During the data preparation stage, digital images in PNG format were selected as cover images because of their lossless compression, which preserves pixel accuracy during manipulation. Each cover image was standardized to a resolution of 512×512 pixels, resulting in a total of 262,144 pixels. Each pixel has three color channels (Red, Green, and Blue), allowing it to store information in its least significant bits. Electronic land certificates in PDF format were used as the payload to simulate real-world storage of confidential government documents.

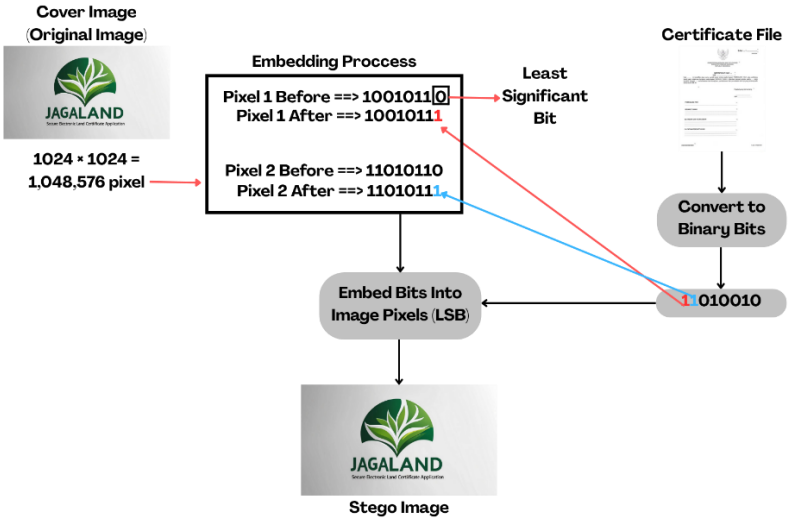

Figure 1: LSB Method

The embedding process involves modifying the least significant bit of each pixel in the cover image to insert binary data representing the certificate file. In a 24-bit RGB image, each pixel contains three color components, and one bit from each component can be used to hide data. This allows three bits of secret information to be stored in each pixel without noticeable visual changes. The embedding algorithm converts the PDF file into a binary stream and sequentially inserts it into the pixels of the image starting from the top-left corner until all the data are embedded. Figure 2 illustrates the general process of data insertion using the LSB technique, where the least significant bits of the pixel values are replaced with bits from the certificate file.

The evaluation stage measures the quality and accuracy of the steganographic process using two main parameters: Mean Square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). MSE calculates the average squared difference between pixel intensities of the cover and stego images, while PSNR measures the ratio between the maximum possible

signal power and the noise power introduced by the embedding process (Filzasavitra, Purboyo, & Saputra, 2019). A smaller MSE value and a higher PSNR value indicate better image quality preservation. Table 1 presents the general classification of PSNR values in relation to perceived image quality (Sabilla, Meirisdiana, Sunaryono, & Husni, 2021).

Table 1: PSNR and MSE Quality Classification

NO	PSNR (dB)	MSE Value	Image Quality	Description
1	> 40	< 1.0	Excellent	Differences are imperceptible to the human eye
2	30–40	1.0 – 10.0	Good	Slight differences, generally acceptable
3	20–30	10 – 50	Fair	Noticeable distortion in detailed areas
4	< 20	> 50	Poor	Visible degradation and loss of quality

Source: Sabilla, I. A., Meirisdiana, M., Sunaryono, D., & Husni, M. (2021).

FINDING AND DISCUSSION

RESEARCH RESULT

This research evaluates the application of the Least Significant Bit (LSB) steganography method for securing electronic land certificates by embedding entire certificate files into digital cover images. The experiment aimed to analyze how the size of the embedded certificate affects image quality and file size after embedding, while ensuring that the stego image remains visually identical to the original.

Figure 2: Cover Image (Original Image)

Five electronic land certificate files in PDF format, with sizes ranging from 100 KB to 1 MB, were embedded into a 2834 KB PNG cover image using the LSB algorithm. After embedding, visual inspection confirmed that all stego images appeared identical to their respective cover images, showing no perceptible color or structure differences. This confirms that the LSB technique can effectively hide data in the least significant bits of an image without altering its visible characteristics.

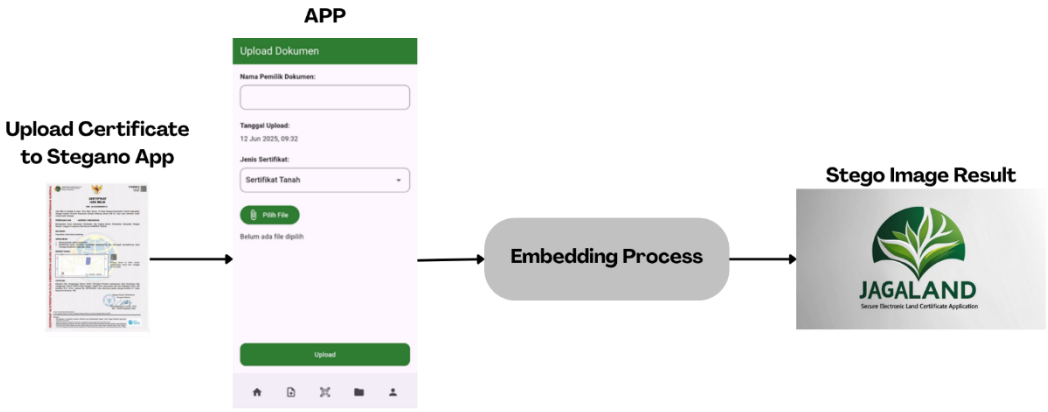

Figure 3: Embedding Proccess

After the embedding process, each stego image was compared with its corresponding original image in terms of visual appearance and file size. The results show that all stego images retained the same visual quality as the original cover images, with no visible distortion, color shifting, or noise. This indicates that the LSB embedding process effectively modifies the least significant bits of the image pixels without causing noticeable changes to the human eye.

Table 2: Comparison of Image File Sizes Before and After Embedding

NO	File Name	Certificate Size (KB)	Image Size Before (KB)	Image Size After (KB)	Size Increase (%)
1	Certificate 1	100	2834	3128	10.4%
2	Certificate 2	300	2834	3614	27.5%
3	Certificate 3	600	2834	4351	53.5%
4	Certificate 4	800	2834	4840	70.8%
5	Certificate 5	1000	2834	5322	87.8%

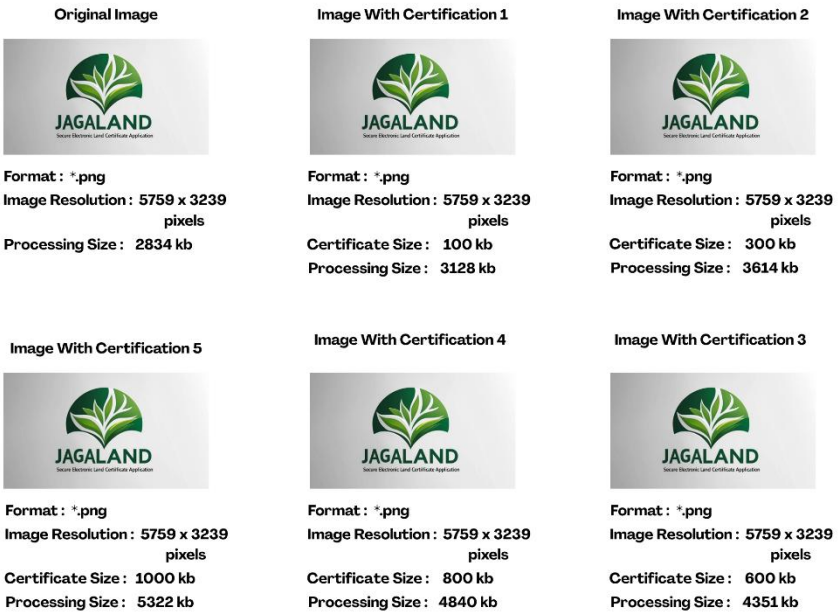

Figure 4: Results of Steganography

Based on Table 2 and Figure 4, it can be observed that the stego image size increases gradually as the embedded certificate file becomes larger. The smallest embedded file (100 KB) caused only a 10.4% increase in image size, while the largest file (1,000 KB) resulted in an 87.8% increase. Despite the file growth, the visual inspection confirmed that the stego images remained visually identical to their respective originals.

These results demonstrate that the LSB method can effectively embed entire electronic land certificate files within image media while maintaining high imperceptibility. The increase in file size is acceptable for digital archiving purposes and is a natural result of embedding large binary data into pixel structures.

DISCUSSION

The quantitative evaluation of the Least Significant Bit (LSB) steganography process was conducted using Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) metrics to measure the degree of image distortion after embedding electronic land certificate files. These parameters are commonly used in digital image analysis to assess visual fidelity and embedding imperceptibility.

MSE calculates the average squared difference between corresponding pixels of the original and stego images. A smaller MSE value indicates that fewer pixel values have changed during the embedding process. In contrast, PSNR represents the logarithmic ratio between the maximum possible pixel value and the noise introduced. A higher PSNR value signifies better image quality (Filzasavitra, Purboyo, & Saputra, 2019).

According to Sabilla et al. (2021), PSNR values greater than 40 dB are classified as *excellent*, indicating imperceptible distortion, while values above 50 dB are considered *very*

high quality. The results of this study, shown in Table 3, confirm that the embedding process successfully preserved the visual integrity of the images, as all PSNR values remained significantly above this threshold.

Table 3: Quantitative Results of Image Quality Measurement

NO	File Name	Certificate Size (KB)	MSE	PSNR (dB)	Quality Description
1	Certificate 1	100	0.009739	68.245862	Excellent (no visible change)
2	Certificate 2	300	0.028472	63.586575	Excellent (imperceptible difference)
3	Certificate 3	600	0.057406	60.541227	Excellent (minor pixel alteration)
4	Certificate 4	800	0.076478	59.295450	Excellent (slight difference)
5	Certificate 5	1000	0.096030	58.306746	Very Good (barely perceptible change)

As illustrated in Table 3, the MSE values remained very low, below 0.1 in all cases, indicating minimal pixel modification caused by the embedding process. Meanwhile, PSNR values ranged between 58.3 dB and 68.2 dB, which corresponds to excellent visual quality according to standard evaluation benchmarks. The results reveal a clear trend: as the size of the embedded certificate file increases, MSE slightly rises and PSNR gradually decreases. This is expected because larger payloads modify more pixels in the image. However, even at the highest embedding capacity (1 MB), the PSNR value remains well above 50 dB, confirming that the resulting stego images retain near-perfect visual fidelity.

These findings align with previous studies by Abdulla (2024) and Aminullah et al. (2022), which emphasized that the LSB steganography technique provides an optimal balance between imperceptibility, embedding capacity, and data recoverability. The consistently high PSNR and low MSE values demonstrate that the LSB method is reliable for securing sensitive digital documents such as electronic land certificates. Similar to the application of cryptographic techniques for securing employee document systems (Adam & Romli, 2024), this study highlights how LSB steganography can serve as a practical and lightweight security mechanism by concealing sensitive certificate data within image media rather than relying on encryption alone.

Overall, the results confirm that embedding complete certificate files into images using the LSB method does not significantly affect image quality while providing an effective means of protecting confidential data. The success of the extraction process also indicates that the steganographic encoding is reversible and accurate, ensuring that the hidden certificate can be retrieved without loss or corruption.

CONCLUSION

This research demonstrates that the application of the Least Significant Bit (LSB) steganography method is effective for securing electronic land certificate files by embedding them within digital image media. The experimental results showed that the embedding process caused only a slight increase in image file size, ranging from 10.4% to 87.8%, depending on the embedded file's size. Despite this increase, the visual appearance of the stego images remained indistinguishable from the original cover images.

Quantitative testing using Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) confirmed the high visual quality of the stego images. MSE values were consistently low (below 0.1), while PSNR values ranged between 58.3 dB and 68.2 dB, indicating *excellent image fidelity* and imperceptibility of the embedded data. These findings verify that the LSB method successfully conceals entire electronic certificate files without visible distortion or data loss.

The ability to extract the embedded certificates accurately also confirms the reversibility and reliability of this method. Therefore, the LSB steganography technique provides a secure, efficient, and visually lossless approach for protecting confidential digital land certificates against unauthorized access or manipulation.

For future research, this work may be further enhanced by integrating cryptographic algorithms such as AES before the embedding process, to add an extra layer of data encryption and strengthen security against steganalysis attacks. Additionally, testing with higher-resolution images or alternative color models may be conducted to analyze capacity and quality trade-offs in more complex embedding scenarios.

REFERENCES

Abdulla, A.A. (2024). Digital image steganography: challenges, investigation, and recommendation for the future direction. *Soft Computing*. 28. 8963–8976. https://doi.org/10.1007/s00500-023-09130-8

Abiyu, A.A., Imelda, M., Hardjianto, M., & Waluyo, S. (2023). Implementasi steganography dengan metode LSB pada PT Samasedia Jasa Teknologi. *2nd Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*. 2(1). 82–83.

Adam, P., & Romli, M. A. (2024). Implementasi sistem keamanan dokumen kepegawaian menggunakan metode AES-256 dan Vigenere Cipher. *Jurnal Komputer dan Teknologi (JUKOMTEK)*, *3*(1), 20–26. https://doi.org/10.58290/jukomtek.v2i2.166

Aminullah, M. N. A., Bakti, R. Y., Hayat, M. A., & Lukman. (2022). Pembuatan verifikasi sertifikat digital sebagai bukti keabsahan menggunakan algoritma steganografi dengan metode Least Significant Bit insertion (LSB). *AINET: Jurnal Informatika Universitas Muhammadiyah Makassar. 4*(1). 24–32. https://doi.org/10.26618/ainet.v4i1.11904

Ashwini, K., Ramesh, B., & Tejaswini, H. (2022). Detection of cyber phishing attack on online voting system using visual cryptography. *International Journal of Advances in Engineering and Management (IJAEM)*. 4(7). 1596–1600. doi: 10.35629/5252-040715961600

Bahtiar, M.F., & Chandra, J.C. (2024). Pengamanan file berbasis desktop dengan algoritma AES-256 dan steganografi LSB di PT Sinarmas Sekuritas. *5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*. 3(2). 99–101.

Filzasavitra, P., Purboyo, T. W., & Saputra, R. E. (2019). Analysis of steganography on PNG image using least significant bit (LSB), peak signal to noise ratio (PSNR), and mean square error (MSE). *Journal of Engineering and Applied Sciences*. 14(21). 7821-7827.

Herviana, W.H., & Djuniadi. (2024). Implementation of Least Significant Bit Steganography to secure text messages in images. *Journal of Information System Exploration and Research*. 2(2). 85–92. https://doi.org/10.52465/joiser.v2i2.438

Maulidina, J.R., Idris, N.B., & Djumhadi. (2024). Implementasi steganografi dan steganalisis menggunakan metode LSB (Least Significant Bit) pada file gambar. *Forbis: Journal Forensic Business Information Systems*. 1(1). 14–15.

Paramita, A., Muchbarak, A., Sulistyohati, A., & Primawati, A. (2023). Terapan metode Least Significant Bit untuk deteksi keaslian e-certificate. *Faktor Exacta*. 16(3). 182–189.

Punia, R., Malik, A., & Singh, S. (2023), *Innovative image interpolation based reversible data hiding for secure communication*, Discover Internet of Things, Vol. 3, Article 22.

Putra, M.R.D., & Pamudji, R.A.N. (2024). Analisis dan perancangan aplikasi steganografi pada media image dengan metode LSB (Least Significant Bit). *IKRAM: Jurnal Ilmu Komputer Al Muslim*. 3(1). 1–2.

Sabilla, I. A., Meirisdiana, M., Sunaryono, D., & Husni, M. (2021). Best ratio size of image in steganography using Portable Document Format with evaluation RMSE, PSNR, and SSIM. *Proceedings of the 2021 4th International Conference of Computer and Informatics Engineering (IC2IE)*. 289–294. https://doi.org/10.1109/IC2IE53219.2021.9649198

Sellyana, A., & Nugraha, N.B. (2023). Penerapan Caesar Cipher dan Least Significant Bit untuk mengamankan data rekam medis. *Jurnal Publikasi Ilmu Komputer dan Multimedia*. 2(1). 51–60.

Sidiq, R.F., Rahayu, R.E.G., & Supriatna, A.D. (2023). Implementasi kriptografi Advanced Encryption Standard dan Least Significant Bit untuk keamanan pesan email dalam gambar. *Jurnal Algoritma*. 20(2). 305–315.

Tinambunan, J., & Mulyati, S. (2024). Pengamanan pengiriman file menggunakan steganografi dengan metode LSB di PT Capture IT. *5th Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI)*. 3(2). 128–129.