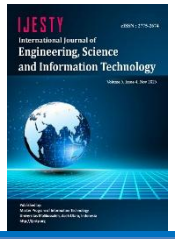
International Journal of Engineering, Science and Information Technology
Volume 5, No. 4 (2025) pp. 251-259
eISSN: 2775-2674
Website: http://ijesty.org/index.php/ijesty
DOI: https://doi.org/10.52088/ijesty.v5i4.1008
Research Paper, Short Communication, Review, Technical Paper



Smart Stego: A Web Application for Hiding Secret Data in Images with LSB and CNN

I Gede Totok Suryawan[1]*, Made Sudarma[2], I Ketut Gede Darma Putra[3], Anak Agung Kompiang Oka Sudana[3]

[1]Department of Engineering Science, Faculty of Engineering, Udayana University, Denpasar, Indonesia
[2]Department of Electrical Engineering, Faculty of Engineering, Udayana University, Denpasar, Indonesia
[3]Department of Information Technology, Faculty of Engineering, Udayana University, Denpasar, Indonesia

**Corresponding author Email: totok.suryawan@gmail.com*

The manuscript was received on 22 February 2025, revised on 15 May 2025, and accepted on 2 August 2025, date of publication 11 November 2025

Abstract

This study develops a web-based steganography model to insert the identity of artisans in the form of palmprint images into the image of gringsing ikat woven cloth as a medium for ownership authentication. The method used in the insertion process combines a Convolutional Neural Network and the Least Significant Bit. In contrast, extracting or re-introducing palmprint images from stego images is carried out using a CNN-based classification model. This system was tested with two scenarios; in the first scenario, one palmprint image was inserted into 26 different cloth motifs, while in the second scenario, one cloth motif was inserted into 99 different palmprint images. The test results showed that the system produced consistent confidence values for all cloth motifs in the first scenario. In contrast, in the second scenario, the system achieved an average confidence of 93.5% and a recognition accuracy of 87%. The developed application has proven to be efficient with a reduction in stego image size of up to 66% while maintaining the quality of the stego image, as well as a speedy average execution time of 0.15 seconds for insertion and 0.09 seconds for extraction. These findings prove that the developed steganography model can effectively insert and re-recognize identity images (palmprints) in woven cloth images and has the potential to be applied as an image-based craft product ownership verification system.

Keywords: *Image Steganography, Convolutional Neural Network, Least Significant Bit, Deep Steganography.*

1. Introduction

Cryptography and steganography are popular methods for securing digital images. Image cryptography involves transforming the original image into an unrecognizable form using cryptographic algorithms. Cryptographic methods are not designed to hide information within multimedia data and do not offer the ownership protection or message-hiding features that watermarking or steganography provides. Cryptography does not provide resistance to data manipulation attacks like watermarking does, and it cannot maintain the confidentiality of the hidden message like steganography does. Cryptography cannot hide the fact that data has been secured, which can raise suspicion. On the other hand, steganography is designed to be undetectable, making it better suited to applications where confidentiality must be completely hidden. Cryptography is not flexible for multimedia applications where the quality and usability of the data must be maintained during the encryption process. Watermarking and steganography excel in this regard because they preserve the original functionality of the data. Cryptography cannot meet the specific needs of watermarking and steganography applications designed to secure copyright and hide messages, making it unsuitable for verifying ownership of digital artwork.

On the other hand, research in steganography mainly uses digital images already of excellent quality, such as lena, babon, peppers, house, moon, house, and kite [1] [2] [3]. It is rare to find research results that apply steganography methods to community artworks such as woven cloth crafts. Therefore, this study uses steganography methods to insert the identity of woven cloth artisans into the cloth image taken directly from the cloth artisans. The image of the woven cloth is used as a cover image, and the palmprint is used as a secret image. The process of inserting palmprints into the cloth image produces a stego image, and this stego image can then be extracted to recognize the palmprint that has been previously inserted. This study aims to verify the ownership of the woven cloth image based on the palmprint inserted into the cloth image. The methods used in the palmprint insertion process are Convolutional Neural Network (CNN) and Least Significant Bit (LSB). In the extraction process, the CNN method is used to classify or recognize palmprints in the stego image. Both models developed are converted into a website-based application, so the insertion and extraction processes can be done easily.

2. Literature Review

In the context of transform-based steganography, three commonly used methods are Discrete Cosine Transform (DCT) [4], Discrete Wavelet Transform (DWT) [5], and Discrete Fourier Transform (DFT) [6]. DCT is widely used in image compression, especially in JPEG format. DCT works by separating an image into frequency components, which allows information to be hidden at frequencies less sensitive to the human eye. However, DCT tends to be more vulnerable to attacks and image modifications, which can reduce the quality of the embedded watermark [7] [8]. DCT, compared to DWT in terms of imperceptibility, robustness, and capacity, shows that while DCT performs well in compression, DWT is superior in terms of attack resistance [7]. Although less commonly used in steganography than DCT and DWT, DFT can convert the time domain to the frequency domain, allowing for watermark embedding at specific frequencies. However, DFT is often more complex in its implementation and may not be as efficient as DCT or DWT regarding speed and storage capacity [9] [10].

Several optimizations of transformation methods have been carried out, including integer-based ones such as Lah transforms [11], Catalan Transform [12], and Laguerre Transform [12] can maintain the security of confidential data but increase time complexity; in addition, the image quality will decrease after insertion due to low storage capacity compared to methods that work on spatial domains such as LSB [13], EMD [14][15] [16], and PVD [17][18]. The LSB method is used by [19] in their paper entitled "An Efficient Steganographic Technique for Hiding Data," presenting a steganography technique that aims to increase data hiding capacity while maintaining visual quality with the inversion method on certain bits.

A comparative analysis of the application of the LSB method in various image formats was conducted by [20]. His paper also stated that LSB has advantages in its ability to hide data with minimal visual changes to the image. However, LSB has the disadvantage that this method is vulnerable to statistical analysis attacks due to the distortion that occurs when more message bits are inserted. A critical review of research results applying the LSB method was conducted by [21]. The review was conducted on 20 research results from 2016 to 2020, evaluating the application of the LSB method implemented for various datasets with two evaluation parameters, namely PSNR and MSE values. The review results show that LSB can improve the quality of image steganography, as indicated by high PSNR values. However, it faces challenges in terms of data embedding capacity and data confidentiality, which are limited to 1 to 4 bits.

The LSB optimization method using a bidirectional coding approach was carried out by [22]. In their paper entitled "A New Approach for Enhancing LSB Steganography Using Bidirection Coding Scheme," they carried out the optimization to minimize distortion in the cover image by dividing the image into small blocks and inserting a secret message based on the level of similarity between the image and message bits. The experimental results showed a significant reduction in MSE values and increased SSIM values compared to the traditional LSB method, especially in smaller image blocks. The weakness of the applied bidirectional coding method is an increase in computational complexity, mainly due to the division of the image into small blocks and the need for additional calculations to determine the coding direction of each block. In addition, this technique is limited to grayscale images, so it is less optimal when applied to color images or other media formats.

Another optimization of LSB is done by combining LSB with AES and Blowfish encryption methods [23]. The weakness of this approach is its higher complexity in terms of encryption algorithms and image processing. In addition, adding encryption algorithms can increase the encryption and decryption process time, which is a challenge in real-time applications or for extensive data. The application of 4-factor security techniques to the LSB method was carried out by [24]. The four factors combine Rail Fence Cipher, RSA Encryption, Aztec Code, and LSB Steganography. Combining four layers of security at once requires higher computing power and can slow down the encryption and decryption process. In addition, although this method is effective in terms of security, its application in a real-time environment or with large image files can be challenging.

Various optimizations have been done to improve the performance of the LSB method, especially in improving the security of stego images from attacks. In general, multiple optimizations can improve data security, but the optimization techniques applied will increase the computational load, so other optimization techniques are needed to improve the performance of this LSB. Deep learning such as CNN has been proven successful in various digital image processing processes such as medical images [25] [26] [27], handwriting images [28], and olso woven cloth [29] can be a solution for optimizing steganography methods such as LSB.

3. Methods

This section will discuss the dataset used and the methods or stages of research that have been carried out in this study. This study uses the gringsing ikat woven cloth dataset as a cover image and the palmprint dataset as a secret image. The application developed is a deep learning application for secret image insertion using CNN-LSB and palmprint recognition using CNN.

3.1. Data Acquisition

The dataset used in this study was taken directly from the artisans of ikat gringsing woven cloth in Tenganan Pegringsingan Village, Karangasem, Bali. The woven cloth data used consisted of twenty-six motifs and 15 images for each motif. The palm data used were ninety-nine palms of different people, and each consisted of 6 images. Examples of several photos of ikat gringsing woven cloth used in this study can be seen in Figure 1. The palm images can be seen in Figure 2 below.

Fig 1. Gringsing Woven Cloth

Fig 2. Palm Print

In general, this research has three stages: data collection, model development, and web-based application development. Details of the research process can be seen in Figure 3 below.

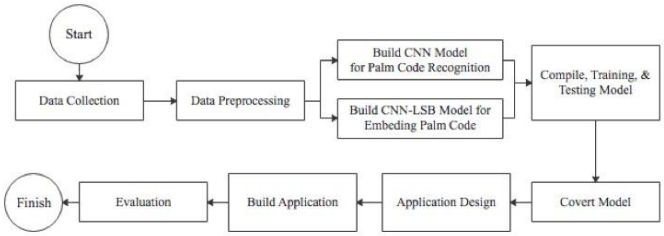


Fig 3. Research Stage

This study began with collecting gringsing ikat woven cloth data and palmprint data, as discussed in the previous point. The collected data was then subjected to a preprocessing process of cropping, changing the color to grayscale, and correcting noise using Contrast Limited Adaptive Histogram Equalization (CLAHE). The following Figure 4 is an example of improving the quality of palmprint images using CLAHE.

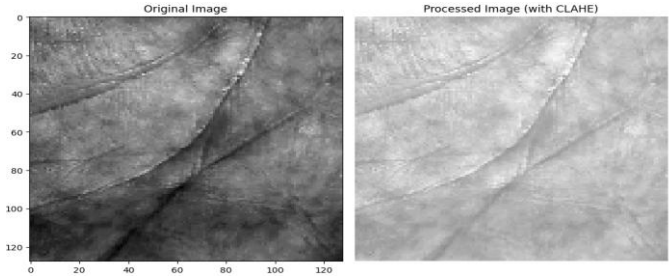


Fig 4. Image Enhancement Using CLAHE

Next, the model development process is carried out, as seen in Figure 3. Two models were developed in this study: the CNN model for palmprint recognition using Alexnet and CNN-LSB for edge detection and palmprint insertion into the image of gringsing woven cloth. AlexNet is a simple yet effective CNN architecture for classification. The basic Alexnet architecture consists of five convolutional layers and three fully connected layers. Figure 5 illustrates the basic architecture of AlexNet.

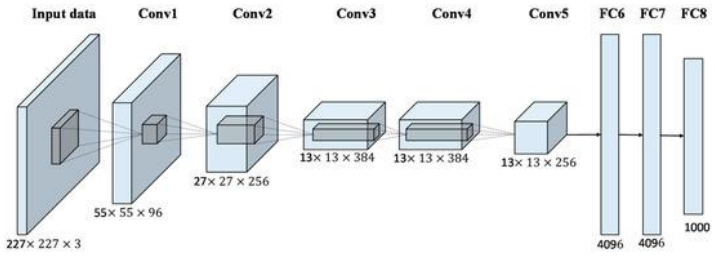


Fig 5. Alexnet Architecture

In this study, we conduct palmprint code classification using the AlexNet model with a pre-training approach provided by Torchvision. We evaluate the effectiveness of the AlexNet architecture—pre-trained on the large and complex ImageNet dataset—in classifying palmprint patterns found in images of Gringsing ikat woven cloth. We expect the use of pre-training to enhance AlexNet's ability to extract relevant features and improve classification accuracy. To optimize model performance, we implement several modifications. Specifically, we freeze the convolutional layers during the feature extraction phase by setting param.requires_grad to False, and we update only the final layers during training. We use the Adam optimizer with a learning rate of 0.001 and apply the cross-entropy loss function to calculate the classification error.

Both models were decompiled, trained for 200 epochs, and tested using previously provided test data. The model is then converted for further use in a website-based application. The results of the application that has been developed will be discussed in the next stage.

4. Results and Discussion

The application developed in this study is web-based and has two menus: "Embed Secret" and "Extract from Stego." The "Embed Secret" menu is used to embed palmprints (secret image) into the image of the gringsing ikat woven cloth (cover image). The output of this embedding process will produce a new image called a stego image (an image containing palmprints). The "Extract from Stego" menu extracts palmprints from stego images. The output of this extraction process is the same palmprint as the palmprint in the embedding process.

4.1. Embedding Process

Embedding palmprints into woven cloth images is done using "Embed Secret." This menu has three sub-menus, namely, the upload cover image menu used to upload gringsing ikat woven cloth, the upload secret image menu used to upload palmprint images, and the menu for selecting the edge detection method to be used, and is equipped with an "embed" button for the process of embedding secret images into cover images. The "Embed Secret" menu can be seen in Figure 6, and the following menu.

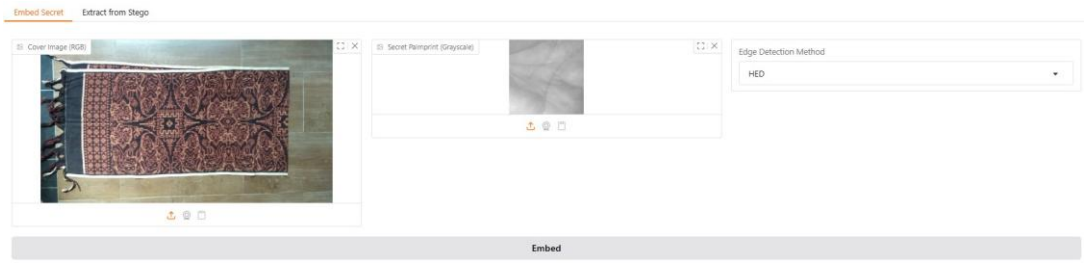


Fig 6. "Embed Secret" Menu

The palmprint embedding process in this study was carried out on edge images so that the developed application is equipped with a choice of edge detection methods. Data insertion on this edge image is carried out to insert more data, maintain the quality of the cover image, and protect the secret image from steganalysis attacks. The following is an example of the edge detection results produced by the application developed in this study, which can be seen in Figure 7 below.

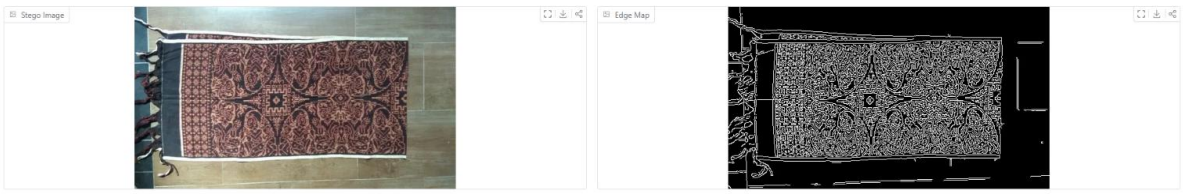


Fig 7. Edge Result

Inserting data into the edge image in this study has been proven to maintain the quality of the woven cloth image. This from the histogram of the cover and stego images in Figure 8; there is no significant difference.

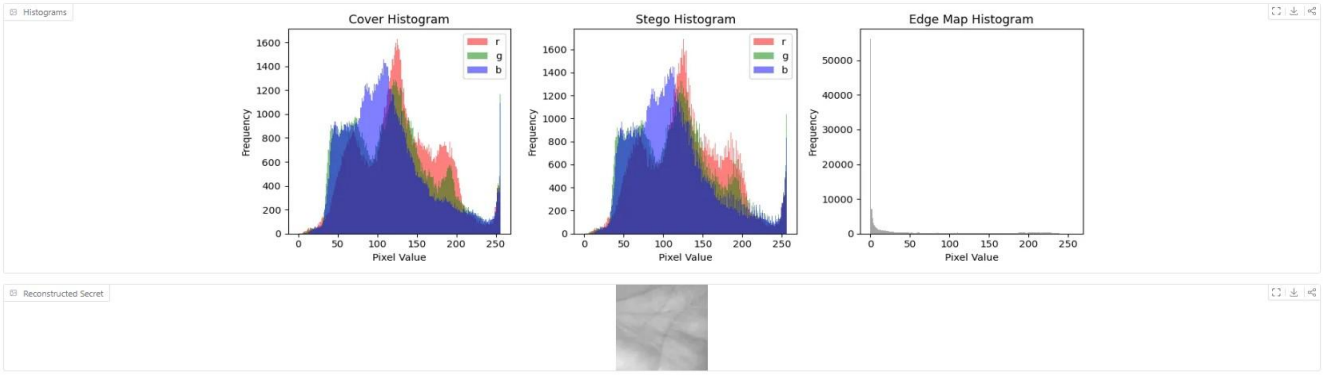


Fig 8. Histogram Result

In addition to being seen from the histogram, the stego image quality produced in this study can also be seen from the PSNR (Peak Signal-to-Noise Ratio) value, which is more than 54 dB. This value is much higher than the standard quality of digital images of 30dB [Reference]. In addition to the PSNR value, this application is also equipped with other matrices such as the size of the cover image and stego image, data insertion capacity and the amount of data inserted, application performance measured by the speed of the embedding and extraction process, resistance to steganalysis attacks, and most importantly equipped with a label of the results of the palmprint prediction that is inserted along with its level of confidence. In addition, as seen in Figure 9, this application is equipped with a stego image download menu at the end of the embedding process.

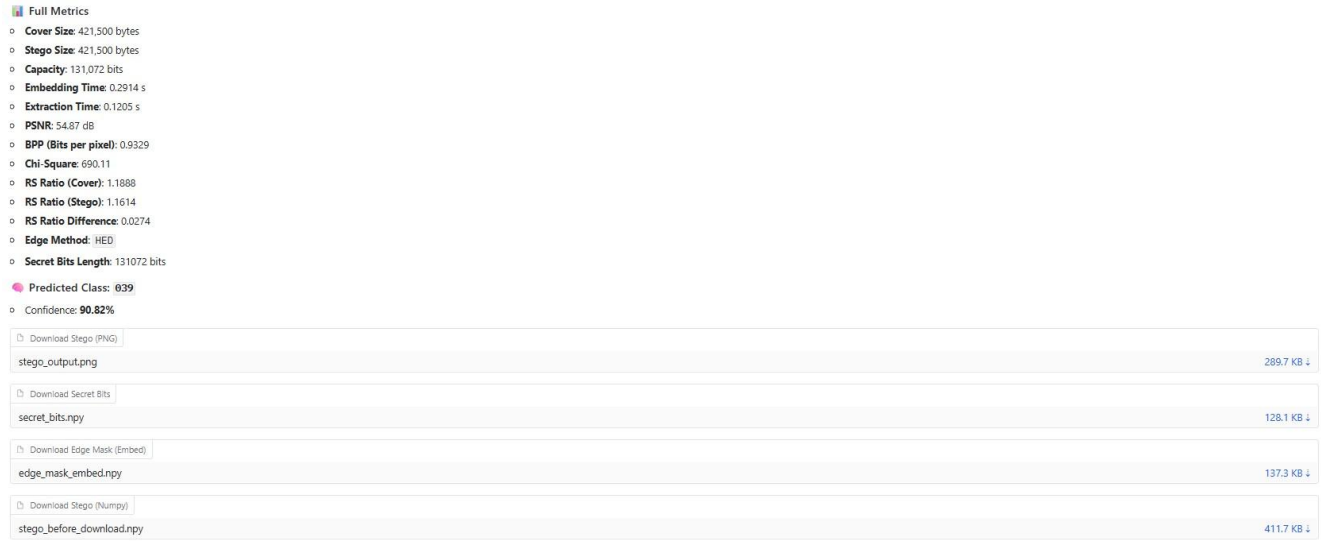


Fig 9. Stego Metric

4.2. Extraction Process

The stego images in this application can be extracted using the “Extract from Stego” menu. This menu has several sub-menus, such as a menu for uploading stego photos, a menu for selecting an edge detection method, and a menu for determining the number of bits to be extracted. It is also equipped with an extract secret image button. The appearance of the “Extract from Stego” menu can be seen in Figure 10 below.

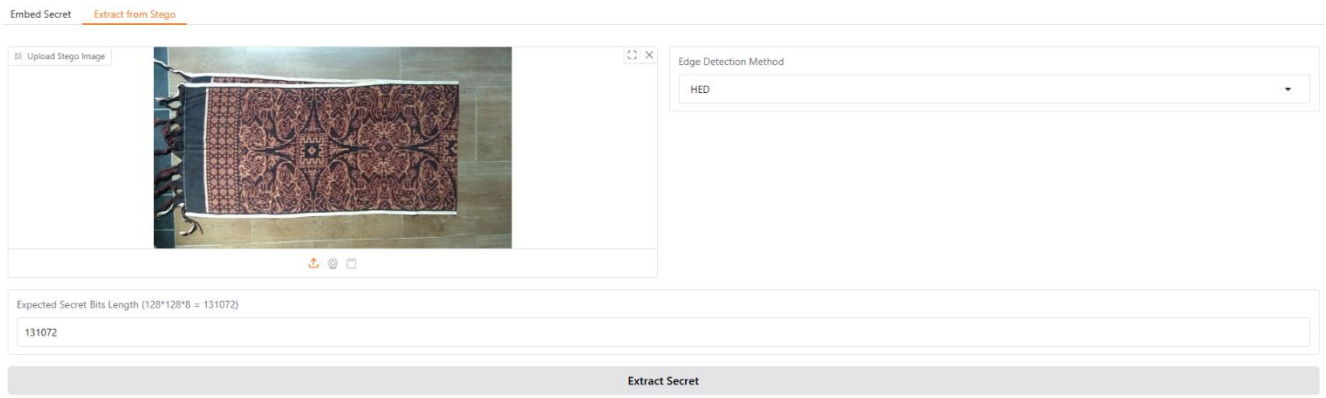


Fig 10. “Extract From Stego” Menu

The palmprint extraction results from the stego image are immediately displayed after the user presses the extract secret button. As seen in Figure 11, this application is equipped with a class or label prediction from the previously inserted palmprint to ensure that the palmprint extraction results are carried out correctly. The prediction results are also equipped with a level of prediction confidence value and the time required for the extraction process. At the end of this application, it is equipped with a download edge mask menu to download the edge detection results according to the previously selected edge detection method.

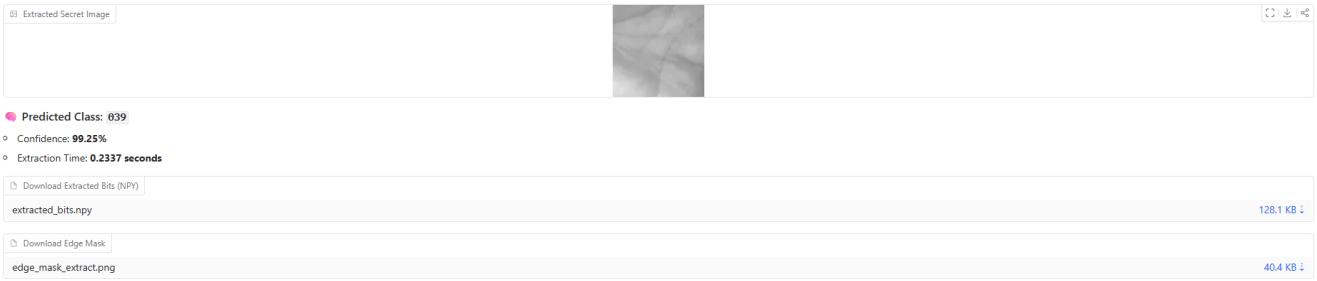


Fig 11. Predicted Class

4.3. Discussion

The application developed in this study has been tested using twenty-six gringsing ikat woven cloth motifs and ninety-nine different people's palmprints. Two test scenarios are used in the embedding and extraction process: (1) One person's palmprint is inserted into twenty-six different cloth motifs, and (2) One woven cloth motif is inserted with ninety-nine different palmprints. The results of the first test show that each cloth motif (cover image) inserted with a palmprint (secret image) produces the same confidence value. The results of the second scenario test produce different confidence values , with an average confidence value of 93.5%. The data from the application test results in this study can be seen in Table 1 below.

Table 1. Confidence Value Stego Image Extraction Result

Palmprint Number	Gringsing Woven Cloth Motif							
	Batun_Cagi	Cakra	Lubeng	Trisula	Wayang_Candi	Gringsing_Isi	…….	Yudha
001	86,66	86,66	86,66	86,66	86,66	86,66	…….	86,66
002	98,28	98,28	98,28	98,28	98,28	98,28	…….	98,28
003	96,69	96,69	96,69	96,69	96,69	96,69	…….	96,69
004	98,82	98,82	98,82	98,82	98,82	98,82	…….	98,82
005	95,16	95,16	95,16	95,16	95,16	95,16	…….	95,16
…….	…….	…….	…….	…….	…….	…….	…….	…….
098	82,96	82,96	82,96	82,96	82,96	82,96	…….	82,96
099	79,53	79,53	79,53	79,53	79,53	79,53	…….	79,53

The application did not correctly recognize all 89 palmprints used for testing in this study. 13 palmprints failed to be recognized, and 86 were successfully recognized during the stego image extraction process. So, the application developed in this study successfully recognized 87% of palmprints correctly.

In this study, we represent image pixel values as raw data in the form of a NumPy array (stego_pixels), where the memory size is determined by the formula height × width × channels × sizeof(pixel_data_type). Rather than storing these pixel values directly to disk, we convert them into a PIL. Image object using the function Image.fromarray(stego_pixels). This process transforms the raw array into a

Pillow-compatible image object that retains both pixel information and internal metadata necessary for image processing. The experimental results demonstrate that this conversion reduces the average stego image file size by approximately 66%, indicating that the proposed steganography model can significantly decrease computational load. Despite the reduction in file size, the visual quality of the stego images remains high. The lowest Peak Signal-to-Noise Ratio (PSNR) value recorded is 53 dB, which falls within the "very good" category for digital image quality, while the highest PSNR reaches 59 dB, with an overall average of 58 dB. In addition to minimizing file size and computational demand, the conversion also improves time efficiency. We evaluate system performance based on insertion time and extraction time, with the results summarized in Table 2, using a dataset of ninety-nine palmprint images.

Table 2. Embedding and Extraction Time

Palmprint Number	Embedding Time (s)	Extraction Time (s)
001-5	0,13	0,08
002-5	0,13	0,07
003-5	0,14	0,08
004-5	0,14	0,08
005-5	0,15	0,09
0099-5	0,14	0,09
…….	…….	…….
0012-5	0,16	0,17
0019-5	0,21	0,11
0031-5	0,17	0,23
0033-5	0,17	0,13
0037-5	0,3	0,12
0051-5	0,22	0,08
0061-5	0,16	0,21
0063-5	0,16	0,12

Table 2 presents the results of timing analysis for 99 palmprint insertion processes. Among them, 91 insertions were completed with an average time of 0.14 seconds, while the remaining 8 insertions took an average of 0.17 seconds. For the corresponding extraction processes, we observed an average time of 0.08 seconds for the 91 cases and 0.13 seconds for the remaining 8 cases. Overall, the system achieved an average insertion time of 0.15 seconds and an average extraction time of 0.09 seconds, demonstrating good time efficiency for the proposed steganography approach.

We conducted a steganalysis evaluation using statistical methods by analyzing the Chi-Square value to assess the detectability of hidden data. This metric measures the deviation of the LSB bit histogram distribution in the stego image from the expected (ideal) distribution in the cover image. A low Chi-Square value indicates that the LSB distribution closely resembles that of a natural image, making the presence of hidden data more challenging to detect. Conversely, a high Chi-Square value reflects a noticeable deviation, which may indicate increased detectability of embedded data. Figure 12 presents the Chi-Square analysis results for the stego images in this study.

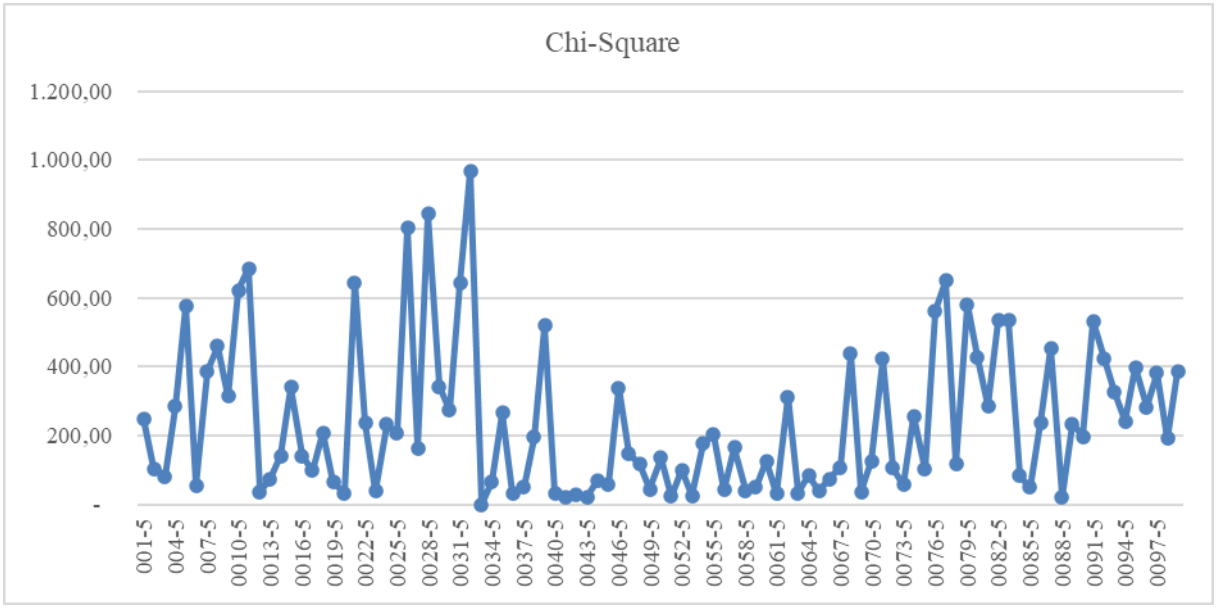


Fig. 12. Chi-Square Value

Figure 11 presents the Chi-Square values obtained from the insertion of 99 palmprint codes into images of Gringsing ikat woven cloth. The analysis yields an average Chi-Square value of 287.19, indicating that, in general, the embedded stego images exhibit characteristics that are difficult to distinguish from the original cover images. This result suggests that the steganography model demonstrates strong concealment capabilities. However, we observe notable variability in model performance. Specifically, four palmprint codes—0026-5, 0028-5, 0033-5, and 0032-5—exhibit significantly higher Chi-Square values of 803.66, 844.25, 849.29, and 968.71, respectively. These

elevated values suggest a higher risk of detection for these specific cases, indicating that the stego content may be more easily distinguishable from the cover image in those instances..

5. Conclusion

This study develops a web-based steganography model to insert palmprint data into a gringsing ikat woven cloth image. The methods used in the insertion process are CNN and LSB. In the extraction process, the CNN method is used to classify or recognize palmprints in the stego image. Based on the test results of the developed website-based steganography model, it successfully inserted palmprints into the gringsing ikat woven cloth image and successfully extracted or reintroduced the palmprints inserted into the image of a cloth. Tested using ninety-nine different people's palmprints, this web-based steganography model successfully recognized 87% of the palmprints of the test data. In addition, this steganography model also shows good performance, consistently recognizing palmprints on twenty-six gringsing ikat woven cloth motifs with an average confidence value of 93.5%. The developed application demonstrates high efficiency, achieving a reduction in stego image size of up to 66% while maintaining image quality. It also delivers fast execution times, with an average of 0.15 seconds for insertion and 0.09 seconds for extraction.

References

[1] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image," *Multimed. Tools Appl.*, vol. 75, no. 22, pp. 14867–14893, 2016, doi: 10.1007/s11042-015-2671-9.

[2] L. Widyawati, I. Riadi, and Y. Prayudi, "Comparative Analysis of Image Steganography using SLT, DCT and SLT-DCT Algorithm," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 20, no. 1, pp. 169–182, 2020, doi: 10.30812/matrik.v20i1.701.

[3] J. Qin, Y. Luo, X. Xiang, Y. Tan, and H. Huang, "Coverless image steganography: A survey," *IEEE Access*, vol. 7, pp. 171372–171394, 2019, doi: 10.1109/ACCESS.2019.2955452.

[4] M. A. Hosen, S. H. Moz, S. S. Kabir, M. N. Adnan, and S. M. Galib, "In-depth exploration of digital image watermarking with discrete cosine transform and discrete wavelet transform," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 33, no. 1, pp. 581–590, 2024, doi: 10.11591/ijeecs.v33.i1.pp581-590.

[5] D. G. and K. S. K. A. R. Babu, R. R. Al-Fatlawy, K. Veeranjaneyulu, "Canonical Huffman Coding (CHC) - Discrete Wavelet Transform (DWT) Method for Image Steganography," in *2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)*, 2024, doi: 10.1109/ICICACS60521.2024.10498392.

[6] M. R. and A. Sengupta, "Design Flow of Secured N-Point DFT Application Specific Processor Using Obfuscation and Steganography," *EEE Lett. Comput. Soc.*, vol. 3, no. 1, pp. 13–16, 2020, doi: 10.1109/LOCS.2020.2973586.

[7] Hosen et al, "In-depth exploration of digital image watermarking with discrete cosine transform and discrete wavelet transform," *Indones. J. Electr. Eng. Comput. Sci.*, 2024, doi: 10.11591/ijeecs.v33.i1.pp581-590.

[8] S. and Rahayu, "Watermarking using DCT and DWT on Pneumonia images," *J. Appl. Intell. Syst.*, 2023, doi: doi:10.33633/jais.v8i3.8914.

[9] G. et Al, "Discrete wavelet transform-based color image watermarking using uncorrelated color space and artificial bee colony," *Int. J. Comput. Intell. Syst.*, 2015, doi: 10.1080/18756891.2015.1001958.

[10] Rana et al, "Transform Domain Image Watermarking using DCT, DWT and SVD," *Int. J. Innov. Technol. Explor. Eng.*, 2019, doi: 10.35940/ijitee.l2733.1081219.

[11] S. K. Ghosal, S. Mukhopadhyay, S. Hossain, and R. Sarkar, "Application of Lah transform for security and privacy of data through information hiding in telecommunication," *Trans. Emerg. Telecommun. Technol.*, vol. 32, no. 2, pp. 1–20, 2021, doi: 10.1002/ett.3984.

[12] S. Mukhopadhyay, S. Hossain, S. K. Ghosal, and R. Sarkar, "Secured image steganography based on Catalan transform," *Multimed. Tools Appl.*, vol. 80, no. 9, pp. 14495–14520, 2021, doi: 10.1007/s11042-020-10424-4.

[13] M. A. Aslam *et al.*, "Image Steganography using Least Significant Bit (LSB)-A Systematic Literature Review," *Proc. 2022 2nd Int. Conf. Comput. Inf. Technol. ICCIT 2022*, no. June 2023, pp. 32–38, 2022, doi: 10.1109/ICCIT52419.2022.9711628.

[14] Z. Qu, H. Sun, and M. Zheng, "An efficient quantum image steganography protocol based on improved EMD algorithm," *Quantum Inf. Process.*, vol. 20, no. 2, pp. 1–29, 2021, doi: 10.1007/s11128-021-02991-8.

[15] Z. S. Younus and M. K. Hussain, "Image steganography using exploiting modification direction for compressed encrypted data," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 2951–2963, 2022, doi: 10.1016/j.jksuci.2019.04.008.

[16] H. S. Leng, J. F. Lee, and H. W. Tseng, "A high payload EMD-based steganographic method using two extraction functions," *Digit. Signal Process. A Rev. J.*, vol. 113, p. 103026, 2021, doi: 10.1016/j.dsp.2021.103026.

[17] S. Prasad and A. K. Pal, "An RGB colour image steganography scheme using overlapping block-based pixel-value differencing," *R. Soc. Open Sci.*, vol. 4, no. 4, 2017, doi: 10.1098/rsos.161066.

[18] A. K. Sahu, G. Swain, M. Sahu, and J. Hemalatha, "Multi-directional block based PVD and modulus function image steganography to avoid FOBP and IEP," *J. Inf. Secur. Appl.*, vol. 58, no. March, p. 102808, 2021, doi: 10.1016/j.jisa.2021.102808.

[19] and L. M. Nashat, Dalia, "An Efficient Steganographic Technique for Hiding Data," *J. Egypt. Math. Soc.*, vol. 10, no. 1, 2019.

[20] I. N. and K. A. T. Ejidokun, O. O. Omitola, "Implementation and Comparative Analysis of Variants of LSB Steganographic Method," in *2022 30th Southern African Universities Power Engineering Conference (SAUPEC)*, 2022, doi: https://doi.org/10.1109/SAUPEC55179.2022.9730643.

[21] and M. W. A. Aslam, Muhammad Adnan, Muhammad Rashid, Farooque Azam, Muhammad Abbas, Yawar Rasheed, Saud S. Alotaibi, "Image Steganography Using Least Significant Bit (LSB)-A Systematic Literature Review," in *2nd International Conference on Computing and Information Technology, ICCIT*, 2022, doi: https://doi.org/10.1109/ICCIT52419.2022.9711628.

[22] and H. A. L. Al-Momin, Mohammed, Issa Ahmed Abed, "A New Approach for Enhancing LSB Steganography Using

Bidirectional Coding Scheme," *Int. J. Electr. Comput. Eng.*, vol. 9, no. 6, 2019, doi: https://doi.org/10.11591/ijece.v9i6.pp5286-5294.

[23] and S. A. Alanzy, May, Razan Alomrani, Bashayer Alqarni, "Image Steganography Using LSB and Hybrid Encryption Algorithms," *Appl. Sci.*, vol. 13, no. 21, 2023, doi: https://doi.org/10.3390/app132111771.

[24] N. S. & S. M. A. Sreenidhi, B. Shruti, Ambati Divya, "Highly Secure Lsb-Based Image Steganography with Four-Factor Security," *Intell. Comput. Syst. Appl.*, 2024, doi: https://doi.org/https://doi.org/10.1007/978-981- 97-5412-0_22.

[25] I. W. M. A. P. I Gede Totok Suryawan, "Convolutional Neural Network for Cataract Clasification Using Primary Dataset," in *2024 9th International Conference on Business and Industrial Research (ICBIR)*, 2024, doi: 10.1109/ICBIR61386.2024.10875946.

[26] I. G. T. Suryawan Udayana, I. Putu Agus Eka Darma, "A deep learning approach for COVID-19 detection via X-ray image with image correction method," *Int. J. Eng. Emerg. Technol.*, vol. 5, no. 2, pp. 111–115, 2020, doi: 10.24843/IJEET.2020.v05.i02.p018.

[27] I. G. T. Suryawan, I. P. Agus, and E. Darma, "Optimasi Convolutional Neural Network Untuk Deteksi Covid-19 Pada X-Ray Thorax Berbasis Dropout," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 9, no. 3, 2022, doi: 10.25126/jtiik.202295143.

[28] I. K. N. P. Suryawan, I Gede Totok, Anak Agung Ngurah Mertha Jaya, da Bagus Ary Indra Iswara, I Putu Mahesa Kama Artha, "Balinese Script Handwriting Recognition Using Convolutional Neural Network," in *2024 IEEE International Symposium on Consumer Technology (ISCT)*, 2024, doi: 10.1109/ISCT62336.2024.10791286.

[29] A. A. K. O. S. I Gede Totok Suryawan, Made Sudarma, I Ketut Gede Darma Putra, "Classifying Ikat Gringsing Woven Cloth Motifs Using Convolutional Neural Network," in *2023 7th International Conference on New Media Studies (CONMEDIA)*, 2024, doi: 10.1109/CONMEDIA60526.2023.10428579.