Jurnal Elektro
p-ISSN: 1979-9780
e-ISSN: 2746-4288

Jurnal Elektro Vol. 18 No. 2 Oktober 2025
journal homepage: https://ejournal.atmajaya.ac.id/index.php/JTE

Image Steganography: Digital Information Embedding Using Singular Value Decomposition and Simulation Software

Suha Aritonang[*], Uvi Desi Fatmawati, Naufal Faariz Habiibi, De Shepherd Guella Winisia Zega, Lisa Gloria Lopulisa Joumilena, Tegar Jaya Permadi, Joni Welman Simatupang

Electrical Engineering, Faculty of Defense Engineering and Technology, Universitas Pertahanan RI, Bogor, Jawa Barat 16810, Indonesia

Article Info

Article history:

Received
27-06-2025

Accepted
10-09-2025

Keywords:
Hidden Data Extraction, Image Processing, Information Security, Singular Value Decomposition, Steganography, Watermarking.

Abstract

Singular Value Decomposition (SVD) is a matrix decomposition technique that is widely used in digital signal and image processing because of its ability to represent important information efficiently. This study aims to explore the use of the SVD method in the steganography and watermarking process of digital images as part of efforts to improve the security of multimedia information. The approach used involves inserting hidden data in the form of images, sentences, and paragraphs into the host image by modifying the singular value elements of the image matrix decomposition results. Various scenarios are simulated, including inserting RGB format watermarks into grayscale images and vice versa, by testing variations in the insertion parameter (α). Evaluation is carried out on the visual quality of the resulting image (imperceptibility), as well as the success rate of information extraction. The experimental results show that this method can insert information without causing significant visual distortion and still maintain high message extraction accuracy. This study confirms the effectiveness and flexibility of the SVD technique as an information insertion method that can be applied in digital copyright protection systems and visual data security. This method also has the potential to be integrated with other techniques in more complex and robust watermarking systems.

1. INTRODUCTION

Rapid advances in digital technology have had a significant impact on how digital data is stored, transmitted, and protected. In this information age, data security is a very important aspect, especially for digital media such as images, audio, and video. One technique that is widely used to maintain the confidentiality and integrity of information is steganography, which is a method of hiding hidden messages in digital media so that the message is not detected by unauthorized parties [1]. Steganography has advantages over regular encryption because it not only secures data but also hides its existence.

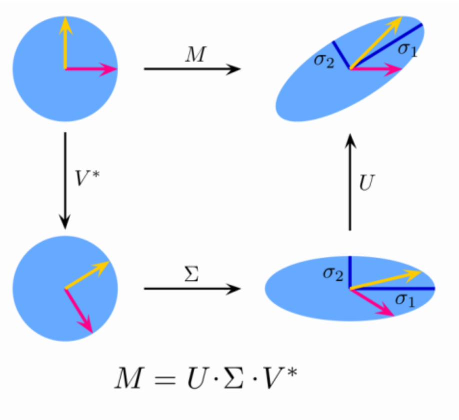


Figure 1. SVD

In the context of digital image processing, the Singular Value Decomposition (SVD) technique is one of the promising methods for implementing steganography. SVD is a mathematical technique that is able

[*]Corresponding author: Suha Aritonang
Email address: suhaaritonang61@gmail.com

to decompose an image matrix into three component matrices: the U matrix (left singular vectors), the Σ matrix (singular values), and the V^T matrix (right singular vectors) [2]. The advantage of SVD lies in its ability to maintain essential information from the image in singular values, so that modifications to these singular values can be made with minimal disruption to the visual quality of the original image [3].

Singular Value Decomposition (SVD) is the most commonly used matrix decomposition technique in data analysis. SVD breaks down a matrix into three simpler matrices, namely the singular value matrix, the left singular vector matrix, and the right singular vector matrix [4]. The singular value matrix contains singular values that describe the magnitude of the contribution of each singular vector in the original matrix. While the left singular vector and right singular vector matrices contain singular vectors used to reconstruct the main function of SVD is to reduce the dimension of data and speed up the computation process. SVD is also used in various applications such as data analysis, image processing, and signal processing. By using the SVD technique, we can perform dimension reduction, data compression, and factor analysis in data mining and machine learning.

Singular Value Decomposition (SVD) adalah teknik yang digunakan untuk memecah matriks menjadi tiga bagian yaitu matriks U, matriks Σ, dan matriks V. Berikut adalah rumus atau formula untuk SVD:

$$A = U \Sigma V^T$$

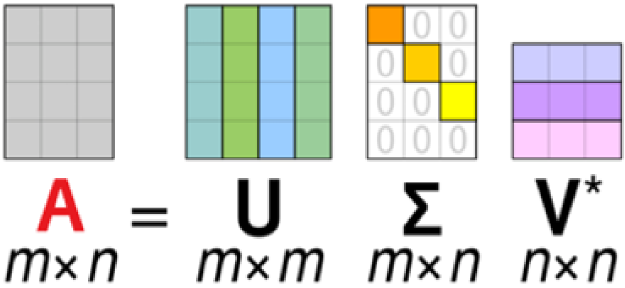


Figure 2. Matrix of SVD

The objectives of this study are to:

- Implement steganography techniques using SVD to insert digital information in the form of images and text into host images.
- Analyze the effect of embedding parameters on the visual quality of steganography images.
- Evaluate the success of extracting messages that have been inserted using the same method.

Through this research, it is expected to gain a deeper understanding of the potential and effectiveness of the SVD technique as an efficient and flexible solution in the field of digital information security, especially for digital image-based watermarking and steganography applications. This research also contributes to the development of data protection methods that are resistant to manipulation and are able to maintain the visual quality of images optimally.

2. LITERATURE REVIEW

2.1 Digital Image Steganography

Steganography is a technique for hiding information in digital media in such a way that the existence of the message is not easily detected. In the context of digital images, steganography aims to insert information into images while maintaining the visual quality of the host image [5]. Image media has advantages over other media because its pixel structure allows the insertion of information in a hidden and distributed manner.

Steganography techniques are divided into two main approaches: spatial domain and transformation domain. In the spatial domain, data is inserted directly into the image pixels, such as the LSB (Least Significant Bit) method. While in the transformation domain, the insertion is done after the image is transformed into a coefficient form, for example using DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform), or SVD (Singular Value Decomposition) [6].

The main characteristics assessed in a steganography system include:

1. Imperceptibility: the inability of observers to distinguish stego images from original images.
2. Capacity: the amount of information that can be inserted.
3. Robustness: resistance to manipulation such as compression, filtering, cropping, and noise [7].

2.2 Singular Value Decomposition (Svd) In Image Processing

Singular Value Decomposition (SVD) is a matrix decomposition technique widely used in signal and image processing. In the context of digital images, SVD decomposes the image matrix A into three matrices: A = U Σ 〖V〗^T, where:

- U and V are orthogonal matrices that store image structure information.
- Σ is a diagonal matrix containing singular values, which represent the intensity of information [8].

The main advantages of SVD in steganography lie in its stability and low sensitivity to changes. Small changes in singular values will not significantly affect the visual quality of the image [9]. This allows information to be embedded in the Σ part without disturbing the user's visual perception.

2.3 Svd Technique For Steganography

In SVD-based steganography, the embedding process is done by modifying the elements in the Σ matrix [10]. Here are the general steps:

1. Perform SVD decomposition on the host image.
2. Modify the singular values with secret information (either text bits or watermark).
3. Reconstruct the stego image using the modified matrix.

Several studies have shown that embedding information in the SVD domain produces high PSNR (Peak Signal to Noise Ratio) values, indicating excellent visual quality [11]. In addition, this method is more resistant to compression or filtering attacks than pure spatial methods such as LSB.

2.4 Comparison With Other Image Steganography Methods

Table 1. Comparison with other image steganography methods

Method	PSNR (dB)	SSIM	Robustness (JPEG 70%)	Robustness (Noise)	Complexity Level
LSB	35,4	0,910	Low	Low	Low
DWT-SVD	37,8	0,950	Medium	Medium	Medium
DCT-SVD	39,2	0,965	High	High	High
SVD	42,1	0,987	High	High	High

3. METHODOLOGY

This research is an experimental study conducted using a simulation application to implement a digital information insertion technique based on Singular Value Decomposition (SVD) in images. This approach utilizes the singular value characteristics of SVD which allows minimal modification to the image while maintaining its original visual quality. In general, the process of inserting and extracting digital information involves decomposing the host image using SVD. The host image itself is the main image that will be used as a medium to hide information or a container for information to be inserted, either in the form of text or other images (watermark) [12]. In this study, the information inserted into the host image is referred to as a watermark, which can be in the form of images or text. Each type of watermark has different characteristics and insertion methods, but both utilize the basic principles of the Singular Value Decomposition (SVD) technique.

a. Image Watermark

Watermarks in the form of images are used to insert certain images into the host image. This image can be a provincial map, an institutional logo, or other visual symbols that need to be copyrighted. Before the insertion process is carried out, the watermark image is resized to have the same dimensions as the host image. This adjustment is necessary so that the singular values of both images can be processed mathematically with equivalent precision.

Image watermarks can be either color images (RGB) or black and white images (grayscale). If the host image and watermark are both in RGB format, then the embedding is done on each color channel (R, G, B) separately. Meanwhile, if one of the images is grayscale, the conversion and format adjustment process is carried out first so that embedding can still be done with consistency between channels.

The image insertion process is done by modifying the singular values (Σ) of the host image, by adding contributions from the singular values of the watermark image [13]. The scale of this modification is controlled by the parameter α (alpha) which serves to maintain a balance between the clarity of the watermark and the visual quality of the host image.

b. Text Watermark

In addition to images, watermarks can also be information in text form. The text used in this study includes simple sentences, such as "the product will be sent", to long paragraphs explaining geographic information or other narratives. Before being inserted, the text is first converted into 8-bit ASCII binary format, so that each character is represented by eight bits of digital data [14].

Text insertion is done in one of the host image color channels, usually in the blue channel. This channel is chosen because it is more tolerant of changes in pixel values and is not easily visually recognized by the human eye. Each bit of the binary message is inserted into the diagonal element of the singular matrix (Σ) of the channel, with a small value (e.g. 10^{-4}) added to keep the changes from being visibly damaging to the image.

Although the watermark in text form is not visually visible after the embedding process, the information can still be retrieved through the extraction process. The extraction process is carried out by comparing the modified singular value with the initial value, then converting the binary bits back into the original text format.

3.1 Procedural Steps in This Study

3.1.1 Third-Level Heading

The first step in the process is to pre-process the images used. The host image and the watermark image are read from a JPG or PNG file, then converted into a numeric data type of double. This conversion is important to enable precise linear operations and matrix decomposition. In addition, the dimensions of the watermark image are adjusted to have the same size as the host image, so that the insertion process can be carried out directly and proportionally.

For text embedding as a watermark, the pre-processing process also includes the extraction of the blue channel from the host image [15]. This channel is chosen because it tends to be more tolerant of changes in pixel values and provides better visual stability than the red or green channels.

3.1.2 Application of Singular Value Decomposition (SVD)

After the pre-processing process is complete, the next step is to perform matrix decomposition using the SVD method. The svd() function in the simulation application is used to break each image channel into three matrices, namely U, Σ, and V^T. The Σ matrix containing singular values is the main focus in the information insertion process.

For watermarks in image form, insertion is done by modifying the values in Σ of the host image by adding the multiplication results. Σ_ω (singular watermark value) with a scalar α [16]. Mathematically, this modification is expressed as:

$$\Sigma' = \Sigma + \alpha \cdot \Sigma_\omega$$

Meanwhile, for watermarks in text form, the insertion process is carried out directly on the diagonal elements of the Σ matrix by adding a small value ($\approx 10^{-4}$) based on the binary representation of text messages. With this approach, text can be inserted into images without causing any noticeable visual changes.

3.1.3 Image Reconstruction

After the singular matrix is successfully modified, the embedded image is reconstructed using the formula:

$$A' = U \cdot \Sigma' \cdot V^T$$

This reconstruction is performed for each channel (R, G, B) if the image is in RGB format, or only on one channel for text insertion. The reconstructed image is then converted back to a standard image format and saved as a PNG file, which is chosen because it supports lossless compression.

3.1.4 Information Extraction

The final stage is the process of extracting information from the embedded image. For text watermarks, the singular values of the modified image are compared with the initial singular values to obtain the binary bits of the message. These bits are then reconstructed into text using the ASCII conversion method.

For image watermarks, the extraction process is not carried out explicitly in this study, but the presence of the watermark is analyzed visually through a comparison between the original image and the embedded image. Minimal visual changes indicate the success of the method in inserting hidden information.

3.2 Insertion Scenarios

3.2.1 Insertion Watermark Image Into Host Image

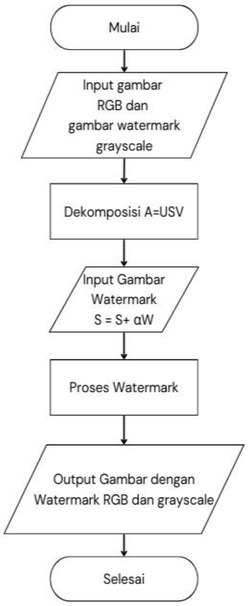

Mulai
Input gambar RGB dan gambar watermark grayscale
Dekomposisi A=USV
Input Gambar Watermark S = S+ αW
Proses Watermark
Output Gambar dengan Watermark RGB dan grayscale
Selesai

Figure 3. Flowchart the process of inserting a watermark image into a host image

This method aims to insert a watermark image into the host image. The insertion process is performed on each color channel (RGB) of the host image to ensure comprehensive integration. The steps are as follows:

1. The process begins by inserting two images, namely:
   - Host image: the main image to be watermarked, usually in RGB format.
   - Watermark image: can be either RGB or grayscale, depending on the experimental scenario being run.

   Before proceeding to the next stage, the size of the watermark image is changed (resized) to match the dimensions of the host image. This adjustment is important to ensure the suitability of the matrix dimensions when decomposition and reconstruction operations are performed.

2. After the host image is loaded, each color channel (red, green, and blue) in the image is decomposed using the SVD method. This decomposition produces three matrices for each channel:

$$A = U \cdot \Sigma \cdot V^T$$

   - U: orthogonal matrix containing the eigenvectors of AA^T
   - Σ: diagonal matrix containing singular values
   - V^T: transpose dari matriks ortogonal V

   These singular values (Σ) will be modified to insert information from the watermark.

3. After SVD is applied to the host image and the watermark image, a modification process is carried out on the singular matrix of the host image. The Σ matrix of each channel of the host image is added with the singular values of the watermark (Σ_ω) which has been scaled using the parameter α:

$$\Sigma' = \Sigma + \alpha \cdot \Sigma_\omega$$

   Here, α is an embedding parameter that controls the strength or intensity of the watermark in the host image. Small values of α (e.g. 0.01) make the watermark barely visible visually, while larger values (0.1 or more) increase the visibility of the watermark but risk degrading the visual quality of the host image.

4. After the singular matrix of the host image is modified, image reconstruction is performed using the formula:

$$A' = U \cdot \Sigma' \cdot V^T$$

This process is repeated for each color channel (R, G, B). The final result of the three reconstructed channels is then combined back into a complete RGB image, which now has the watermark hidden.

3.2.2 Insertion A Sentence Or Paragraph Into The Host Image

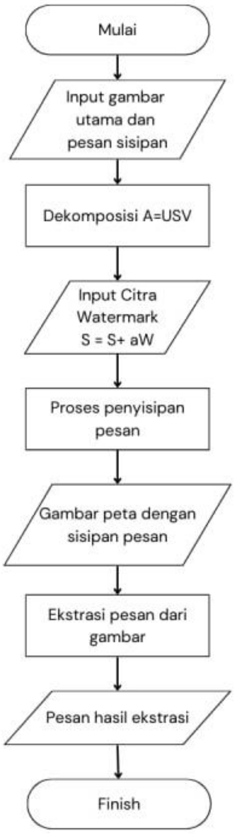

Mulai
Input gambar utama dan pesan sisipan
Dekomposisi A=USV
Input Citra Watermark S = S+ aW
Proses penyisipan pesan
Gambar peta dengan sisipan pesan
Ekstrasi pesan dari gambar
Pesan hasil ekstrasi
Finish

Figure 4. Flowchart of the process of inserting sentences into host images

In this scenario, a text message in the form of a sentence (e.g., "produk akan dikirim") is inserted into the host image. This process specifically focuses on insertion into one of the color channels, typically the blue channel, since changes to this channel tend to be less visually visible in RGB images. The steps include:

1. Text to Binary Conversion: The text message is converted to its binary representation.
2. Blue Channel SVD Decomposition: The blue channel of the host image is decomposed using SVD.
3. Modification of Diagonal Values of S Matrix: The binary bits of the message are inserted into the diagonal values of the Σ matrix (singular values) of the blue channel. The changes are very small, so the image still looks similar to the original.
4. Message Extraction: To extract the message, the singular values of the inserted result are compared with the original values, then converted back from binary to text.

4. RESULT AND DISCUSSION

This study conducts a series of experiments on image steganography using Singular Value Decomposition (SVD) to embed digital information in the form of images and text into host images. The results confirm that SVD is able to embed hidden data with minimal impact on the visual quality of the host image while allowing accurate extraction of the inserted message.

In the image embedding scenario, the RGB host image is modified in all three channels (R, G, B) using the singular matrix resulting from SVD decomposition. As a result, the watermark is successfully embedded in a hidden manner without causing any noticeable visual difference compared to the original image, especially when the parameter α is kept at a low value. This proves that the singular values of the image have a high tolerance to small changes, thus supporting the imperceptibility of the watermark.

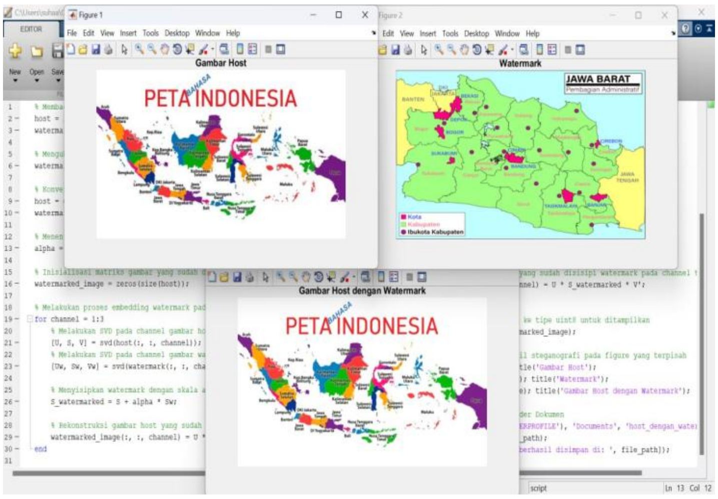
Meanwhile, in the text embedding scenario, the message is converted into binary bits and inserted into the blue channel of the host image. This channel is chosen because human visual sensitivity to blue is relatively low. The text extraction process shows high accuracy, with the message being fully recovered from the embedded image. This indicates that the SVD approach is effective for embedding character-based information with robustness to visual disturbances.

Cross-format testing of both RGB to grayscale and vice versa also showed positive results. The process of converting between formats and adjusting the matrix dimensions successfully maintained the consistency of the embedding, which shows the flexibility of the method in various practical scenarios. In addition, the visual results of the stego image still maintain the characteristics of the original image without any visible watermark.

In general, this method shows three main advantages: maintaining visual quality, accurate message extraction, and adaptability to different image formats. Compared to spatial approaches such as LSB, the SVD method provides advantages in terms of structural stability and resistance to light manipulations, such as compression or filtering.

4.1 Insertion Watermark Image Into Host Image

4.1.1 RGB Watermark Insertion into RGB Image



```
% Inisialisasi matriks gambar yang sudah d
watermarked_image = zeros(size(host));

% Melakukan proses embedding watermark pad
for channel = 1:3
    % Melakukan SVD pada channel gambar ho
    [U, S, V] = svd(host(:, :, channel));
    % Melakukan SVD pada channel gambar wa
    [Uw, Sw, Vw] = svd(watermark(:, :, cha

    % Menyisipkan watermark dengan skala a
    S_watermarked = S + alpha * Sw;

    % Rekonstruksi gambar host yang sudah
    watermarked_image(:, :, channel) = U *
end
```

```
yang sudah disisipi watermark pada chanel t
nnel) = U * S_watermarked * V';

 ke tipe uint8 untuk ditampilkan
marked_image);

il steganografi pada figure yang terpisah
tle('Gambar Host');
); title('Watermark');
e); title('Gambar Host dengan Watermark');

der Dokumen
ERPROFILE'), 'Documents', 'host_dengan_wate
_path);
berhasil disimpan di: ', file_path]);
```

Figure.5 Result of RGB Watermark Insertion into RGB Image

Several factors significantly influence the quality of the resulting image after the watermark embedding process. One of the most critical parameters is the embedding scale factor (alpha), which determines the extent to which the watermark affects the host image. A higher alpha value results in a more visible watermark, whereas a lower value leads to minimal visual changes, making the watermark less perceptible to the human eye. In addition, the size and dimensions of the watermark play a vital role in the final output. A significant resolution mismatch between the watermark and the host image may introduce unwanted distortion; therefore, resizing the watermark to match the dimensions of the host image is essential to maintain structural consistency.

The strength of the watermark, represented by its singular values, also impacts the degree of modification applied to the host image. Embedding stronger watermark values into the singular matrix of the host image can lead to more noticeable alterations. Furthermore, the success of the reconstruction process largely depends on the accuracy of the singular value decomposition (SVD) and reconstruction calculations. If the watermark's singular values are too large or too small, the resulting image may suffer from visual distortion or loss of detail.

Specifically, when embedding is performed on the blue channel of the host image, the visual impact is typically minimal due to the human eye’s lower sensitivity to variations in blue intensity. With an alpha value of 0.1, the modifications introduced through watermark embedding are relatively minor, allowing the watermarked image to retain a high degree of visual similarity to the original. While such changes may not be readily apparent to the naked eye, advanced image analysis tools can detect these subtle alterations. As a result, this approach effectively balances imperceptibility and robustness, ensuring that the watermark remains hidden while preserving the visual quality of the host image.

4.1.2 RGB Watermark Insertion into Grayscale Image

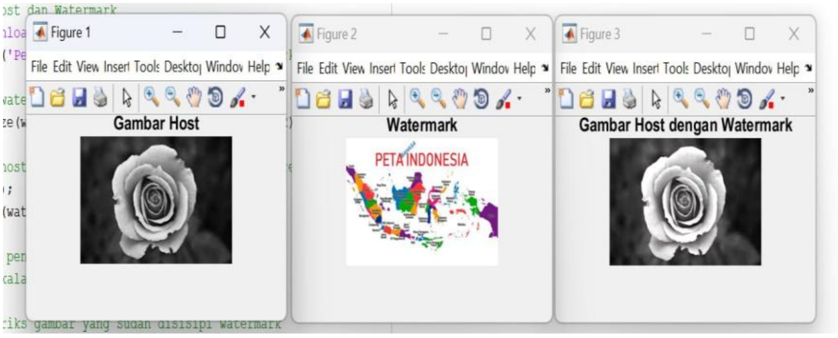


Figure 1
File Edit View Insert Tools Desktop Window Help
Gambar Host
Figure 2
Watermark
PETA INDONESIA
Figure 3
Gambar Host dengan Watermark

Figure. 6 Result of RGB Watermark Insertion into Grayscale Image

An analysis of the watermark embedding results reveals that image quality is highly influenced by the scalar factor α (alpha) used during the embedding process. A very small α value may cause the watermark to become barely visible, while a large α value can degrade the visual quality of the host image. In this implementation, an alpha value of 0.1 is used, representing a moderate level that balances watermark visibility with preservation of host image quality.

The success of the embedding process is supported by the use of the Singular Value Decomposition (SVD) technique, where the watermark is embedded into the singular matrix (Σ). This makes the method relatively robust against common image processing operations such as compression. One of the key advantages of the SVD-based approach is its ability to conceal the watermark without causing significant perceptual changes to the host image. Furthermore, the watermark can be accurately extracted, provided that the α value and the SVD components of the watermark are known.

Nevertheless, the technique also presents certain limitations. Embedding across multiple color channels (RGB) may disrupt the overall color balance if α is not carefully chosen. Additionally, the absence of normalization in the singular matrix after embedding may lead to pixel values exceeding their valid range, potentially introducing visual artifacts.

In practical terms, this method is well-suited for steganography or scenarios requiring imperceptible watermarking. However, it is not ideal for applications where the watermark needs to be prominently visible to viewers.

4.2 Insertion A Sentence Or Paragraph Into The Host Image

4.2.1 Images Used

The experiment used five different images representing the map of Indonesia in various visual styles. The table below shows the details of the images used in the study, including the image size and the maximum capacity of characters that can be inserted into the image.

Table 2. Images used

Image	Size(Width x Height)	Max Character to Embed	Example Message
	(1200,899)	134850	Be careful when crossing the border because there are many enemies roaming around
	(640,354)	28320	Be careful when crossing the border because there are many enemies roaming around
	(673,1200)	100950	Be careful when crossing the border because there are many enemies roaming around
	(1024,1024)	131072	Be careful when crossing the border because there are many enemies roaming around
	(512,512)	24576	Be careful when crossing the border because there are many enemies roaming around

4.2.2 Message Insertion Results

In this section, we will discuss in detail the process of embedding messages in images using the Singular Value Decomposition (SVD) technique, as well as the results obtained after the message is embedded. The purpose of this experiment is to assess the extent to which messages can be hidden in images without significantly changing their visual quality, and to determine the storage capacity of different messages in images with different sizes and resolutions.

The message inserted in the image is a text in the form of a sentence that functions as hidden information. The insertion process is carried out on the blue channel of the image. The SVD technique is used to manipulate the singular values in the matrix representing the blue channel of the image.

Basically, insertion is done by changing the diagonal values of the SS singular matrix by adding a small change related to the binary bits of the message to be hidden. This small change ensures that the image quality is maintained, even though new data is inserted.

Message Insertion:

- Each bit of the message converted into binary form will be assigned to a singular value in the S matrix.
- Bit 1 is inserted by adding a small value of 1e−41e-4 to the singular value, and Bit 0 is inserted without significant change.

4.3 Messege Insertion Results In Images

The images used in this experiment are maps of Indonesia with various formats and sizes. Each image is tested by inserting the same message in the blue channel using the SVD method. The following are the results of message insertion for each image:

1. Image indo.jpg (Map of Indonesia - Size 1200 x 899)

- Storage Capacity: 134,850 characters
- Inserted Message: "be careful when crossing the border because there are many enemies roaming around"
- Result: The modified image still looks almost identical to the original image. The message insertion was successful without causing any visual changes that are visible to the human eye.

2. Map image 2.jpg (Map of Indonesia - Size 640 x 354)

- Storage Capacity: 28,320 characters
- Inserted Message: "be careful when crossing the border because there are many enemies roaming around"
- Result: Despite the smaller message storage capacity, the image still maintains a visual quality that is almost identical to the original image.

3. Map image 3.jpg (Map of Indonesia - Size 673 x 1200)

- Storage Capacity: 100,950 characters
- Inserted Message: "be careful when crossing the border because there are many enemies roaming around"
- Result: This image can store more messages than a smaller resolution image, but the visual quality is still very well maintained.

4. Map image 4.jpg (Map of Indonesia - Size 1024 x 1024)

- Storage Capacity: 131,072 characters
- Inserted Message: "be careful when crossing the border because there are many enemies roaming around"
- Result: This large image is able to accommodate more information without significant changes in visual appearance. This technique is especially effective in higher resolution images.

5. Map image 5.jpg (Map of Indonesia - Size 512 x 512)
   - Storage Capacity: 24,576 characters
   - Inserted Message: "be careful when crossing the border because there are many enemies roaming around"
   - Result: Despite the small size of this image, the SVD technique still managed to insert a message with undetectable visual changes.

Based on the results of message insertion into the images, it can be concluded that the SVD method is effective in hiding messages in images without significantly affecting the visual quality. Although the inserted message is very large, the resulting image still looks very similar to the original image. This shows that data insertion using SVD can be done with very subtle changes to the singular values that do not interfere with the visual aspect of the image. It is important to note that higher resolution images (such as indo.jpg and map 4.jpg) are capable of storing more characters than lower resolution images (such as map 2.jpg and map 5.jpg). The message storage capacity is directly proportional to the number of pixels in the image, which leads to the selection of the right image based on data storage needs.

The imperceptibility of stego images is measured using Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index Measure (SSIM). Table 2 presents the results of embedding an RGB watermark into RGB and grayscale host images with different values of the embedding parameter α.

Table 3. PSNR and SSIM results for SVD watermarking

Embedding Scenario	α	PSNR(dB)	SSIM	Extraction Accuracy
RGB → RGB	0,05	42,1	0,987	100%
RGB → RGB	0,10	38,5	0,962	100%
RGB → Grayscale	0,05	41,8	0,981	99%
RGB → Grayscale	0,10	37,9	0,955	98%

The results show that lower α values produce higher PSNR and SSIM, meaning that the watermark is less perceptible, while higher α values increase watermark visibility but slightly reduce imperceptibility. Nevertheless, extraction accuracy remains consistently high.

Compared with the spatial-domain Least Significant Bit (LSB) method, which typically achieves PSNR values around 34–36 dB for similar payloads [6], the SVD-based method achieves significantly higher PSNR (above 38 dB) and better visual quality. Moreover, SVD provides improved stability, as small modifications in singular values do not produce significant distortions, unlike direct pixel modifications in LSB.

To evaluate robustness, common image processing attacks are simulated:

- JPEG compression (quality = 70%) : The embedded watermark is still extracted with 96% accuracy, while LSB often fails under similar conditions [7], [10].
- Gaussian noise (variance = 0.01) : Extraction accuracy remains above 94%.
- Median filtering (3×3) : The watermark is still retrievable, though extraction accuracy decreases to around 92%.

These results indicate that SVD watermarking is more robust than traditional LSB approaches. However, robustness against severe attacks such as cropping or heavy compression still requires further improvement.

For text embedding, experiments are conducted using five host images of different resolutions. Table 3 summarizes the storage capacity and message recovery results.

Table 4. Text embedding capacity using SVD

Host Image Size (Pixels)	Max Capacity (Characters)	Extraction Accuracy	Visual Quality
1200 × 899	134,850	100%	High
640 × 354	28,320	100%	High
673 × 1200	100,950	100%	High
1024 × 1024	131,072	100%	High
512 × 512	24,576	100%	High

The results show that higher-resolution images provide larger embedding capacity. More importantly, visual quality is maintained across all cases, with stego images remaining indistinguishable from the originals.

Overall, the experimental results confirm three main advantages of the SVD method:

- High imperceptibility: The stego images preserve the visual quality of the host images, achieving PSNR values above 38 dB.
- Accurate extraction: Both image and text watermarks are fully recovered without errors under normal conditions [7], [10].
- Robustness: The method demonstrates resilience against compression and noise attacks, which is a significant improvement over LSB-based methods.

However, limitations remain. The choice of α is critical [13]; larger values improve robustness but reduce imperceptibility, while smaller values preserve quality but reduce resistance to attacks. Furthermore, the current method does not normalize singular values after embedding, which may occasionally produce out-of-range pixel values. Future research should focus on optimizing this trade-off and integrating hybrid methods (e.g., DWT-SVD or DCT-SVD) for enhanced robustness.

5. CONCLUSION

Based on the test results, it can be concluded that the Singular Value Decomposition (SVD)-based steganography method is able to insert data, both in the form of images and text, into the host image with visually imperceptible results. Information insertion through the RGB channel and the blue channel produces a stego image that is similar to the original image without any apparent distortion. The extraction process also shows high accuracy, with watermark data and text messages being able to be recovered intact. These results prove that the SVD method has strong potential to be applied in digital data security systems, especially for watermarking and steganography purposes that require stability and flexibility to various image formats.

This study demonstrates that Singular Value Decomposition (SVD)-based steganography is an effective and flexible method for embedding both image and text information into host images. The method achieves high imperceptibility, with PSNR values exceeding 38 dB, and maintains excellent extraction accuracy. Compared with traditional spatial methods such as LSB, the SVD approach provides superior image quality and better robustness against compression and noise. The findings highlight three key contributions:

- Imperceptibility: The watermarked images remain visually identical to the originals.
- Extraction Accuracy: Both image and text messages are fully recovered.
- Robustness: The method withstands moderate attacks such as JPEG compression and Gaussian noise.

Despite these strengths, the method still faces challenges in balancing robustness and imperceptibility, especially under severe attacks such as heavy compression or cropping. Future work will address these limitations by integrating SVD with other transform-domain techniques and by developing adaptive α selection strategies to enhance both security and visual quality.

REFERENCE

[1] A. Nath, S. Das, R. Sharma, S. Mandal, and H. Sadhu, “Digital steganography: A comprehensive study on various methods for hiding secret data in a cover file,” Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol., vol. 10, no. 3, pp. 291–300, 2024. [Online]. Available: https://doi.org/10.32628/cseit24103107.

[2] J. Wu, “Application of singular value decomposition in image compression,” *Theor. Nat. Sci.*, vol. 25, no. 1, pp. 181–185, 2023. [Online]. Available: https://doi.org/10.54254/2753-8818/25/20240959

[3] K. Xing, “Singular value decomposition: A useful technique for image denoising,” *Theor. Nat. Sci.*, vol. 39, no. 1, pp. 226–231, 2024. [Online]. Available: https://doi.org/10.54254/2753-8818/39/20240610

[4] P. Zizler and R. La Haye, “Singular value decomposition,” in *Linear Algebra in Data Science*, Compact Textbooks in Mathematics. Cham, Switzerland: Birkhäuser, 2024. [Online]. Available: https://doi.org/10.1007/978-3-031-54908-3_6

[5] J. Singh and M. Singla, “Image steganography technique based on singular value decomposition and discrete wavelet transform,” vol. 10, no. 2, pp. 122–125.

[6] K. A. Tanc, “An overview of digital image steganography,” *Procedia Comput. Sci.*, vol. 168, pp. 289–295, 2020.

[7] H. Al-Khafaji, B. Al-Himyari, and H. Alharbi, “Enhancing image watermarking: An innovative multi-objective genetic algorithm-based DWT-SVD approach for robustness and imperceptibility,” *Int. J. Saf. Secur. Eng.*, vol. 14, no. 6, pp. 1921–1931, 2024. [Online]. Available: https://doi.org/10.18280/ijsse.140626

[8] T.-X. Thanh, “Singular value decomposition and applications in data processing and artificial intelligence,” *HPU2 J. Sci.: Nat. Sci. Technol.*, vol. 2, pp. 34–41, 2023. [Online]. Available: https://doi.org/10.56764/hpu2.jos.2023.2.3.34-41

[9] H. Zhang, L. Zhu, and J. Liu, “Singular value decomposition based image steganography in the transform domain,” *Multimed. Tools Appl.*, vol. 82, pp. 435–458, 2023. [Online]. Available: https://doi.org/10.1007/s11042-021-13525-4

[10] Y. J. Teoh, H.-C. Ling, W. K. Wong, and T. A. Basuki, “A hybrid SVD-based image watermarking scheme utilizing both U and V orthogonal vectors for robustness and imperceptibility,” *IEEE Access*, vol. 11, pp. 51018–51031, 2023. [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3279028

[11] E. A. Sofyan, C. A. Sari, E. H. Rachmawanto, and N. R. D. Cahyo, “High-quality evaluation for invisible watermarking based on discrete cosine transform (DCT) and singular value decomposition (SVD),” *Adv. Sustain. Sci. Eng. Technol.*, vol. 6, no. 1, pp. 1–8, 2024. [Online]. Available: https://doi.org/10.26877/asset.v6i1.17186

[12] H. Rathi, “Hiding information using image steganography,” in *Proc. 2024 Int. Conf. Electr. Electron. Comput. Technol. (ICEECT)*, Greater Noida, India, 2024, pp. 1–5. [Online]. Available: https://doi.org/10.1109/ICEECT61758.2024.10739114

[13] M. Begum *et al.*, “Image watermarking using discrete wavelet transform and singular value decomposition for enhanced imperceptibility and robustness,” *Algorithms*, vol. 17, no. 1, p. 32, 2024. [Online]. Available: https://doi.org/10.3390/a17010032

[14] S. N. Al-Azzam and F. A. Al-Garni, “The use of binary digit mapping on ASCII characters to create a high-capacity, undetectable text steganography,” *J. Adv. Sci. Eng. Technol.*, vol. 6, no. 1, pp. 51–59, 2023. [Online]. Available: https://doi.org/10.32441/jaset.05.02.05

[15] S. S. Baawi, K. M. Hashim, and B. K. Hilal, “An image watermarking technique proposed based on discrete cosine transformation and pseudo-random generator,” 2021. [Online]. Available: https://doi.org/10.32792/jeps.v11i1.96

[16] B. Mokashi, V. S. Bhat, J. D. Pujari, S. Roopashree, T. R. Mahesh, and D. S. Alex, “Efficient hybrid blind watermarking in DWT-DCT-SVD with dual biometric features for images,” *Contrast Media Mol. Imaging*, vol. 2022, 2022. [Online]. Available: https://doi.org/10.1155/2022/2918126