DAFTAR PUSTAKA

[1] P. Purwoto, M. H. Prasetyo, A. Y. Sulistyawan, and K. C. S. Wibawa, "Corporate Responsibility For Personal Data Breach Cases," *International Journal of Multidisciplinary Research and Analysis*, vol. 06, no. 06, pp. 2757–2760, 2023, doi: 10.47191/ijmra/v6-i6-75.

[2] "No Title," pp. 49–56, 2021.

[3] P. S. Shukla, "Multi-Modal Biometric Authentication System Using Cnn," no. February, pp. 108–114, 2024.

[4] Q. A. Al-Haija and S. O. Al-Salameen, "Biometric Authentication System on Mobile Environment: A Review," *Computer Systems Science and Engineering*, vol. 0, no. 0, pp. 1–10, 2024, doi: 10.32604/csse.2024.050846.

[5] W. E. Al-ahmadi, A. O. Aljahdali, and F. Thabit, "A secure fingerprint hiding technique based on DNA sequence and mathematical function," pp. 1–33, 2024, doi: 10.7717/peerj-cs.1847.

[6] D. Prabhu, S. Vijay Bhanu, and S. Suthir, "Privacy preserving steganography based biometric authentication system for cloud computing environment," *Measurement: Sensors*, vol. 24, no. October, p. 100511, 2022, doi: 10.1016/j.measen.2022.100511.

[7] P. Kampanakis, E. Crocket, M. Campagna, A. Petcher, and S. Gueron, "Practical Challenges with AES-GCM and the need for a new cipher," pp. 1–12, 2024.

[8] A. A. Ahmed and N. H. M. Ali, "E-VOTING SYSTEM FINGERPRINT AUTHENTICATION , AES-GCM ENCRYPTION AND HYBRID BLIND WATERMARKING," vol. 6, no. 2, pp. 997–1018, 2025.

[9] S. K. Akshay, S. P. Vimalbhai, R. A. Rameshbhai, S. Mo, and P. V. Jadeja, "International Journal of Research Publication and Reviews Hybrid AES – RSA Encryption and Decryption for Secure Data Transmission," vol. 6, no. 10, pp. 1615–1621, 2025.

[10] H. Chi, C. Chang, and C. Lin, "Data Hiding Methods Using Voting Strategy and Mapping Table," pp. 365–377, doi: 10.53106/160792642024052503003.

[11] M. Y. Satriyawibawa, P. N. Andono, L. W. Soong, and N. P. Kiat, "LSB-2 Steganography with Brotli Compression and base64 Encoding for Improving Data Embedding Capacity," vol. 8, no. 2, pp. 877–884, 2024.

[12] M. Squared, “Analisis Perbandingan Kapasitas Penyisipan Data dan Kualitas Citra Dalam Teknik Steganografi LSB dan MSB Menggunakan Peak to Signal to Noise Ratio dan Mean Squared Error,” no. September, pp. 344–355, 2025.

[13] F. N. Hakim and M. Sholikhan, “Enhancing Data Security through Digital Image Steganography : An Implementation of the Two Least Significant Bits (2LSB) Method,” vol. 02, no. November, pp. 222–235, 2024.

[14] A. A. Permana and H. Amna, “Implementasi Steganografi File Citra Digital Menggunakan Metode Least Significant Bit,” *Jurnal Teknik*, vol. 11, no. 1, pp. 62–72, 2022, doi: 10.31000/jt.v11i1.6161.

[15] T. I. B, S. Nurmuslimah, and A. Taufiqurrahman, *Steganography on Color Images Using Least Significant Bit (LSB) Method*, vol. 1. Atlantis Press International BV. doi: 10.2991/978-94-6463-174-6.

[16] D. Budiman and S. Mubaroq, “Combination RC4 Algorithm and Base64 Encryption on The Least Significant Bit Method,” vol. 8, no. 2, pp. 103–114, 2022, doi: 10.24014/coreit.v8i2.20106.

[17] N. Alzin, Z. Mahrousa, and M. Rahhal, “AN INTEGRATED SECURITY MODEL USING AES AND RSA FOR THE CLOUD COMPUTING SYSTEM,” no. July, pp. 1781–1788, 2021.

[18] K. Lata, C. Gupta, and L. Reddy, “Results in Engineering A cryptographic framework for secure medical imaging in smart healthcare environments,” *Results in Engineering*, vol. 27, no. April, p. 106780, 2025, doi: 10.1016/j.rineng.2025.106780.

[19] A. O. Report, *Biometric vulnerabilities Ensuring future law enforcement preparedness An Observatory Report from the Europol Innovation Lab*. doi: 10.2813/8081090.

[20] W. Fisher, R. E. Craft, W. Fisher, and M. Ekstrom, “Data Confidentiality :,” no. February, 2024.

[21] M. Boryczka, “Hiding Information in Digital Images Using Ant Algorithms,” pp. 1–30, 2023.

[22] T. Radivilova, I. Dobrynin, A. Snihurov, S. Stanhei, and S. Bulba, “Image Steganography Method using LSB and AES Encryption Algorithm ⋆,” pp. 32–44, 2025.

[23] M. Caesar, G. Indrawan, I. G. Agung, G. Arya, and I. W. Supriana, “Penyisipan Pesan Tersembunyi Dalam Citra Menggunakan Metode Spread

Spectrum dan Least Significant Bit (LSB),” vol. 13, no. 3, pp. 635–646, 2025.

[24] R. D. Labati and F. Scotti, “Fingerprint,” pp. 1–6, 2021, doi: 10.1007/978-3-642-27739-9.

[25] “A PRIMER ON FOR ID”.

[26] A. Durbet and K. Thiry-atighehchi, “UntargetedNear-collision Attacks on Biometrics: Real-world Bounds and TheoreticalLimits,” vol. 1, no. 1.

[27] P. Studi *et al.*, “BERBASIS MOBILE PADA KANTOR KEPOLISIAN,” vol. 11, no. 3, 2023.

[28] M. Chiriţă, “A Note on Advanced Encryption Standard with Galois / Counter Mode Algorithm Improvements and S-Box Customization”.

[29] E. Ebrahimi, “Post-quantum Security of plain OAEP Transform”.

[30] A. Murphy and A. O. Neill, “Instantiability of Classical Random-Oracle-Model Encryption,” pp. 1–54, 2022.

[31] A. Pallakonda *et al.*, “AI-Driven Attack Detection and Cryptographic Privacy Protection for Cyber-Resilient Industrial Control Systems,” pp. 1–34, 2025.

[32] H. Kario, “Everlasting ROBOT : the Marvin Attack,” no. May, pp. 1–20, 2023.

[33] W. Li and Q. Huang, “A hybrid encryption algorithm based approach for secure privacy protection of big data in hospitals,” *Egyptian Informatics Journal*, vol. 28, no. September, p. 100569, 2024, doi: 10.1016/j.eij.2024.100569.

[34] V. Mahesh and B. Batta, “" RSA-AES Hybrid Encryption : Combining The Strengths Of Two Powerful Algorithms For Enhanced Security ",” vol. 10, no. 2, pp. 992–998, 2023.

[35] A. Encryption, “Cyber Security (CYBER);,” vol. 1, pp. 1–39, 2025.

[36] A. Nitaj, W. Susilo, and J. Tonien, “Enhanced S-boxes for the Advanced Encryption Standard with maximal periodicity and better avalanche property,” vol. 1757.

[37] D. Temoshok, J. L. Fenton, Y. Choong, N. Lefkovitz, and J. P. Richer, *NIST Special Publication Authentication and Authenticator Management NIST SP 800-63B-4 Authentication and Authenticator Management*.

[38] D. Sarah and C. Peter, “On the practical cost of Grover for AES key recovery,” pp. 1–22, 2024.

[39] C. Gidney and M. Eker, “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits,” pp. 1–31, 2021.