Implementasi Algoritma Aes Dengan Steganografi Menggunakan Metode *Spread Spectrum* Untuk Pengamanan Data Pada Citra

1st Muhammad Pamungkas Megananda
Fakultas Informatika
Universitas Telkom
Purwokerto, Indonesia
pamungkasme@students.telkomuniversity.ac.id

2nd Muhammad Fajar Sidiq
Fakultas Informatika
Universitas Telkom
Purwokerto Indonesia
mfsidiq@telkomuniversity.ac.id

3rd Arif Amrulloh
Fakultas Informatika
Universitas Telkom
Purwokerto, Indonesia
arifta@telkomuniversity.ac.id

***Abstrak* — Seiring dengan perkembangan teknologi informasi, keamanan data merupakan aspek yang sangat penting dalam era digital, Otoritas Jasa Keuangan (OJK) melaporkan dalam kurun waktu 2020 hingga 2023 terjadi lebih dari 20 kasus pencurian data. Dari banyaknya kasus, diperlukan metode pengamanan data yang efektif dengan mengombinasikan kriptografi dan steganografi. Penelitian ini bertujuan untuk menerapkan algoritma kriptografi Advanced Encryption Standard (AES) dan metode steganografi Spread Spectrum untuk mengamankan data dengan menyisipkan file berformat PDF ke dalam citra digital berformat PNG. Algoritma AES digunakan untuk mengenkripsi pesan sehingga hanya dapat diakses oleh pihak yang memiliki kunci, sementara metode steganografi Spread Spectrum digunakan untuk menyembunyikan pesan dalam citra digital tanpa mengurangi kualitas visual yang signifikan. Penelitian ini mencakup proses enkripsi isi pesan dengan AES, lalu merubah ke bentuk bit yang kemudian bit-bit di lakukan spreading pada cover objek dengan metode steganografi spread spectrum, kemudian pada proses ekstraksi file dilakukan despreading untuk mengambil bit-bit yang terdapat pada stego image dan mengembaliikannya ke bentuk file. Selanjutnya setalah pengujian, dilakukan evaluasi kualitas citra yang dihasilkan berdasarkan parameter PSNR (Peak Signal to Noise Ratio) dan MSE (Mean Squared Error). Hasil penelitian menjunjukkan bahwa metode yang digunakan mampu menyisipkan dan mengekstrak data dengan kualitas citra yang masih baik (PSNR > 40 dB) dan waktu waktu proses yang singkat. Dengan demikian, penelitian ini menunjukkan kombinasi AES dan Steganografi Spread Spectrum berhasil dalam menjaga data, terutama dalam konteks perlindungan dokumen digital rahasia.**

***Kata kunci*— Keamanan data, Kriptografi, AES, Steganografi, Spread Spectrum.**

I. PENDAHULUAN

Seiring berkembangnya teknologi informasi, kejahatan seperti pencurian data oleh pihak tidak sah juga meningkat, khususnya kejahatan siber yang kini dikenal luas. Salah satu dampaknya adalah kebocoran informasi akibat lemahnya perlindungan data pribadi, terutama di sektor perbankan, yang dimanfaatkan untuk tindakan penipuan [1]. Otoritas Jasa Keuangan (OJK) mencatat lebih dari 20 kasus kejahatan siber yang menyebabkan kebocoran data nasabah dari berbagai bank sepanjang 2020 hingga 2023, dengan kerugian finansial mencapai triliunan rupiah [2]. Oleh karena itu, keamanan data menjadi sangat penting untuk mencegah penyalahgunaan informasi, salah satunya dengan memanfaatkan kriptografi dan steganografi sebagai teknik perlindungan ganda terhadap data digital [3].

Oleh Karena itu, penelitian ini bertujuan untuk menggabungan teknik kriptografi dan steganografi untuk pengamanan data pada sarana digital, menggunakan algoritma kriptografi simetris yaitu algoritma Advanced Encryption Standart (AES) untuk enkripsi dan dekripsi informasi dan metode steganografi *spread spectrum* sebagai metode penyisipan, yang memiliki tujuan akan keberhasilan dari gabungan algoritma AES dan *spread spectrum* sebagai sarana pengamanan informasi yang diharapkan dapat memberikan kontribusi dalam memperkecil tindakan kejahatan yang menyebabkan kebocoran informasi.

II. KAJIAN TEORI

A. Penelitian terdahulu

Penelitian mengenai pengamanan data teks menggunakan metode spread sprectrum yang bertujuan untuk mengamankan data teks pada gambar digital [4]. Proses dimulai dengan mengubah nilai RGB pixel gambar dan data teks menjadi bentuk biner, kemudian dilakukan penyebaran (spreading) dari data teks pada gambar digital yang diikuti dengan pembangkitan kunci dan modulasi hasil penyebaran menggunakan kunci yang telah dibangkitkan. Hasilnya adalah stego image dengan

nilai RGB pixel yang berubah dari 0 menjadi 1, sehingga tidak mempengaruhi reproduksi warna RGB gambar.

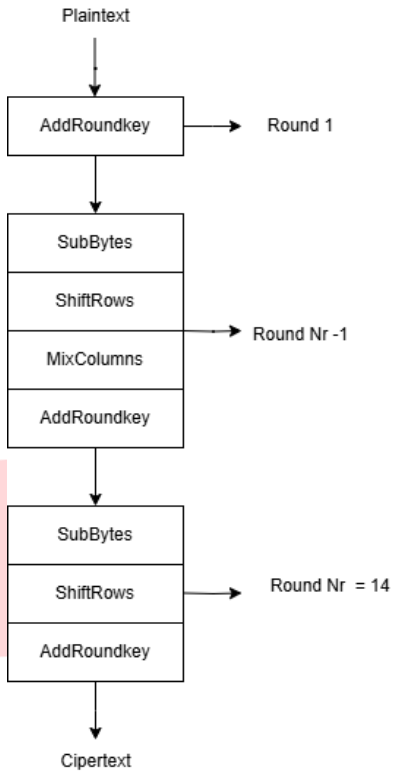
Penelitian mengenai kombinasi algoritma AES dengan steganografi LSB untuk keamanan teks rahasia [5]. Sistem yang dibangun memliki menu enkripsi dan deskripsi untuk menrubah teks rahasia menjadi ciphertext yang kemudian dilakukan penyisipan ke gambar menggunakan steganografi LSB dengan rata-rata waktu 0,019818 detik untuk enkripsi dan 0,020114 detik untuk dekripsi dengan file citra berukuran 128x128 piksel sebanyak 2 citra, 256x256 piksel sebanyak 2 dan ukuran 512 citra sebanyak 1, serta perubahan ukuran file citra dengan rata-rata 0-2KB, sehingga kualitas gambar hampir sama dengan yang asli.

B. Kriptografi

Kriptografi diartikan dari Bahasa Yunani '*crypto*' dan '*graphia*' yang berarti '*secret*' dan '*writing*' dimana jika diartikan secara umum menjadi tulisan rahasia, dimana kriptografi dibagi menjadi dua tipe yaitu simetris dan asimetris, dimana yang menjadi pembeda adalah kunci untuk enkripsi dan dekripsi, pada kriptografi simetris yang disebut sebagai algoritma klasik pada prosesnya kunci yang digunakan sama untuk melakukan enkripsi dan dekripsinya sedangkan kriptografi asimetris atau algoritma kunci publik memiliki kunci yang berbeda pada proses enkripsi dan dskripsi [6], [7].

C. Advanced Encryption Standard (AES)

Algoritma AES merupakan algoritma simetris yang mempunyai kunci yang sama pada proses enkripsi dan dekripsinya yang menggunakan kunci sepanjang 128, 192, 256 bit. Kelebihan AES berada pada kunci dimana panjang minimal 128 bit, sehingga dengan teknologi yang ada pada saat ini AES masih bisa bertahan dari serangann *exhaustive key lookup*. Panjang kunci 128 bit yang mempunyai kombinasi 2^{128} hampir tidak bisa di selesaikan dengan cara mencoba keseluruhan dari kombinasi yang ada menggunakan super komputer di era sekarang, sedangkan kekurangan AES terletak pada manajemen kuncinya yang bisa bocor dengan estimasi waktu yang panjang [8].



GAMBAR 1

Gambar 1 menunjukkan proses enkripsi AES yang terdiri dari 4 proses transformasi *AddRounkey, SubBytes, ShiftRows*, dan *MixColumns.*

D. Steganografi

Steganografi adalah cara untuk menyembunyikan informasi pada sarana penyimpan, kata '*steganos*' dan '*graphien*' diartikan dari Bahasa Yunani yang berarti '*tersembunyi*' dan '*tulisan*' dimana jika diartikan secara umum menjadi tulisan tersembunyi. Steganografi dapat diartikan sebagai ilmu mengaburkan pesan dengan maksud tidak menimbulkan kecurigaan. Pada abad ke-5 SM, steganografi di terapkan dengan cara mencukur rambut seorang budak dan memberikan tato di kepalanya, kemudian budak diberangkatkan setelah rambutnya tumbuh. Pada steganografi terdapat evaluasi performa dengan menghitung tingkat distorsi yang dihasilkan pada proses penyisipan dengan PSNR dan MSE yang dapat dihitung dengan :

$$PSNR = 20\,log_{10}\left(\frac{255}{\sqrt{MSE}}\right)$$

dimana MSE didaptkan dari :

$$MSE = \frac{1}{MNC}\sum_{x}^{M}\sum_{y}^{N}\sum_{c}^{C}[f1(x,y,c) - f2(x,y,c)]^2$$

Nilai PSNR diperngaruhi dari nilai MSE, semakin kecil nilai MSE. PSNR dapat ditulis menggunakan satuan decibel (dB). Nilai PSNR yang baik umumnya bernilai 20 dB hingga 40 dB [9], [10], [11].

E. Spread Spectrum

Spread spectrum merupakan salah satu teknik dalam penerapan steganografi dimana prosesnya dilakukan pentransmisian dengan cara *pseudonoise code* yang menyebarkan sinyal *bandwith* lebih besar dari sinyal

komunikasi informasi, dimana nantinya sinyal hendak dikumpulkan kembali sebagai kunci menggunakan tiruan yang dihasilkan dari *pseudonoise code*, *spread spectrum* juga memberlakukan setiap pixel dari *cover-object* yang berarti menggunakan seluruh pixel yang tersedia sebagai tempat beradanya informasi yang menjadikan keamanan lebih tinggi [12], [13], [14].

F. Pengamanan Data

Perkembangan teknologi yang terjadi pada saat ini menyebabkan perubahan cara dalam menjaga privasi baik itu perorangan atau organisasi. Dengan era digitalisasi, data pribadi dapat digunakan oleh pihak yang tidak sah untuk tindakan kejahatan yang merugikan pihak yang berkepentingan, dari bahaya yayng mengancam, data pribadi perlu dijaga secara benar untuk menghindari kerugian baik yang bersifat materil atau non materil [15].

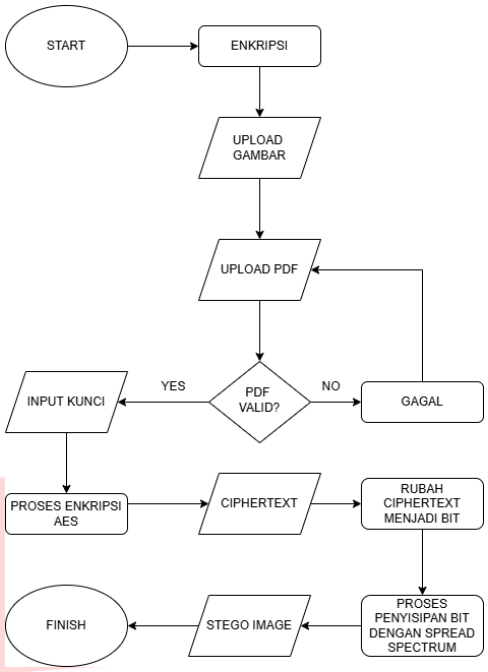
Di Indonesia yang mengatur tantang keamanan data pribadi dijelaskan pada Undang-undang (UU) Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Undang-undang berlaku untuk setiap orang, badan publik, dan organisasi internasional.

III. METODE

Sistem yang dibuat pada penelitian ini dibangun menggunakan bahasa pemrograman python yang memiliki fitur untuk upload gambar, upload file dan input kunci. Sistem ini dirancang untuk mengenkripsi isi file pdf dengan algoritma AES dan menyembunyikan isi file ke dalam gambar menggunakan steganografi *spread spectrum.* Berikut alur penelitian yang dilaksanakan meliputi :

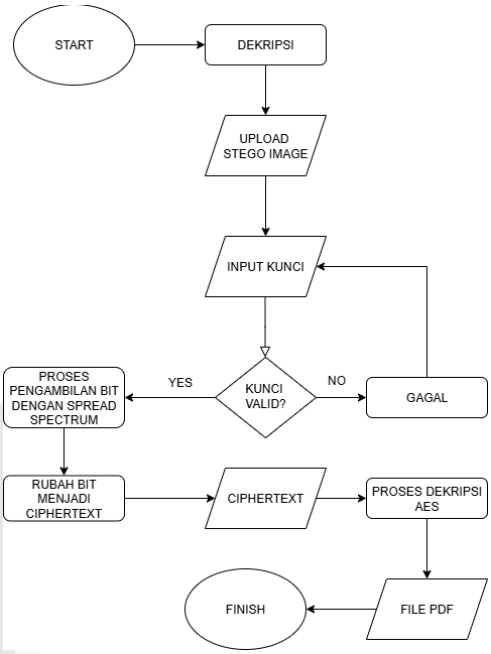
A. Perancangan Sistem

Pada tahap ini dilakukan perancangan sistem yang akan digunakan pada penelitian ini yaitu steganografi dengan algoritma AES menggunakan bahasa pemrograman python. Sistem yang dibangun memiliiki fitur enkripsi dan dskripsi.
Berikut flowcart pada sistem :



GAMBAR 2

Gambar 2 menunjukkan flowcart proses enkripsi pada penyisipan pesan menggunakan *spread spectrum*

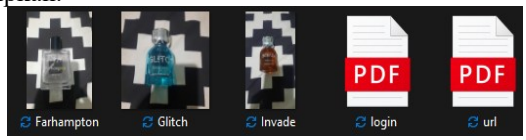


GAMBAR 3

Gambar 3 menunjukkan flowcart proses dekripsi pada pengambilan pesan menggunakan *spread spectrum*

B. Pegumpulan Data

Pengumpulan data pada penelitian ini berupa file PNG sebagai media penampung dan file pdf pesan yang di sisipkan.



GAMBAR 4

Gambar 4 menunjukkan data penelitian yang hendak digunakan pada penelitian

C. Implementasi

Pada tahap implementasi dilakukan pengujian sistem yang sebelumnya di rancang untuk menguji keberhasilan dengan cara mengenkripsi isi file pdf dan merubah betuk cipertext yang berbentuk byte menjadi bit, kemudian menyisipkan bit-bit kedalam gambar menggunakan *spread spectrum* dan menghitung kualitas visual yang terjadi saat proses penyisipan.

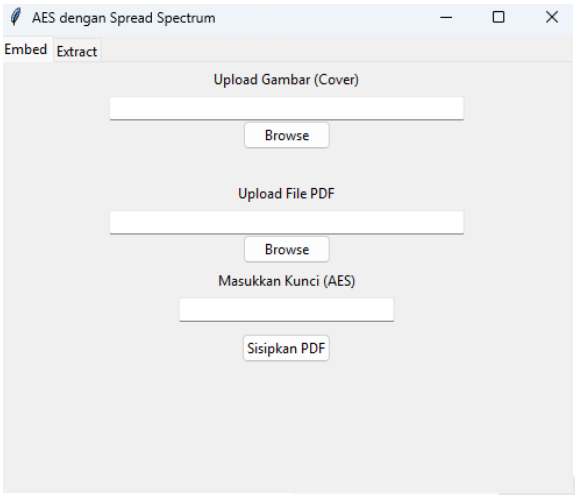
D. Hasil dan Pembahasan

Pada tahap ini dilakukan pembahasan dari pengujian yang telah dilakukan dan menyimpulkan hasil penelitan mengenai keberhasilan dari kombinasi algoritma AES dengan steganografi *spread spectruum* dalam keamanan pesan rahasia, serta melakukan analisis perbedaan pada kualitas gambar.

IV. HASIL DAN PEMBAHASAN

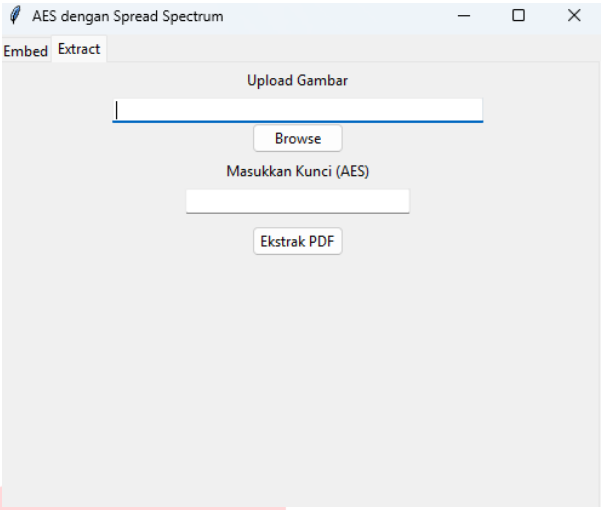
Pada bagian ini menampilkan sistem yang telah dibangun dan melakukan pembahasan dari proses pengujian, seperti :

A. Hasil Akhir Sistem



GAMBAR 5

Gambar 5 menunjukkan halaman untuk penyisipan dengan mengupload gambar sebagai cover, file pdf sebagai pesan yang disisipkan dan input kunci



GAMBAR 6

Gambar 6 menunjukkan halaman ekstraksi dengan upload *stego image* dan input kunci untuk mendapatkan file pdf yang sebelumnya disisipkan.

B. Pengujian

Pengujian dilakukan dengan menyisipkan 2 file pdf pada tiap gambar dengan kunci yang berbeda, berikut table pengujian :

TABEL 1

No	Cover	Resolusi	Size (Kb)	Size pdf (Kb)	Keterangan
1	Farhampton.png	3000x4000	3060	1	Berhasil
				1,3	
2	Glitch.png	2992x2992	2430	1	Berhasil
				1,3	
2	Invade.png	2250x4000	1890	1	Berhasil
				1,3	

Pengujian menunjukkan keberhasilan pada proses penyisipan dan ekstraksi.

C. Hasil pengujian

Setelah proses pengujian terdapat penuruan kualitas gambar yang disebabkan oleh distorsi saat proses penyisipan, berikut tabel hasil pengujian :

TABEL 2

No	Cover	File	Kunci	MSE	PSNR
1	Farhampton.png	login.pdf	admin123	2.94	43.45 dB
		url.pdf	rahasia2	3.12	43.19 dB
2	Glitch.png	login.pdf	admin123	3.94	42.18 dB
		url.pdf	rahasia2	4.18	41.92 dB
2	Invade.png	login.pdf	admin123	3.92	42.20 dB
		url.pdf	rahasia2	4.16	41.94 dB

Hasil menunjukkan kualitas gambar masih tergolong baik dengan nilai PSNR>40 dB yang menunjukkan tingkat distorsi yang rendah dan kunci mempengaruhi pada nilai PSNR dengan menunjuukan kunci admin123 mendapat nilai PSNR lebih tinggi.

Dari penjelasan di atas dapat disimpulkan bahwa cover farhampthon.png memiliki kualitas paling baik dengan nilai PSNR tertinggi dan MSE terendah dibandingkan dengan cover Invade.png dan Glitch.png.

V. KESIMPULAN

Berdasarkan hasil pengujian penerapan Algoritma AES dan steganografi *spread spectrum* yang sudah di lakukan dapat disimpulkan bahwa seluruh proses pengujian pada citra berformat *PNG sebagai penampung pesan dan file *PDF sebagai pesan tersembunyi berhasil dan berjalan dengan baik.

Data dari pesan asli yang di enkripsi dengan algoritma AES serta input kunci dirubah dari ciphertext berbentuk byte menjadi bit-bit dan menyebarkan pada pada piksel gambar denagn *spread spectrum* yang membentuk *stego image* dan mengambil bit-bit yang tersebar pada *stego image* untuk dirubah menjadi ciphertext yang berbentuk byte dan di dekripsikan kembali dengan algoritma AES menjadi pesan asli degan kunci yang sama. Nilai kualitas pada citra menunjukkan nilai PSNR > 40 dB yang membuktikan kualitas masih terjaga sehingga kombinasi Algoritma AES dan steganografi *spread spectrum* dapat di gunakan sebagai sarana pengamanan data pada file ke dalam gambar agar tetap terjaga kerahasiaannya.

REFERENSI

[1] Y. Otniel Purba and A. Mauluddin, "Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online," *JCIC J. CIC Lemb. Ris. Dan Konsult. Sos.*, vol. 5, no. 2, pp. 55–66, Sep. 2023, doi: 10.51486/jbo.v5i2.113.

[2] S. W. Annafa, "Tanggung Jawab Hukum Bank dalam Kasus Kebocoran Data Nasabah," *Kampus Akad. Publising*, vol. 1, no. 6, pp. 129–135, 2024, doi: https://doi.org/10.61722/jmia.v1i6.2885.

[3] R. Humayrah, A. M. Elhanafi, and M. T. Batubara, "Analisa Histogram dan PSNR Pada Citra True Color Dalam Pengamanan Teks Menggunakan Spread Spectrum dan LSB," *Unity Acad.*, vol. 2, no. 1, pp. 188–200, 2023, doi: https://doi.org/10.70340/jirsi.v4i2.

[4] Y. R. Nasution, M. Furqan, and M. Sinaga, "Implementasi Steganografi Menggunakan Metode Spread Spectrum Dalam Pengamanan Data Teks Pada Citra Digital," *J-Sakti*, vol. 4, no. 2, pp. 351–358, 2020, doi: https://tunasbangsa.ac.id/ejurnal/index.php/jsakti.

[5] Chaerul Umam, Muslih Muslih, and Daffa Fadillah, "Kombinasi Steganografi LSB dan Kriptografi AES dalam Sekuriti Teks Rahasia Pada Citra Berwarna," *Semin. Nas. Teknol. Dan Multidisiplin Ilmu SEMNASTEKMU*, vol. 2, no. 1, pp. 109–118, Dec. 2022, doi: 10.51903/semnastekmu.v2i1.160.

[6] A. Hafiz, "Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB)," *Core*, vol. 17, pp. 194–198, 2019, doi: oai:ojs2.jurnal.dcc.ac.id:article/201.

[7] A. A. Permana and H. Amna, "Implementasi Steganografi File Citra Digital Menggunakan Metode Least Significant Bit," *J. Tek.*, vol. 11, no. 1, Jun. 2022, doi: 10.31000/jt.v11i1.6161.

[8] I. M. Yusup, C. Carudin, and I. Purnamasari, "Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen," *J. Tek. Inform. Dan Sist. Inf.*, vol. 6, no. 3, Dec. 2020, doi: 10.28932/jutisi.v6i3.2817.

[9] K. Aviantoro and Y. Darnita, "Implementasi Wiener, Contrast Stretching, Sharpening Filtrer Pada Citra Semangka Menggunakan MSE,RMSE, DAN PSNR," *Djtechno J. Teknol. Inf.*, vol. 5, no. 2, pp. 195–205, Aug. 2024, doi: 10.46576/djtechno.v5i2.4613.

[10] M. V. M. Bere, P. A. Nani, S. D. B. Mau, Y. C. H. Siki, and Y. P. Bria, "Pengukuran Perubahan Kualitas Warna Kain Tenun Malaka Berdasarkan Perbandingan Nilai RGB, MSE dan PSNR," *KONSTELASI Konvergensi Teknol. Dan Sist. Inf.*, vol. 4, no. 1, pp. 184–195, Jun. 2024, doi: 10.24002/konstelasi.v4i1.9215.

[11] Mahmoud Hassaballah, Ed., *Digital Media Steganography: Principles, Algorithms, and Advances*. 125 London Wall, London EC2Y 5AS, United Kingdom: Academic Press (an imprint of Elsevier), 2020.

[12] F. S. Imami, "Digital Signature Menggunakan Metode Spread Spectrum Sebagai Perlindungan Hak Cipta Pada Citra Digital MPEG-4," *Jatikom*, vol. 3, no. 1, pp. 35–41, 2020, doi: https://ejournal.upi.edu/index.php/JATIKOM.

[13] R. A. Fauzan, S. Saidah, B. Hidayat, and N. K. C. Pratiwi, "Dual Steganography in Digital Images with Spread Spectrum Insertion Method," *J. Meas. Electron. Commun. Syst.*, vol. 05, pp. 07–14, 2019, doi: 10.25124/jmecs.v5i1.2073.

[14] Abid Yahya, *Steganography Techniques for Digital Images*. Gewerbestrasse 11, 6330 Cham, Switzerland: Springer International Publishing AG, 2019.

[15] C. Vania, M. Markoni, H. Saragih, and J. Widarto, "Tinjauan Yuridis terhadap Perlindungan Data Pribadi dari Aspek Pengamanan Data dan Keamanan Siber," *J. Multidisiplin Indones.*, vol. 2, no. 3, pp. 654–666, Mar. 2023, doi: 10.58344/jmi.v2i3.157.