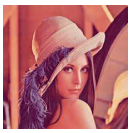
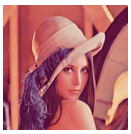
seconds. The execution time depends on the size of the image and the length of the inserted message. Then for the extracting process, the average time needed for execution is 22.07 seconds.

In theory, if the size of the Cover image is 225×225 pixels, the secret message that can be inserted into the Cover image is (225 × 225 × 3)/5 = 30375 characters. But the experiment gave poor results when the length of the secret message inserted was more than or equal to 200 characters. Table IV shows the Stego Image results that have been inserted a secret message with a length of more than or equal to 200 characters. The more messages inserted, the worse the damage that occurs in the Stego image. There is a noticeable change in the Stego image that the human senses can detect. This can evoke suspicion. For this scenario, although the Stego image can be distinguished from the Cover image, we found that the message was still successfully extracted correctly in the recovery test. This may happen because of the use of PRNG, which has a certain cycle length. A further investigation is needed to find why this phenomenon occurred, which currently cannot be covered in this paper.

TABLE IV
MESSAGE INSERTION RESULTS

Cover Image	Length of Char	Stego Image	MSE	PSNR
	200		0.009	67.320
	1.000		0.028	62.583
	6.065		0.048	60.247
	30.375		0.239	53.259

IV. CONCLUSION

This study tries to hide a text message into a color image using the steganography technique. The method used is Pixel Value Modification (PVM) which is combined with the modulo function and Pseudo-Random Number Generator. PVM successfully hides a secret message with a length of fewer than 200 characters in a 255×255 pixel color image. PVM can meet the imperceptibility, fidelity, and recovery criteria. The results of the imperceptibility test indicate that the Stego image cannot be distinguished from the Cover image. While the results of the fidelity test show that MSE value is close to zero and the PSNR value is above 40 dB. Furthermore, the recovery results are indicated by the inserted secret message that can be extracted correctly if given the correct secret key. However, when testing is done by inserting a secret message that the length is more than or equal to 200 characters in a 255×255 pixel color image, this method's imperceptibility component cannot be fulfilled.

REFERENCES

[1] O. R. Shahin, A. Ben Aissa, Y. Fouad, H. Al-Mahdi, and M. Alsmarah, "A New Method of Data Encryption based on One to One Functions," vol. 10, no. 3, pp. 1169–1175, 2020.

[2] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*. 2014.

[3] A. S. Ansari, M. S. Mohammadi, and M. T. Parvez, "A multiple-format steganography algorithm for color images," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2991130.

[4] J. R. Jayapandiyan, C. Kavitha, and K. Sakthivel, "Enhanced Least Significant Bit Replacement Algorithm in Spatial Domain of Steganography Using Character Sequence Optimization," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.3009234.

[5] K. Wang and Q. Gao, "A Coverless Plain Text Steganography Based on Character Features," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2929123.

[6] A. A. Alsabhany, F. Ridzuan, and A. H. Azni, "The Adaptive Multi-Level Phase Coding Method in Audio Steganography," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2940640.

[7] X. Yi, K. Yang, X. Zhao, Y. Wang, and H. Yu, "Ahcm: Adaptive huffman code mapping for audio steganography based on psychoacoustic model," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 8, 2019, doi: 10.1109/TIFS.2019.2895200.

[8] X. Duan *et al.*, "High-Capacity Image Steganography Based on Improved FC-DenseNet," *IEEE Access*, vol. 8, 2020, doi: 10.1109/access.2020.3024193.

[9] X. Zhang, F. Peng, and M. Long, "Robust Coverless Image Steganography Based on DCT and LDA Topic Classification," *IEEE Trans. Multimed.*, vol. 20, no. 12, 2018, doi: 10.1109/TMM.2018.2838334.

[10] O. F. AbdelWahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 3, pp. 1168–1175, 2019, doi: 10.12928/TELKOMNIKA.V17I3.12230.

[11] Z. Yahya, M. Hassan, S. Younis, and M. Shafique, "Probabilistic Analysis of Targeted Attacks Using Transform-Domain Adversarial Examples," *IEEE Access*, vol. 8, 2020, doi: 10.1109/ACCESS.2020.2974525.

[12] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *J. Syst. Softw.*, 2008, doi: 10.1016/j.jss.2007.01.049.

[13] M. Asikuzzaman and M. R. Pickering, "An Overview of Digital Video Watermarking," *IEEE Transactions on Circuits and Systems for Video Technology*. 2018, doi: 10.1109/TCSVT.2017.2712162.

[14] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, "Cryptanalytic attacks on pseudorandom number generators," 1998, doi: 10.1007/3-540-69710-1_12.

[15] M. Aljohani, I. Ahmad, M. Basheri, and M. O. Alassafi, "Performance Analysis of Cryptographic Pseudorandom Number Generators," *IEEE Access*, vol. 7, 2019, doi: 10.1109/ACCESS.2019.2907079.

[16] G. Marsaglia, "Xorshift RNGs," *J. Stat. Softw.*, 2003, doi: 10.18637/jss.v008.i14.

[17] S. Deshmukh, K. Doshi, and Y. Borse, "Securing Images Using Layered Morphing," 2018, doi: 10.1109/ICCUBEA.2018.8697888.

[18] R. Munir, "Pengantar Ilmu Kriptografi," *Penerbit Andi*, 2008, doi: 10.1017/CBO9781107415324.004.

[19] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research," *Neurocomputing*, vol. 335, 2019, doi: 10.1016/j.neucom.2018.06.075.

[20] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," *J. Syst. Eng. Electron.*, vol. 29, no. 3, 2018, doi: 10.21629/JSEE.2018.03.21.