

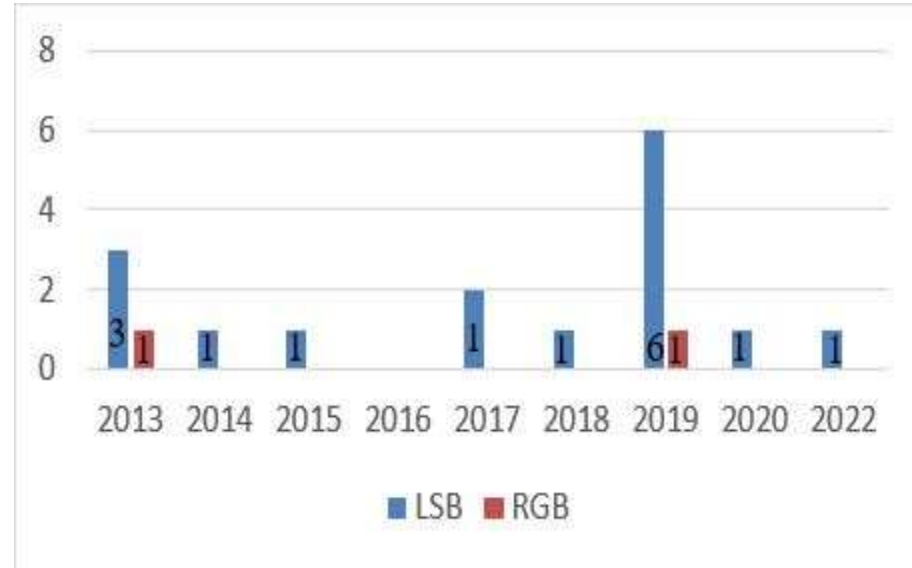
A Novel LSB Image Steganography Modification: Bit Modification on RGB Image Component

By:

Yenni Seftiardiyah, Mochamad Alfian Rosid, Sukma Aji

Faculty of Science and Technology
Universitas Muhammadiyah Sidoarjo
Indonesia

Introduction



Survey 54 jurnal tentang Steganografi gambar berfokus menggunakan metode Least Significant Bit dan RGB pada komponen gambar

Related Work and Methodology

- A. K. Sahu and G. Swain -> “A Novel n-Rightmost Bit Replacement Image Steganography Technique”
- M. M. Hashim, M. S. Mohd Rahim, and A. A. Alwan -> “A review and open issues of multifarious image steganography techniques in spatial domain”
- S. Wendzel *et al.* -> “A Revised Taxonomy of Steganography Embedding Patterns”
- 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”

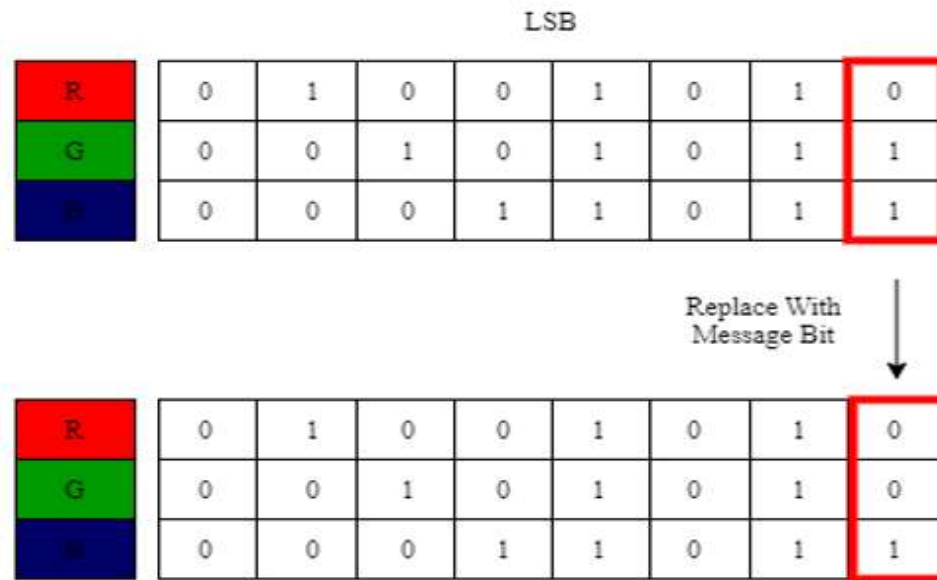
Related Work and Methodology

- X. Huan, H. Zhou, and J. Zhong -> “LSB based image steganography by using the fast marching method”
- I. Martmez, W. Fuertes, M. Palacios, D. Escudero, and T. Noboa -> “RSA Over-Encryption Employing RGB Channels through a Steganography Variant”
- S. Farrag and W. Alexan -> “Secure 2D image steganography using recamán’s sequence”
- M. Abdur, R. Ahmed, M. Adnan, and A. Ahmed -> “Digital Image Security: Fusion of Encryption, Steganography and Watermarking”

Related Work and Methodology

- M. M., A. A., and F. A. -> “An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection”
- J. Nath and A. Nath -> “Advanced Steganography Algorithm using Encrypted secret message”

Related Work and Methodology



Related Work and Methodology

Bit 7

R	0	1	0	0	1	0	1	0
G	0	0	1	0	1	0	1	1
B	0	0	0	1	1	0	1	1

Replace With
Message Bit

R	0	1	0	0	1	0	1	0
G	1	0	1	0	1	0	1	1
B	0	0	0	1	1	0	1	1

Bit 6

R	0	1	0	0	1	0	1	0
G	0	0	1	0	1	0	1	1
B	0	0	0	1	1	0	1	1

Replace With
Message Bit

R	0	0	0	0	1	0	1	0
G	0	0	1	0	1	0	1	1
B	0	1	0	1	1	0	1	1

Bit 5

R	0	1	0	0	1	0	1	0
G	0	0	1	0	1	0	1	1
B	0	0	0	1	1	0	1	1

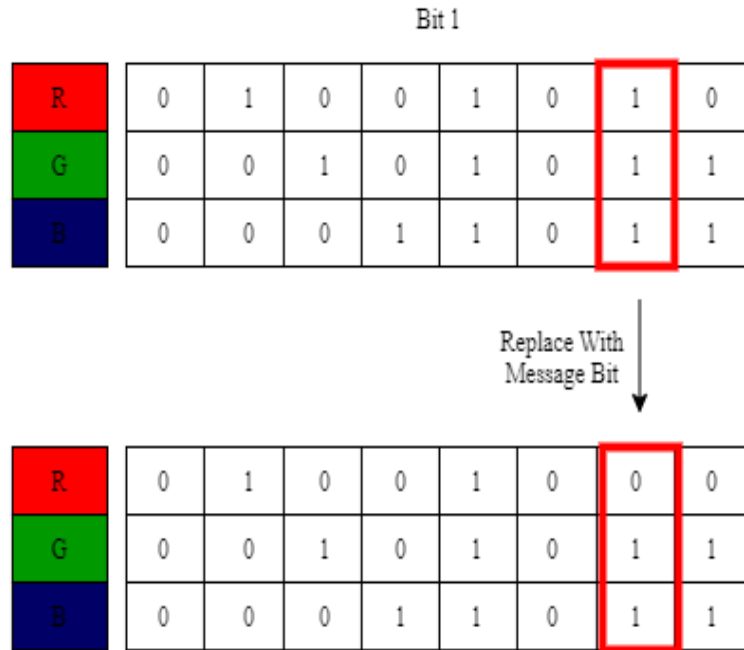
Replace With
Message Bit

R	0	1	1	0	1	0	1	0
G	0	0	1	0	1	0	1	1
B	0	0	0	1	1	0	1	1

Related Work and Methodology



Related Work and Methodology



Related Work and Methodology

Use three image samples as a carrier



baboon.png



mosque.png



plane.png

Related Work and Methodology

Mean Square Error(MSE)

Dalam pemrosesan citra digital, terutama dalam steganografi citra, MSE digunakan untuk membandingkan nilai rata-rata kesalahan kuadrat antara citra pembawa dan citra yang berisi pesan rahasia. Jika nilai MSE mendekati 0, semakin baik nilainya [31],[32].

$$MSE = \frac{1}{MN} \sum_{x=0}^M \sum_{y=1}^N [\hat{C}(x, y) - C(x, y)]^2$$

Dimana,

X dan Y = koordinat gambar

M dan N = dimensi gambar

$\hat{C}(x, y)$ = gambar mengandung pesan rahasia

C(x,y) = carrier image

Related Work and Methodology

Peak Signal Noise Ratio (PSNR)

PSNR digunakan untuk membandingkan kualitas gambar dari gambar carrier dengan gambar yang berisi pesan rahasia; semakin baik nilai PSNR yang dihasilkan, semakin baik kualitas gambar, semakin mirip gambar stego dengan gambar carrier [33].

$$PSNR = 10 \log_{10} \left(a \frac{MAXVAL^2}{MSE} \right)$$

Dimana,

PSNR= peak signal noise ratio (dB)

MAXVAL = nilai maksimal pada piksel, dimana 255 [34]

MSE = mean square error

Related Work and Methodology

Root Mean Square Error (RMSE)

RMSE merupakan akar kuadrat pengukuran dari MSE [14], yang berarti perhitungannya lebih akurat daripada MSE

$$RMSE = \sqrt{MSE}$$

Dimana,

RMSE = root mean square error

MSE = mean square error

Related Work and Methodology

Structural Similarity Index Metric (SSIM)

SSIM adalah metode perhitungan untuk membandingkan kesamaan dua gambar (Wang, 2004); dalam metode ini, degradasi gambar dapat menyebabkan perubahan persepsi. SSIM dalam metode perhitungan memiliki beberapa faktor, misalnya, masking pencahayaan, masking kontras, dan lain-lain [31]

$$SSIM = \frac{(2\mu_X\mu_Y + c_1)(2\sigma_{XY} + c_2)}{(\mu_X + \mu_Y + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)}$$

Dimana,

μ dan σ = standar deviasi gambar asli X dan gambar berisi pesan rahasia Y

XY = kovarian dari X dan Y

C_1 dan c_2 = konstanta untuk menghindari instabilitas numerik [32]

References

- [1] A. Sajid Ansari, M. Sajid Mohammadi, and M. Tanvir Parvez, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 1, pp. 11–25, 2019, doi: 10.5815/ijcnis.2019.01.02.
- [2] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Opt. Laser Technol.*, vol. 116, no. February, pp. 92–102, 2019, doi: 10.1016/j.optlastec.2019.03.005.
- [3] M. Garg, "A Novel Text Steganography Technique Based on Html Documents," *Int. J. Adv. Sci. Technol.*, vol. 35, pp. 129–138, 2011.
- [4] X. Li, W. Zhang, B. Ou, and B. Yang, "A brief review on reversible data hiding: Current techniques and future prospects," *2014 IEEE China Summit Int. Conf. Signal Inf. Process. IEEE ChinaSIP 2014 - Proc.*, pp. 426–430, 2014, doi: 10.1109/ChinaSIP.2014.6889278.
- [5] B. J. Mohd, S. Abed, B. Na'ami, and T. Hayajneh, "Hierarchical steganography using novel optimum quantization technique," *Signal, Image Video Process.*, vol. 7, no. 6, pp. 1029–1040, 2013, doi: 10.1007/s11760-012-0301-9.
- [6] M. Marsaline Beno, A. George, I. R. Valarmathi, and S. M. Swamy, "Hybrid optimization model of video steganography technique with the aid of biorthogonal wavelet transform," *J. Theor. Appl. Inf. Technol.*, vol. 63, no. 1, pp. 190–199, 2014.
- [7] P. Pathak, A. K. Chattopadhyay, and A. Nag, "A new audio steganography scheme based on location selection with enhanced security," *1st Int. Conf. Autom. Control. Energy Syst. - 2014, ACES 2014*, pp. 1–4, 2014, doi: 10.1109/ACES.2014.6807979.
- [8] M. Tayel, A. Gamal, and H. Shawky, "A proposed implementation method of an audio steganography technique," *Int. Conf. Adv. Commun. Technol. ICACT*, vol. 2016-March, no. 3, pp. 180–184, 2016, doi: 10.1109/ICACTION.2016.7423320.
- [9] A. Odeh, K. Elleithy, and M. Faezipour, "Steganography in text by using MS word symbols," *Proc. 2014 Zo. 1 Conf. Am. Soc. Eng. Educ. - "Engineering Educ. Ind. Involv. Interdiscip. Trends"*, *ASEE Zo. 1 2014*, no. April, 2014, doi: 10.1109/ASEEZone1.2014.6820635.
- [10] S. Sharma, A. Gupta, M. C. Trivedi, and V. K. Yadav, "Analysis of different text steganography techniques: A survey," *Proc. - 2016 2nd Int. Conf. Comput. Intell. Commun. Technol. CICT 2016*, pp. 130–133, 2016, doi: 10.1109/CICT.2016.34.

References

- [11] A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," *Proc. 2015 IEEE Int. Conf. Electr. Comput. Commun. Technol. ICECCT 2015*, pp. 1–4, 2015, doi: 10.1109/ICECCT.2015.7226122.
- [12] F. Akhter and M. Selim, "A New Approach of Graph Realization for Data Hiding using Human Encoding," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 12, 2016, doi: 10.14569/ijacsa.2016.071256.
- [13] T. Anwar, S. Paul, and S. K. Singh, "Message transmission based on DNA cryptography: Review," *Int. J. Bio-Science Bio-Technology*, vol. 6, no. 5, pp. 215–222, 2014, doi: 10.14257/ijbsbt.2014.6.5.22.
- [14] M. Cui and Y. Zhang, "Incorporating Randomness into DNA Steganography to Realize Secondary Secret key, Self-destruction, and Quantum Key Distribution-like Function," *bioRxiv*, p. 725499, 2019, [Online]. Available: <http://biorxiv.org/content/early/2019/08/05/725499.abstract>
- [15] S. Alam, S. M. Zakariya, and M. Q. Rafiq, "Analysis of modified lsb approaches of hiding information in digital images," *Proc. - 5th Int. Conf. Comput. Intell. Commun. Networks, CICN 2013*, pp. 280–285, 2013, doi: 10.1109/CICN.2013.66.
- [16] A. K. Sahu and G. Swain, "A Novel n-Rightmost Bit Replacement Image Steganography Technique," *3D Res.*, vol. 10, no. 1, 2019, doi: 10.1007/s13319-018-0211-x.
- [17] M. M. Hashim, M. S. Mohd Rahim, and A. A. Alwan, "A review and open issues of multifarious image steganography techniques in spatial domain," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 4, pp. 956–977, 2018.
- [18] S. Wendzel *et al.*, "A Revised Taxonomy of Steganography Embedding Patterns," *ACM Int. Conf. Proceeding Ser.*, no. Ares, 2021, doi: 10.1145/3465481.3470069.
- [19] 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.
- [20] X. Huan, H. Zhou, and J. Zhong, "LSB based image steganography by using the fast marching method," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 3, pp. 1–5, 2019, doi: 10.14569/IJACSA.2019.0100301

References

- [21] I. Martmez, W. Fuertes, M. Palacios, D. Escudero, and T. Noboa, "RSA Over-Encryption Employing RGB Channels through a Steganography Variant," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 11, no. 4, pp. 1432–1439, 2021, doi: 10.18517/ijaseit.11.4.13728.
- [22] S. Farrag and W. Alexan, "Secure 2D image steganography using recaman's sequence," *Proc. - 2019 Int. Conf. Adv. Commun. Technol. Networking, CommNet 2019*, pp. 1–6, 2019, doi: 10.1109/COMMNET.2019.8742368.
- [23] M. Abdur, R. Ahmed, M. Adnan, and A. Ahmed, "Digital Image Security: Fusion of Encryption, Steganography and Watermarking," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, pp. 224–228, 2017, doi: 10.14569/ijacsa.2017.080528.
- [24] M. M., A. A., and F. A., "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 3, pp. 361–366, 2016, doi: 10.14569/ijacsa.2016.070350.
- [25] J. Nath and A. Nath, "Advanced Steganography Algorithm using Encrypted secret message," *Int. J. Adv. Comput. Sci. Appl.*, vol. 2, no. 3, 2011, doi: 10.14569/ijacsa.2011.020304.
- [26] C. Paper and A. N. St, "Symmetric Key Cryptography Using Random Key Symmetric key cryptography using Random key generator," no. November, 2015.
- [27] A. Seif and W. Alexan, "A High Capacity Gray Code Based Security Scheme for Non-Redundant Data Embedding," *Proc. 2020 Int. Conf. Innov. Trends Commun. Comput. Eng. ITCE 2020*, no. February, pp. 130–136, 2020, doi: 10.1109/ITCE48509.2020.9047755.
- [28] N. Sakib, A. Hira, M. N. Mollah, S. M. Sharun, S. B. Mohamed, and M. A. Rashid, "SNR improvement and bandwidth optimization technique using PCM-DSSS encryption scheme," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 6, no. 5, pp. 638–643, 2016, doi: 10.18517/ijaseit.6.5.921.
- [29] D. T. Joy, G. Kaur, A. Chugh, and S. B. Bajaj, "Computer Vision for Color Detection," *Int. J. Innov. Res. Comput. Sci. Technol.*, vol. 9, no. 3, pp. 53–59, 2021, doi: 10.21276/ijircst.2021.9.3.9.
- [30] N. Phuangsaikai, J. Jakmune, and S. Kittiwachana, "Investigation into the predictive performance of colorimetric sensor strips using RGB, CMYK, HSV, and CIELAB coupled with various data preprocessing methods: a case study on an analysis of water quality parameters," *J. Anal. Sci. Technol.*, vol. 12, no. 1, 2021, doi: 10.1186/s40543-021-00271-9

References

- [31] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," *J. Comput. Commun.*, vol. 07, no. 03, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.
- [32] J. Søgaard, L. Krasula, M. Shahid, D. Temel, K. Brunnström, and M. Razaak, "Applicability of existing objective metrics of perceptual quality for adaptive video streaming," *IS T Int. Symp. Electron. Imaging Sci. Technol.*, 2016, doi: 10.2352/ISSN.2470-1173.2016.13.IQSP-206.
- [33] R. Hassan, S. Kasim, W. A. Z. W. C. Jafery, and Z. A. Shah, "Image enhancement technique at different distance for Iris recognition," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 7, no. 4–2 Special Issue, pp. 1510–1515, 2017, doi: 10.18517/ijaseit.7.4-2.3392.
- [34] B. R. Jana, H. Thotakura, A. Baliyan, M. Sankararao, R. G. Deshmukh, and S. R. Karanam, "Pixel density based trimmed median filter for removal of noise from surface image," *Appl. Nanosci.*, no. 0123456789, 2021, doi: 10.1007/s13204-021-01950-0.
- [35] M. Dalal and M. Juneja, "Steganography and Steganalysis (in digital forensics): a Cybersecurity guide," *Multimed. Tools Appl.*, vol. 80, no. 4, pp. 5723–5771, 2021, doi: 10.1007/s11042-020-09929-9.
- [36] T. Bhuiyan, A. H. Sarower, M. Rashed Karim, and M. Maruf Hassan, "An image steganography algorithm using LSB replacement through XOR substitution," *2019 Int. Conf. Inf. Commun. Technol. ICOIACT 2019*, pp. 44–49, 2019, doi: 10.1109/ICOIACT46704.2019.8938486.
- [37] Scijs, "No Title," 25 April, 2017. <https://github.com/scijs/baboon-image> (accessed Aug. 17, 2022).
- [38] Abejo, "No Title." <https://www.freeimages.com/photo/plane-1449679> (accessed Aug. 17, 2022).
- [39] Irothko, "No Title." <https://www.freeimages.com/photo/singapore-mosque-1502213> (accessed Aug. 17, 2022).
- [40] J. Peng *et al.*, "Implementation of the structural SIMilarity (SSIM) index as a quantitative evaluation tool for dose distribution error deflection," *Med. Phys.*, vol. 47, no. 4, pp. 1907–1919, 2020, doi: 10.1002/mp.14010.
- [41] Z. A. Khan, T. Hussain, A. Ullah, S. Rho, M. Lee, and S. W. Baik, "Towards efficient electricity forecasting in residential and commercial buildings: A novel hybrid CNN with a LSTM-AE based framework," *Sensors (Switzerland)*, vol. 20, no. 5, pp. 1–16, 2020, doi: 10.3390/s20051399.
- [42] Q. A. Al-Haija and A. Ishtaiwi, "Machine Learning Based Model to Identify Firewall Decisions to Improve Cyber-Defense," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 11, no. 4, pp. 1688–1695, 2021, doi: 10.18517/ijaseit.11.4.14608.

