BAB 6

6. 1 KESIMPULAN

Dari penelitian yang dilakukan dapat disimpulkan beberapa hal sebagai berikut: Pengaruh penggunaan metode least significant bit memiliki nilai baik dan dapat ditetapkan menjadi proses penyisipan yang baik. Teknik steganografi sangat efektif digunakan untuk menyembunyikan data atau informasi kedalam sebuah gambar. Kualitas gambar hasil metode lsb tidak berbeda dengan metode dwt yang menunjukan meskipun berbeda domain yaitu spatial dan domain frekuensi gambar yang disisipi tidak rusak. Dari hasil PNSR dan MSE yang dilakukan pada 3 gambar dengan format yang berbeda (jpg, bmp dan png) tidak terlihat perbedaan yang signifikan. Hampir semua relative memberikan hasil yang sama. Hal ini berarti format data pada gambar tidak mempengaruhi kualitas gambar, hasil pnsr dan msE

6. 2 Saran

Adapun saran untuk penelitian selanjutnya :

1 Jumlah karakter pesan yang diinput harus diketahui berapa banyak dengan menggunakan metode *least significant bit.*

2 Penelitian yang ada bisa dikembangkan menjadi sebuah aplikasi berbasis mobile.

3 Harus dilakukan penambahan data gambar dengan model gambar selain RGB.

REFERENSI

Afrose, S., Jahan, S., & Chowdhury, A. (2015). A hybrid SVD-DWT-DCT based method for image compression and quality measurement of the compressed image. *2nd International Conference on Electrical Engineering and Information and Communication Technology, ICEEiCT 2015*, (May), 21–23. https://doi.org/10.1109/ICEEICT.2015.7307442

Amin, M. M. (2016). Image Steganography Dengan Metode Least Significant Bit (Lsb). *CSRID (Computer Science Research and Its Development Journal)*, *6*(1), 53. https://doi.org/10.22303/csrid.6.1.2014.53-64

Anita, & Parmar, A. (2015). Image security using watermarking based on DWT-SVD and Fuzzy Logic. *2015 4th International Conference on Reliability, Infocom Technologies and Optimization: Trends and Future Directions, ICRITO 2015*. https://doi.org/10.1109/ICRITO.2015.7359302

Avinash K, G., & Madhuri S, J. (2014). An Image Steganography Algorithm with Five Pixel Pair Differencing and Gray Code Conversion. *International Journal of Image, Graphics and Signal Processing*, *6*(3), 12–20. https://doi.org/10.5815/ijigsp.2014.03.02

Baby, D., Thomas, J., Augustine, G., George, E., & Michael, N. R. (2015). A novel DWT based image securing method using steganography. *Procedia Computer Science*, *46*(Icict 2014), 612–618. https://doi.org/10.1016/j.procs.2015.02.105

Badescu, I., & Dumitrescu, C. (n.d.). Steganography in image using discrete wavelet transformation, (313), 69–72.

Bal, S. N., Nayak, M. R., & Sarkar, S. K. (2018). On the implementation of a secured watermarking mechanism based on cryptography and bit pairs matching. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2018.04.006

Basuki, B., Sukono, F., & Carnia, E. (2017). Model Optimisasi Portofolio Investasi Mean-Variance Tanpa dan Dengan Aset Bebas Risiko pada Saham Idx30. *Jurnal Matematika Integratif*, *12*(2), 107. https://doi.org/10.24198/jmi.v12.n2.11927.107-116

Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. *Pattern Recognition*. https://doi.org/10.1016/j.patcog.2003.08.007

Cho, D. X., Thuong, D. T. H., & Dung, N. K. (2019). A Method of Detecting Storage Based Network Steganography Using Machine Learning. *Procedia Computer Science*, *154*, 543–548. https://doi.org/10.1016/j.procs.2019.06.086

GAN, J., & HE, S. (2009). Face recognition based on 2DLDA and SVM. *Journal of Computer Applications*, *29*(7), 1927–1929. https://doi.org/10.3724/sp.j.1087.2009.01927

Gupta, N., & Sharma, N. (2014). Dwt and LSB based Audio Steganography. *ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology*, 428–431. https://doi.org/10.1109/ICROIT.2014.6798368

Ignatius, D. R., Setiadi, M., Santoso, H. A., Rachmawanto, E. H., & Sari, C. A. (2018). An Improved Message Capacity and Security using Divide and Modulus Function in Spatial Domain Steganography, 186–190.

Image, I. J. (2013). Genetic Algorithm Based Image Steganography for Enhancement of Concealing Capacity and Security, (June), 18–25. https://doi.org/10.5815/ijigsp.2013.07.03

Image Steganography Using Frequency Domain. (2014). *International Journal of Scientific & Technology Research*, *3*(9), 226–230.

Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, 299–326. https://doi.org/10.1016/j.neucom.2018.06.075

Karthikeyan, R., & Hegde, G. (2018). High performance VLSI architecture for 3-D DWT (discrete Wavelet Transform). *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018*, (Icisc), 892–897. https://doi.org/10.1109/ICISC.2018.8398929

Kaur, R. (2016). XOR-EDGE based Video Steganography and Testing against Chi-Square Steganalysis. *I.J. Image, Graphics and Signal Processing*, *9*(September), 31–39. https://doi.org/10.5815/ijigsp.2016.09.05

Liu, Q., Sung, A. H., Ribeiro, B., Wei, M., Chen, Z., & Xu, J. (2008). Image complexity and feature mining for steganalysis of least significant bit matching steganography. *Information Sciences*, *178*(1), 21–36. https://doi.org/10.1016/j.ins.2007.08.007

Malo, F. X. K., Santoso, A. J., & Pranowo. (2017). Mobile Base least significant bit method for steganography. *Advanced Science Letters*, *23*(3), 2223–2227. https://doi.org/10.1166/asl.2017.8773

Mostafa, H., Ali, A. F., & El Taweal, G. (2016). Hybrid Curvelet Transform and Least Significant Bit for image steganography. *2015 IEEE 7th International Conference on Intelligent Computing and Information Systems, ICICIS 2015*, 300–305. https://doi.org/10.1109/IntelCIS.2015.7397238

Mudnur, S. P., Goyal, S. R., Jariwala, K. N., Patel, W. D., & Ramani, B. (2018). for Enhancing the Robustness of the Stego Image Using Haar DWT and LSB Techniques. *2018 Conference on Information and Communication Technology (CICT)*, (2), 1–4.

Nikhil Simha, H. N., Prakash, P. M., Kashyap, S. S., & Sarkar, S. (2017). FPGA implementation of image steganography using Haar DWT and modified LSB techniques. *2016 IEEE International Conference on Advances in Computer Applications, ICACA 2016*, 26–31. https://doi.org/10.1109/ICACA.2016.7887918

Sari, W. S., Rachmawanto, E. H., Setiadi, D. R. I. M., & Sari, C. A. (2018). A Good Performance OTP Encryption Image based on DCT-DWT Steganography. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, *15*(4), 1987. https://doi.org/10.12928/telkomnika.v15i4.5883

tavoli, R., bakhshi, M., & salehian, F. (2016). A New Method for Text Hiding in the Image by Using LSB. *International Journal of Advanced Computer Science and Applications*, *7*(4), 126–132.

https://doi.org/10.14569/ijacsa.2016.070416

Thanki, R., & Borra, S. (2018). A color image steganography in hybrid FRT–DWT domain. *Journal of Information Security and Applications*, *40*, 92–102. https://doi.org/10.1016/j.jisa.2018.03.004

Utomo, T. P. (2012). Steganografi Gambar Dengan Metode Least Significant Bit Untuk Proteksi Komunikasi Pada Media Online. *UIN Sunan Gunung Djati Bandung*, 14.

Vadlamudi, L. N., Vaddella, R. P. V., & Devara, V. (2018). Robust image hashing using SIFT feature points and DWT approximation coefficients. *ICT Express*, *4*(3), 154–159. https://doi.org/10.1016/j.icte.2017.12.004

Verma, V., Poonam, & Chawla, R. (2014). An enhanced Least Significant Bit steganography method using midpoint circle approach. *International Conference on Communication and Signal Processing, ICCSP 2014 - Proceedings*, 105–108. https://doi.org/10.1109/ICCSP.2014.6949808

Xu, W. L., Chang, C. C., Chen, T. S., & Wang, L. M. (2016). An improved least-significant-bit substitution method using the modulo three strategy. *Displays*, *42*, 36–42. https://doi.org/10.1016/j.displa.2016.03.002

Yang, C., Liu, F., Luo, X., & Liu, B. (2008). Steganalysis frameworks of embedding in multiple least-significant bits. *IEEE Transactions on Information Forensics and Security*, *3*(4), 662–672. https://doi.org/10.1109/TIFS.2008.2007240