BAB II

TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Berikut beberapa penelitian terdahulu yang berkaitan dengan penelitian ini.

Tabel 2.1 Penelitian Terdahulu

Topik	Metode	Hasil	Referensi
Keamanan Data	Modifikasi Algoritma *Advanced Encryption Standard* (AES)	Algoritma AES yang dimodifikasi memengaruhi waktu yang dibutuhkan *cryptanalyst* untuk memecahkan kunci enkripsi, sehingga memberikan tingkat keamanan yang lebih tinggi.	[1]
Kerahasiaan Data Teks	Kriptografi *Reverse Cipher* dikombinasikan dengan metode RSA	Aplikasi keamanan data teks yang memungkinkan pengguna mengenkripsi data teks menggunakan metode *Reverse Cipher* kemudian mengenkripsi ulang menggunakan metode RSA dan mendekripsi data teks terenkripsi.	[2]
Keamanan Informasi	Algoritma *discrete wavelet transform* (DWT), algoritma *advanced encryption*	Hasil riset menunjukkan bahwa sistem yang diajukan dapat meningkatkan kualitas *stego-image* (PSNR mencapai 47,8 dB) dan indeks kemiripan struktural (SSIM mencapai 0,92). Selain itu, eksperimen membuktikan	[3]

	standard (AES) dan *teknik least significant bit* (LSB)	bahwa kombinasi teknik tersebut dapat mempertahankan kualitas *stego-image* hingga 68%, meningkatkan kinerja sistem hingga 44%, dan meningkatkan ukuran data rahasia dibandingkan dengan penggunaan teknik secara terpisah.	
Keamanan Pesan	Algoritma *Vigenere Cipher* dan metode *Least Significant Bit* (LSB)	Dalam penelitian ini, ditemukan bahwa gambar yang telah dienkripsi akan berubah menjadi abu-abu atau dalam bentuk citra *grayscale*. Hal ini membuat pesan yang tersembunyi menjadi lebih sulit ditemukan oleh penyerang.	[4]
Keamanan Pesan	Metode *hybrid hill cipher* dan kriptografi RSA	Telah dibuktikan bahwa enkripsi *hybrid hill cipher* dengan kunci matriks 3x3 dan RSA dengan kunci 512-*bit* dapat mengatasi masalah keamanan pertukaran data, sehingga orang yang tidak berhak tidak dapat membaca pesan yang dikirim.	[5]
Keamanan Data	Metode *Multiple Rounds Variable*	Skema MRVB yang diusulkan dibandingkan dengan enkripsi data DES dan AES standar, hasilnya menunjukkan bahwa	[6]

	Block (MRVB), algoritma DES dan AES	MRVB memberikan akselerasi dan peningkatan *throughput* yang signifikan dari proses data kriptografi.	
Keamanan Data	Algoritma RSA	Sebagai hasilnya, penelitian ini akan membantu para peneliti dan praktisi memahami kriptografi RSA masa lalu dan sekarang dan potensi aplikasinya di bidang lain.	[7]
Keamanan Data	Metode *Least Significant Bit* (LSB)	Tujuan yang diharapkan termasuk menggunakan *Python* untuk membuat perangkat lunak steganografi pada gambar digital dari *file* gambar PNG, menyembunyikan keberadaan pesan atau informasi tersembunyi, dan memastikan bahwa gambar digital dan kualitas *file* gambar asli adalah sama tidak bervariasi secara signifikan.	[8]
Keamanan Data	Steganografi citra *Least Significant Bit* (LSB), *Most Significant Bit*	Teknik LSB memberikan nilai PSNR dan SSIM yang lebih tinggi daripada teknik MSB dan PVD dan mencapai MSE yang lebih rendah daripada dua teknik lainnya.	[9]

	(MSB) dan *Pixel Value Differencing* (PVD)		
Kemananan Izin Mendirikan Bangunan (IMB)	Algoritma RSA	RSA memiliki proses enkripsi dan dekripsi berdasarkan konsep bilangan prima dan aritmatika modulo. Baik kunci dekripsi dan kunci enkripsi adalah bilangan bulat. Kunci enkripsi tidak dirahasiakan dan dipublikasikan, sehingga kunci enkripsi juga dikenal sebagai kunci publik, tetapi kunci dekripsi bersifat rahasia.	[10]
Keamanan *digital signature*	Algoritma *Secure Hash Algorithm* (SHA)	Sistem yang diciptakan ini bertujuan untuk mengatasi permasalahan dan hambatan yang selama ini masih dihadapi oleh para dosen pengusul proposal Hibah Dikti, terutama saat proses verifikasi dokumen yang masih dilakukan secara manual.	[11]
Keamanan Pesan	Algoritma *AES–256*, *Blowfish*, dan teknik substitusi LSB	Kinerja skema yang diusulkan dievaluasi dalam hal pengujian pendengaran, waktu eksekusi, kemampuan menyisipkan, plot bentuk gelombang, serta sejumlah besar ukuran statistik, domain	[12]

		waktu dan frekuensi domain. Selain itu, perbandingan antara skema yang diusulkan menggunakan AES-256 dan rekanan yang terdokumentasi juga disediakan. Hasil numerik menunjukkan bahwa skema yang diusulkan memiliki kinerja yang sangat baik.	
Keamanan Data	Algoritma *Rivest Code 4 (RC4)*	Hasil yang diperoleh dari penelitian ini adalah aplikasi kriptografi dokumen dapat mengenkripsi dan mendekripsi dokumen menggunakan algoritma *Rivest Code 4* (RC 4).	[13]
Penyembunyian Data	Metode steganografi berbasis LSB menjadi dua kategori: LSBR (penggantian LSB) dan LSBM (pencocokan LSB)	Pengujian kami menggunakan steganalisis menunjukkan bahwa penerapan metode kami menghasilkan tingkat kesalahan deteksi sekitar 10% lebih tinggi daripada menggunakan dua metode steganografi.	[14]
Keamanan Data	Algoritma RSA dan AES	Hasil penelitian menyimpulkan bahwa penggunaan algoritma enkripsi AES lebih efisien	[15]

		daripada enkripsi RSA dalam melindungi data digital. Hal ini dikarenakan proses enkripsi dan dekripsi dengan menggunakan algoritma AES lebih cepat, meskipun perbedaan waktu pengujian kedua algoritma enkripsi tidak begitu penting.	

Berikut *critical riview* penelitian terdahulu yang berkaitan dengan penelitian ini

Tabel 2.2 *Critical Riview* Jurnal 1

Judul	Implementasi Kriptografi dengan Modifikasi Algoritma *Advanced Encryption Standard* (AES) untuk Pengamanan *File Document*
Nama jurnal, Volume, Nomor, Tahun	JINACS: Volume 01 Nomor 01, 2019
Penulis	Lilik Asih Indrayani, I Made Suartana
Metode/Algoritma	Modifikasi Algoritma *Advanced Encryption Standard* (AES)
Hasil	Hasil pengujian menunjukkan bahwa semakin besar putaran dan panjang kunci maka waktu yang dibutuhkan proses enkripsi dan dekripsi semakin lama.
Kekuatan Penelitian	Tampilan aplikasi yang sederhana, sehinga mudah untuk menggunakan enkripsi dan dekripsi. Karena menggunakan algoritma AES yang dimodifikasi dan memberikan tingkat keamanan yang lebih tinggi karena proses enkripsi dan dekripsi

	memakan waktu lebih lama daripada algoritma AES standar.
Kelemahan Penelitian	Proses enkripsi dan dekripsi menggunakan algoritma AES yang dimodifikasi membutuhkan waktu yang lebih lama dibandingkan dengan algoritma AES standar
Kesimpulan	Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa perubahan algoritma AES pada proses enkripsi dan dekripsi *file* dokumen dengan menambah jumlah putaran dan panjang kunci akan mempengaruhi durasi proses enkripsi dan dekripsi. Semakin besar putaran dan semakin panjang kuncinya, semakin lama pula proses enkripsi dan dekripsinya. Selain itu, hasil pengujian berdasarkan perbandingan waktu komputasi algoritma AES standar dan algoritma AES modifikasi menunjukkan bahwa algoritma AES modifikasi memiliki nilai waktu yang lebih tinggi daripada algoritma AES standar, sehingga dapat dikatakan bahwa algoritma AES modifikasi Algoritma AES menunjukkan tingkat keamanan yang lebih tinggi karena memengaruhi waktu yang dibutuhkan *cryptanalyst* untuk meretas sistem

Tabel 2.3 *Critical Riview* Jurnal 2

Judul	Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode *Reverse Chiper* Dan RSA Berbasis Android
Nama jurnal, Volume, Nomor, Tahun	Jurnal Teknik Informatika Kaputama (JTIK) Vol. 3 , No. 2, Juli 2019

Penulis	Yusfrizal
Metode/Algoritma	Kriptografi *Reverse Cipher* dikombinasikan dengan metode RSA
Hasil	Hasil dari penelitian ini adalah terciptanya aplikasi keamanan data teks yang memungkinkan pengguna untuk mengenkripsi data teks menggunakan metode *reverse cipher* kemudian mengenkripsi ulang menggunakan metode RSA dan mendekripsi data dari *ciphertext*.
Kekuatan Penelitian	1. Tampilan sederhana yang memudahkan enkripsi dan dekripsi. 2. Memerlukan sedikit spesifikasi hardware dan software. 3. Instal file dengan mudah di ponsel Android
Kelemahan Penelitian	1. Aplikasi ini hanya dapat bekerja pada sistem operasi Android. 2. Hanya dapat dijalankan dalam mode *standalone*, bukan sebagai aplikasi sistem jaringan
Kesimpulan	1. Teks dilindungi menggunakan kombinasi metode *Reverse Cipher* dan enkripsi RSA 2. Proses enkripsi diawali dengan mengenkripsi plainteks menggunakan *Reverse Cipher* kemudian mengenkripsi ulang menggunakan RSA sehingga menghasilkan *cipherteks* 3. Proses dekripsi dimulai dengan mendekripsi *ciphertext* RSA, kemudian mendekripsi lagi dengan *Reverse Cipher* dan menghasilkan *plaintext* 4. Aplikasi ini mengenkripsi dan mendekripsi teks saja

Tabel 2.4 *Critical Riview* Jurnal 3

Judul	*Hybrid information security system via combination of compression, cryptography, and image steganography*
Nama jurnal, Volume, Nomor, Tahun	*International Journal of Electrical and Computer Engineering* (IJECE) Vol. 12, No. 6, *December* 2022, pp. 6574~6584
Penulis	Wid Akeel Awadh, Ali Salah Alasady, Alaa Khalaf Hamoud
Metode/Algoritma	Algoritma *Discrete Wavelet Transform* (DWT), algoritma *Advanced Encryption Standard* (AES) dan teknik *Least Significant Bit* (LSB)
Hasil	Hasil penelitian menunjukkan bahwa sistem yang diusulkan mampu mengoptimalkan kualitas citra *stego* (nilai PSNR 47,8 dB) dan indeks kesamaan struktural (nilai SSIM 0,92). Selain itu, hasil pengujian menunjukkan bahwa kombinasi teknik mempertahankan kualitas gambar *stego* sebesar 68%, meningkatkan kinerja sistem sebesar 44%, dan meningkatkan ukuran data rahasia dibandingkan dengan hanya menggunakan masing-masing teknik.
Kekuatan Penelitian	Kombinasi prosedur kompresi, enkripsi, dan metode penyimpanan data dapat meningkatkan kinerja dan keamanan sistem lebih dari sekadar menjalankan algoritma secara mandiri.
Kelemahan Penelitian	Jika hanya menjalankan salah satu algoritma, hasil yang didapat kurang maksimal
Kesimpulan	Artikel ini memperkenalkan skema keamanan hibrid untuk menyembunyikan data gambar rahasia di *file* gambar lain, dengan asumsi keamanan dan kapasitas tinggi. Berdasarkan hasil

	eksperimen, kualitas gambar *Stego* secara konsisten baik dengan rata-rata PSNR 47,8 dB dan rata-rata SSIM 0,92. Hasil dari metode yang diusulkan juga menunjukkan bahwa kombinasi teknik meningkatkan keamanan data dan kinerja sistem karena memiliki tingkat keamanan *hybrid*.

Tabel 2.5 *Critical Riview* Jurnal 4

Judul	Implementasi Steganografi Pada Citra Digital Dengan Modifikasi Algoritma *Vigenere Cipher* dan *Metode Least Significant Bit* (LSB)
Nama jurnal, Volume, Nomor, Tahun	Jurnal Teknik Informatika (JUTIF) Vol. 4, No. 2, April 2023, hlm. 333-344
Penulis	Gilang Miftakhul Fahmi, Khairunnisak Nur Isnaini, Didit Suhartono
Metode/Algoritma	Algoritma *Vigenere Cipher* dan metode *Least Significant Bit* (LSB)
Hasil	Hasil penelitian menunjukkan bahwa gambar terenkripsi berubah menjadi abu-abu atau memiliki gambar *grayscale*, sehingga semakin sulit bagi penyerang untuk menemukan pesan tersembunyi.
Kekuatan Penelitian	Dengan mengkombinasikan kriptografi Algoritma *Vigenere Cipher* dan metode *Least Significant Bit* (LSB), menghasilkan keamanan ganda pada *file*
Kelemahan Penelitian	Pada hasil *stego image* warna citra mengalami penurunan yang cukup signifikan karena warnanya berubah menjadi abu-abu
Kesimpulan	Aplikasi penyembunyian ini telah berhasil diimplementasikan sesuai dengan kebutuhan dan tujuan penyembunyian informasi dalam gambar untuk keamanan informasi. Kedua, memodifikasi

	algoritma enkripsi *Vigenere* dengan mengubah huruf abjad menjadi huruf *Hijaiyah* meningkatkan keamanan pesan tersembunyi, seperti yang ditunjukkan oleh hasil enkripsi. Selain itu, gambar *stego* skala abu-abu yang dihasilkan dapat menutupi pesan sehingga isinya tidak mudah ditemukan. Isi pesan disamarkan dan dapat ditampilkan kembali sehingga memenuhi kriteria pengambilan yaitu pesan terenkripsi dapat dibaca kembali

Tabel 2.6 *Critical Riview* Jurnal 5

Judul	*Message Security Using a Combination of Hill Cipher and RSA Algorithms*
Nama jurnal, Volume, Nomor, Tahun	Jurnal Matematika Dan Ilmu Pengetahuan Alam LLDikti Wilayah 1 (JUMPA), 1 (1) (2021) 20-28
Penulis	Yogi Suryo Santoso
Metode/Algoritma	Metode *hybrid hill cipher* dan kriptografi RSA
Hasil	Enkripsi *hybrid Hill* dengan kunci matriks 3x3 dan kunci RSA 512-*bit* telah terbukti mengatasi masalah keamanan dalam pertukaran data dan membuat pesan yang dikirimkan tidak dapat dibaca oleh orang yang tidak berhak.
Kekuatan Penelitian	Dengan menggabungkan kriptografi *hybrid hill cipher* dan RSA, menghasilkan keamanan pada pesan
Kelemahan Penelitian	Pesan terenkripsi tidak memiliki sarana penyembunyian, yang menimbulkan kecurigaan di kalangan pengamat

Kesimpulan	1. Algoritma *Hill* dan RSA dapat digabungkan untuk proses keamanan pesan sehingga proses pertukaran data dapat dilakukan dengan aman. 2. Proses pertukaran pesan memakan waktu lebih lama dengan penerapan kombinasi algoritma *Hill* dan RSA yang aman. 3. Panjang pesan mempengaruhi berapa lama proses enkripsi dan dekripsi pesan berlangsung. 4. Pesan yang sama yang dienkripsi dengan algoritma RSA akan memiliki *cipher* yang sama

Tabel 2.7 *Critical Riview* Jurnal 6

Judul	*Improving the Efficiency and Scalability of Standard Methods for Data Cryptography*
Nama jurnal, Volume, Nomor, Tahun	*IJCSNS International Journal of Computer Science and Network Security*, VOL.21 No.12, *December* 2021
Penulis	Mua'ad M. Abu-Faraj, Ziad A. Alqadi
Metode/Algoritma	Metode Multiple Rounds Variable Block (MRVB), algoritma DES dan AES
Hasil	Metode MRVB yang diusulkan dibandingkan dengan *cipher* data DES dan AES standar, hasilnya menunjukkan bahwa MRVB memberikan akselerasi dan peningkatan *throughput* yang signifikan dari proses data kriptografi.
Kekuatan Penelitian	Dapat membandingkan metode MRVB dengan standar enkripsi data DES dan AES
Kelemahan Penelitian	Karena metode baru digunakan dalam penelitian, diperlukan pemahaman yang lebih baik tentang metode ini

Kesimpulan	MRVB yang efisien dan sangat aman telah diusulkan. Metode yang diusulkan diimplementasikan menggunakan banyak pesan dan menawarkan parameter kualitas yang sangat baik (MSE dan PSNR) selama fase enkripsi dan dekripsi. Metode MRVB yang diusulkan menggunakan gambar warna rahasia untuk menghasilkan banyak PK yang menyertakan kunci dan putaran kerja. Jumlah putaran yang dilakukan dapat dikontrol oleh pengguna berdasarkan satu putaran. PK merupakan kombinasi kompleks dari WK dan RK. Jumlah dan konten dari kunci ini bergantung pada rahasia *image_key* yang digunakan dan ukuran blok data yang dipilih, membuat peretasan menjadi tidak mungkin.

Tabel 2.8 *Critical Riview* Jurnal 7

Judul	*Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes: Past and Present Status*
Nama jurnal, Volume, Nomor, Tahun	10.1109/ACCESS.2021.3129224 VOLUME 9, 2021
Penulis	Raza Imam, Qazi Mohammad Areeb, Abdulrahman Alturki, And Faisal Anwer
Metode/Algoritma	Algoritma RSA
Hasil	Sebagai hasilnya, penelitian ini akan membantu para peneliti dan praktisi memahami keadaan kriptografi RSA dulu dan sekarang dan potensi penerapannya di bidang lain.

Kekuatan Penelitian	Artikel ini menyajikan studi sistematis dan mendalam tentang kriptografi berbasis RSA, yang mencakup beberapa bidang
Kelemahan Penelitian	Karena studi ini mencakup kriptografi RSA secara sistematis dan terperinci, diperlukan pemahaman yang lebih dalam tentang pembahasan yang dijelaskan.
Kesimpulan	Penelitian kami memeriksa dan merekomendasikan sejumlah jalan baru yang sangat penting untuk menetapkan praktik terbaik dalam penelitian RSA untuk perubahan dan peningkatan algoritma RSA. Sebagai studi pertama dari jenisnya, studi ini juga memberikan panduan bagi para profesional dan peneliti keamanan RSA.

Tabel 2.9 *Critical Riview* Jurnal 8

Judul	Implementasi Steganografi File Citra Digital Menggunakan Metode *Least Significant Bit*
Nama jurnal, Volume, Nomor, Tahun	JT : Jurnal Teknik, Vol. 11 No. 01 Th. 2022
Penulis	Angga Aditya Permana, Habib Amna
Metode/Algoritma	Metode *Least Significant Bit* (LSB)
Hasil	Tujuan yang diharapkan termasuk membuat perangkat lunak untuk steganografi pada gambar digital *file* gambar PNG menggunakan *Python* dan menutupi keberadaan pesan atau informasi tersembunyi, dan membuat *file* gambar yang kualitasnya tidak jauh berbeda dengan gambar digital dibandingkan dengan *file* gambar asli yang berbeda.

Kekuatan Penelitian	Dengan menggunakan metode *least significant bit* (LSB), kualitas yang dihasilkan tidak jauh berbeda dengan citra digital dari *file* citra aslinya
Kelemahan Penelitian	Karena hanya metode *least significant bit* (LSB) yang digunakan, pesan tersembunyi dapat dibaca saat terdeteksi. Ini karena pesan tersebut sebelumnya tidak dienkripsi
Kesimpulan	Metode *least significant bit* (LSB) memungkinkan pembuatan aplikasi steganografi dengan mengganti 8, 16, dan 24 *bit* dalam representasi *biner* dari *file* gambar BMP 24 *bit* dengan representasi *biner* dari pesan rahasia yang disembunyikan. Performa yang ditangkap tidak melibatkan penskalaan *file* gambar, dan tidak mudah bagi mata manusia untuk mengenali dan membedakan *file* gambar asli dan *file* gambar yang disisipkan dengan pesan rahasia.

Tabel 2.10 *Critical Riview* Jurnal 9

Judul	*A Comparative Analysis of LSB, MSB and PVD Based Image Steganography*
Nama jurnal, Volume, Nomor, Tahun	*International Journal of Research and Review*, Vol.8; Issue: 9; September 2021
Penulis	Alade Oluwaseun. Modupe, Amusan Elizabeth Adedoyin, Adedeji Oluyinka Titilayo, Fenwa Olusayo Deborah
Metode/Algoritma	Steganografi citra *Least Significant Bit* (LSB), *Most Significant Bit* (MSB) dan *Pixel Value Differencing* (PVD)

Hasil	LSB menawarkan PSNR dan SSIM yang lebih tinggi daripada MSB dan PVD dengan MSE yang lebih rendah daripada dua teknik lainnya
Kekuatan Penelitian	Dapat mengetahui perbandingan steganografi citra *Least Significant Bit* (LSB), *Most Significant Bit* (MSB) dan *Pixel Value Differencing* (PVD) pada citra *grayscale* dan citra berwarna.
Kelemahan Penelitian	Tidak adanya tampilan aplikasi sehingga dalam pemahaman kurang maksimal
Kesimpulan	Dalam makalah ini, analisis komparatif kinerja metode LSB, MSB dan PVD yang digunakan dalam penyembunyian citra dilakukan. Teknik LSB memberikan nilai PSNR dan SSIM yang lebih tinggi dibandingkan dengan metode MSB dan PVD dengan MSE yang lebih rendah dibandingkan kedua teknik lainnya.

Tabel 2.11 *Critical Riview* Jurnal 10

Judul	*Implementation Of The Rsa Cryptographic Algorithm In The Qr-Code Android-Based Building Permit Checking Application*
Nama jurnal, Volume, Nomor, Tahun	JURNAL NUANSA INFORMATIKA Volume 15 Nomor 1, Januari 2021
Penulis	Darsanto, Rio Andriyat Krisdiawan, Dias Eka Prayuda
Metode/Algoritma	Algoritma RSA
Hasil	RSA memiliki proses enkripsi dan dekripsi berdasarkan konsep bilangan prima dan aritmatika modulo. Baik kunci dekripsi dan kunci enkripsi adalah bilangan bulat. Kunci enkripsi tidak dirahasiakan dan dipublikasikan, sehingga kunci

	enkripsi juga dikenal sebagai kunci publik, tetapi kunci dekripsi bersifat rahasia.
Kekuatan Penelitian	Keunggulan dari sistem yang dibuat adalah sistem ini dapat memindai kode *QR* yang dienkripsi dengan algoritma RSA, sehingga kode *QR* yang dibuat tidak dapat dengan mudah dipalsukan atau dibaca oleh aplikasi sejenis.
Kelemahan Penelitian	Tidak adanya fitur seperti cetak surat izin di *web* administrator. Sistem bawaan belum berfungsi di aplikasi ios
Kesimpulan	1. Sistem dapat membantu pengguna untuk memberi keamanan pada surat izin. 2. Sistem ini dapat memindai / *scan Qrcode* pada surat izin DPMPTSP. 3. Sistem ini dapat mengenkripsi dan mendekripsi digit dalam *Qrcode* menggunakan algoritma RSA.

Tabel 2.12 *Critical Riview* Jurnal 11

Judul	Penerapan *Digital Signature* Untuk Mengesahan Proposal Hibah Dikti Menggunakan *Secure Hash Algorithm*
Nama jurnal, Volume, Nomor, Tahun	JOINTECS (*Journal of Information Technology and Computer Science*), Vol. 5 No. 2 (2020) 105 - 112
Penulis	Eugenius Kau Suni, Haidar Ilham Maulana
Metode/Algoritma	Algoritma *Secure Hash Algorithm* (SHA)
Hasil	Sistem yang diciptakan ini bertujuan untuk mengatasi permasalahan dan hambatan yang selama ini masih dihadapi oleh para dosen pengusul proposal Hibah Dikti, terutama saat proses

	verifikasi dokumen yang masih dilakukan secara manual.
Kekuatan Penelitian	Pembahasan detail sehingga sehingga mudah dipahami
Kelemahan Penelitian	Karena dibahas secara detail, sulit menemukan kelemahan dalam penelitian ini
Kesimpulan	Pembuatan sistem pengesahan dokumen proposal Hibah Dikti dengan digital *signature* menggunakan *secure hash alogrithm* ini telah diselesaikan dengan baik. Sistem yang dihasilkan bertujuan untuk mengatasi permasalahan dan kendala yang dihadapi oleh dosen pengusul proposal Hibah Dikti secara khusus saat pengesahan dokumen yang masih dilakukan secara manual

Tabel 2.13 *Critical Riview* Jurnal 12

Judul	*A Comparative Study of Audio Steganography Schemes*
Nama jurnal, Volume, Nomor, Tahun	*International Journal of Computing and Digital Systems, Int. J. Com. Dig. Sys*. 10, No.1 (Apr-2021)
Penulis	Farah Hemeida, Wassim Alexan and Salma Mamdouh
Metode/Algoritma	Algoritma AES–256, *Blowfish*, dan teknik substitusi LSB
Hasil	Kinerja skema yang diusulkan dievaluasi dalam hal uji pendengaran, waktu aktif, kemampuan integrasi, pelacakan bentuk gelombang, serta sejumlah besar pengukuran statistik dalam domain waktu dan domain frekuensi. Selain itu, disajikan perbandingan skema yang diusulkan menggunakan

	AES-256 dengan rekan-rekannya dalam literatur. Hasil *numerik* menunjukkan bahwa skema yang diusulkan bekerja dengan sangat baik.
Kekuatan Penelitian	Menggunakan kombinasi algoritma AES-256, teknik substitusi *Blowfish* dan LSB, menciptakan keamanan ganda untuk pesan
Kelemahan Penelitian	Media yang digunakan untuk menyembunyikan pesan terenkripsi, yaitu *audio*, membutuhkan ruang penyimpanan yang besar
Kesimpulan	Makalah ini mengusulkan sistem keamanan pesan dua lapis dimana lapisan pertama adalah lapisan kriptografi dan lapisan kedua adalah lapisan steganografi. Skema yang diusulkan menggunakan AES–256, *Blowfish*, atau peta Logistik untuk lapisan kriptografi. Lapisan steganografi menggunakan teknik substitusi LSB untuk menutupi pesan acak dalam suara sampul dengan beralih secara bergantian antara saluran kiri dan kanan dari suara sampul. Kinerja yang diusulkan dievaluasi dan analisis keamanan dilakukan. Selanjutnya, kinerja skema yang diusulkan menggunakan AES-256 dibandingkan dengan rekan-rekannya dalam *literatur* dan terbukti berkinerja lebih baik dalam hal PSNR.

Tabel 2.14 *Critical Riview* Jurnal 13

Judul	Penerapan Algoritma *Rivert Code 4* (RC 4) Pada Aplikasi Kriptografi Dokumen
Nama jurnal, Volume, Nomor, Tahun	Jurnal PETIR Vol. 11 No. 1 Maret 2018
Penulis	Harni Kusniyati, Satya Diansyah, Raka Yusuf

Metode/Algoritma	Algoritma *Rivest Code 4* (RC4)
Hasil	Hasil yang diperoleh dari penelitian ini adalah aplikasi kriptografi dokumen dapat mengenkripsi dan mendekripsi dokumen menggunakan algoritma *Rivest Code 4* (RC 4).
Kekuatan Penelitian	Pembahasan detail sehingga sehingga mudah dipahami
Kelemahan Penelitian	Karena dibahas secara detail, sulit menemukan kelemahan dalam penelitian ini
Kesimpulan	Aplikasi kriptografi menggunakan algoritma RC 4 telah berhasil diimplementasikan pada tahap perancangan dan pembangunan aplikasi menggunakan pemodelan UML. Kata sandi enkripsi *file* tidak mudah dibaca karena RC 4 menerapkan pengacakan kunci yang sangat kompleks yang sulit diretas. Aplikasi ini telah memenuhi komponen kriptografi yaitu kerahasiaan, keutuhan dan keaslian data

Tabel 2.15 *Critical Riview* Jurnal 14

Judul	*A New Method of Coding for Steganography Based on LSB Matching Revisited*
Nama jurnal, Volume, Nomor, Tahun	*Security and Communication Networks* Volume 2021, Article ID 6610678
Penulis	Mansoor Fateh, Mohsen Rezvani, Yasser Irani
Metode/Algoritma	Metode steganografi berbasis LSB menjadi dua kategori: LSBR (penggantian LSB) dan LSBM (pencocokan LSB)
Hasil	Pengujian kami menggunakan *steganalisis* menunjukkan bahwa penerapan metode kami menghasilkan tingkat kesalahan deteksi sekitar

	10% lebih tinggi daripada menggunakan dua metode steganografi
Kekuatan Penelitian	Metode yang diusulkan dapat digunakan pada langkah pertama dari setiap metode duplikasi untuk mengurangi distorsi gambar citra. Jadi metode ini merupakan metode pengkodean baru untuk steganografi
Kelemahan Penelitian	Tidak adanya tampilan aplikasi sehingga dalam pemahaman kurang maksimal
Kesimpulan	Hasil percobaan kami menunjukkan bahwa skema yang kami usulkan membutuhkan lebih sedikit modifikasi daripada metode LSB dasar.

Tabel 2.16 *Critical Riview* Jurnal 15

Judul	*Comparative Study of* Critical Riview Jurnal 15*RSA Asymmetric Algorithm and AES Algorithm for Data Security*
Nama jurnal, Volume, Nomor, Tahun	Edu Komputika Journal, Edu Komputika 9 (1) (2022)
Penulis	Siti Alvi Sholikhatin, Adam Prayogo Kuncoro,Afifah Lutfia Munawaroh, dan Gilang Aji Setiawan
Metode/Algoritma	Algoritma RSA dan AES
Hasil	Penelitian menunjukkan bahwa menggunakan algoritma enkripsi AES lebih optimal daripada enkripsi RSA dalam melindungi data digital. Namun, karena proses enkripsi dan dekripsi lebih cepat dengan algoritma AES, perbedaan waktu pengujian antara kedua algoritma enkripsi tidak terlalu besar.

Kekuatan Penelitian	Dengan menggabungkan algoritma RSA dan AES, ini menciptakan keamanan ganda untuk *file*
Kelemahan Penelitian	*File* terenkripsi tidak ada media untuk menyembunyikan, hal ini menimbulkan kecurigaan bagi para pengamat
Kesimpulan	Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa penggunaan algoritma enkripsi AES dalam melindungi data digital lebih optimal dibandingkan dengan enkripsi RSA. Namun, karena proses enkripsi dan dekripsi lebih cepat dengan algoritma AES, perbedaan waktu pengujian antara kedua algoritma enkripsi tidak terlalu besar..

2.2 Teori Pendukung

2.2.1 *CodeIgniter*

CodeIgniter adalah sebuah *framework* yang dibuat dengan bahasa pemrograman PHP untuk memudahkan pembuatan atau pengembangan aplikasi *web* oleh *web programmer*. *CodeIgniter* memiliki kecepatan eksekusi tercepat dibandingkan *framework* lainnya. *CodeIgniter* adalah *open source* dan menggunakan pola dasar MVC (*Model*, *View*, *Controller*), model konseptual modern saat ini. Metode MVC (*Model*, *View*, *Controller*) terdiri dari tiga elemen [16]:

a. *Model*

Model dihubungkan dengan *database*, sehingga model biasanya akan berisi kelas-kelas atau fungsi untuk membuat, memperbarui, menghapus data, mencari data, dan mengambil data dari *database*

b. *View*

View adalah bagian dari *user interface* atau bagian yang nantinya akan terlihat oleh *end user*.

c. *Controller*

Controller, koneksi antara *view* dan *model*, berarti *controller* ini digunakan sebagai jembatan antara keduanya, karena *model* tidak dapat dihubungkan langsung ke *view* atau sebaliknya.

2.2.2 PHP

PHP adalah singkatan dari *Hypertext Preprocessor* yang digunakan sebagai bahasa *script server-side* dalam pengembangan web yang disisipkan pada dokumen HTML. Menggunakan PHP memungkinkan *web* menjadi dinamis, membuat pengelolaan situs *web* menjadi lebih mudah dan efisien [13].

2.2.3 *MySQL*

MySQL adalah program penyimpanan data *multi*-pengguna yang memungkinkan anda mengirim dan menerima data dengan cepat dan memiliki sistem keamanan yang sangat baik. *MySQL* sendiri menggunakan perintah dasar SQL (*Structured Query Language*). Anda dapat menggunakan *MySQL* sebagai *database* gratis di bawah GNU/GPL (*General Public License*) [17].

2.2.4 *Waterfall*

Model waterfall adalah model klasik dimana perangkat lunak dibangun secara sistematis dan satu demi satu. Model ini tepat disebut "*Linear Sequential Model*". Model ini sering disebut sebagai "*classical life cycle*" atau metode air terjun. Model ini menggunakan pendekatan yang sistematis dan berurutan. Disebut *waterfall* karena bagian yang dilewati harus menunggu langkah sebelumnya selesai dan berjalan secara berurutan.

2.2.5 Kriptografi

Kriptografi adalah ilmu dan seni mengamankan pesan. Dengan menggunakan teknik kriptografi, pesan yang dikirim mengalami proses enkripsi agar pesan dapat dikirim kembali, sehingga pesan tersebut hanya dapat dibaca oleh orang yang memiliki kunci rahasia. Kriptografi memiliki empat tujuan dasar, yang juga merupakan aspek keamanan informasi : Kerahasiaan, adalah layanan yang dirancang untuk melindungi konten informasi dari siapa pun kecuali mereka yang

memiliki izin atau kunci rahasia untuk membuka/mendekripsi informasi terenkripsi. Integritas data mengacu pada pemeliharaan perubahan data ilegal.

Untuk menjaga integritas data, sistem harus [5] mampu mendeteksi perusakan data oleh orang yang tidak berwenang, termasuk penyisipan, penghapusan, dan penggantian data lain dengan data asli. Otentikasi mengacu pada identifikasi atau pengenalan dalam entitas sistem dan dalam informasi itu sendiri. Kedua pihak yang berkomunikasi harus memperkenalkan diri. Informasi yang dikirim melalui saluran harus diautentikasi dalam hal keasliannya, konten data, waktu transmisi, dan lain-lain. *Non-repudiation*, atau *non-denial* adalah upaya untuk mencegah seseorang menolak untuk mengirimkan atau membuat informasi [5].

Algoritma kriptografi terdiri dari tiga fungsi dasar [18], yaitu :

a. Enkripsi adalah tentang keamanan data yang dikirimkan, sehingga kerahasiaan tetap terjaga. Pesan asli disebut *plaintext* dan diubah menjadi kode yang tidak dapat dipahami.
b. Dekripsi adalah kebalikan dari enkripsi. Pesan terenkripsi dikembalikan ke bentuk aslinya. Ini disebut mendekripsi pesan. Algoritma yang digunakan untuk dekripsi tentunya berbeda dengan yang digunakan untuk enkripsi.
c. Kunci, dalam hal ini kunci digunakan untuk enkripsi dan dekripsi. Kunci dibagi menjadi dua bagian, yaitu: kunci rahasia (*private key*) dan kunci publik (*public key*).

Secara umum, algoritma kriptografi diklasifikasikan berdasarkan kesamaan kunci sebagai berikut [18]:

a. Algoritma Kunci Simetris.

   Secara umum, kriptografi simetris bekerja dalam mode *cipher blok*, yaitu setiap kali proses enkripsi atau dekripsi dilakukan pada blok data (dengan ukuran tertentu), atau mereka bekerja dalam mode aliran (*block cipher*), yaitu setiap

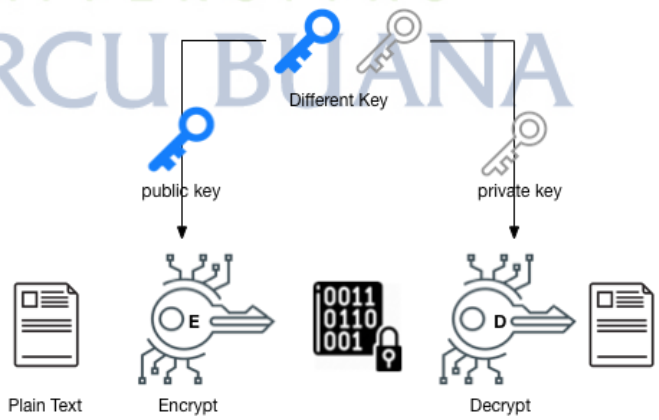
kali enkripsi atau dekripsi dilakukan pada *bit* atau *byte* data [13].

b. Algoritma Kunci Asimetris

Berbeda dengan kriptografi kunci simetris, kriptografi kunci publik memiliki dua kunci yang berbeda untuk proses enkripsi dan dekripsi. Saat kunci digunakan untuk proses enkripsi (sering disebut kunci publik) dan dekripsi (sering disebut kunci *private*) menggunakan kunci yang berbeda. Entitas pengirim mengenkripsi dengan kunci publik sementara entitas penerima mendekripsi dengan kunci *private*.

2.2.6 *Rivest-Shamir-Adleman* (RSA)

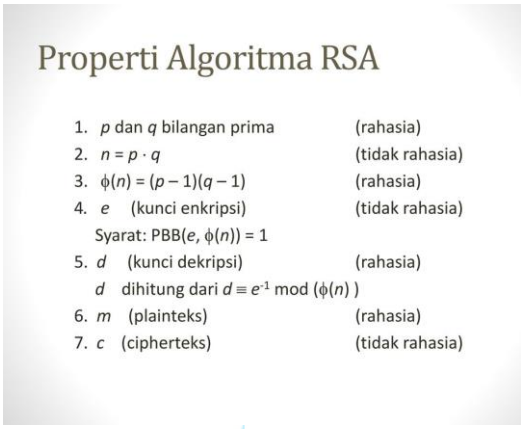
Algoritma RSA adalah algoritma kriptografi kunci asimetris yang dikembangkan pada tahun 1977 oleh tiga peneliti MIT, *Ron Rivest*, *Adi Shamir*, dan *Leonard Adleman*. Nama algoritma ini diambil dari inisial nama belakang tiga orang. Algoritma ini memiliki dua kunci, yaitu kunci *private* dan kunci publik. Tingkat keamanan algoritma ini didasarkan pada panjang kunci yang digunakan. Semakin panjang digitnya, semakin sulit solusinya untuk dipecahkan [5]. Gambar 2.1 menunjukkan bagaimana kunci asimetris bekerja dengan kunci publik dan kunci pribadi.



Gambar 2.1 Proses enkripsi dan dekripsi dengan kunci asimetris

Algoritma RSA dimulai dengan membangkitkan pasangan kunci yang terdiri dari kunci publik dan kunci *private*. Kunci publik

yang dihasilkan digunakan dalam proses enkripsi. Kunci pribadi digunakan oleh penerima dalam proses dekripsi pesan. Formula lengkap algoritma RSA dapat dilihat pada gambar 2.2



Gambar 2.2 Rumus Algoritma RSA

2.2.7 Steganografi

Steganografi adalah usaha atau proses penyembunyian data dan informasi penting di media lain, yang dapat berupa teks, video, audio, dan gambar. Steganografi tidak dapat dipisahkan dari enkripsi. Perbedaan utamanya adalah enkripsi membuat data tidak dapat dipecahkan dan tidak dapat dibaca, tetapi *ciphertext* dapat dilihat oleh manusia, berbeda dengan steganografi, yang bertujuan untuk menyembunyikan informasi sensitif sehingga tidak dapat dilihat oleh mata manusia dalam bentuk media. [4].

Media penyisipan pesan rahasia yang digunakan dalam teknik steganografi digital antara lain: [8]:

a. Teks

   Dalam algoritma steganografi yang menggunakan teks sebagai media penyisipan, teknik NLP biasanya digunakan untuk memastikan bahwa teks yang disisipkan dengan pesan rahasia tidak menimbulkan kecurigaan bagi orang yang melihatnya. Contoh format teks : teks *file*, *html*, *pdf*, dll.

b. Audio

Format ini sering dipilih karena *file* dalam format ini biasanya berukuran relatif besar. Sehingga juga dapat menampung pesan rahasia dalam jumlah yang banyak. Contoh format audio : *wav*, *voc*, *mp3*, dll.

c. Citra

Format ini adalah salah satu format *file* yang paling sering dipertukarkan di dunia *Internet*, sehingga juga merupakan format yang paling banyak digunakan. Alasan lainnya adalah banyaknya algoritma steganografi yang tersedia untuk media penyimpanan gambar. Contoh format citra : *bitmap* (*bmp*), *gif*, *pcx*, *jpeg*, dll.

d. Video

Sebenarnya format ini merupakan format dengan ukuran *file* yang relatif besar, namun jarang digunakan karena ukurannya yang terlalu besar sehingga mempengaruhi kepraktisannya dan juga kurangnya algoritma yang mendukung format ini. Contoh format video : *mpeg*, *avi*, dll.

Manfaat menggunakan steganografi adalah memungkinkan Anda mengirim pesan secara diam-diam tanpa mengetahui pesan sedang dikirim karena pesan disembunyikan. Akibatnya, pihak ketiga tidak mengetahui keberadaan pesan tersebut. Sebaliknya, penggunaan kriptografi akan menarik kecurigaan pihak ketiga dapat menimbulkan kecurigaan bahwa ada sesuatu yang tersembunyi di dalam pesan yang anda kirimkan. Steganografi juga memiliki kekurangan. Namun, steganografi memakan banyak ruang untuk menyembunyikan beberapa bagian pesan. Kelemahan ini masih dapat diatasi dengan pengembangan teknik steganografi [19].

2.2.8 *Least Significant Bit* (LSB)

Least significant bit adalah bagian dari barisan data *biner* (basis dua) yang memiliki nilai paling tidak signifikan/minimum. Terletak di ujung kanan kolom *bit*. Sedangkan *most significant bit* adalah sebaliknya, yaitu angka paling signifikan/terbesar dan letaknya disebelah paling kiri. Contohnya adalah bilangan *biner* dari 255 adalah

11111111 (kadang-kadang diberi huruf b pada akhir bilangan menjadi 1111 1111b). Bilangan tersebut dapat berarti:

$$\mathbf{1 * 2^7 + 1 * 2^6 + 1 * 2^5 + 1 * 2^4 + 1 * 2^3 + 1 * 2^2 + 1 * 2^1 + 1 * 2^0}$$
$$\mathbf{= 128 + 64 + 32 + 16 + 8 + 4 + 2 + 1 = 225}$$

Dari barisan angka 1 di atas, angka 1 paling kanan bernilai 1, dan itu adalah yang paling kecil. Bagian tersebut disebut dengan *least significant bit* (*bit* yang paling tidak berarti), sedangkan bagian paling kiri bernilai 128 dan disebut dengan *most significant bit* (*bit* yang paling berarti) [19].

Metode *Last Significat Bit* memiliki kelebihan dan kekurangan dalam penerapannya, yaitu:

Kelebihan Teknik LSB [9]:

a) Digunakan untuk penyisipan data.
b) Banyak teknik yang menggunakan cara ini karena sangat mudah dilakukan.
c) Gambar aslinya sangat mirip dengan gambar *Stego*.
d) Distorsi lebih kecil dari gambar aslinya.
e) Lebih banyak data dapat disematkan ke dalam gambar.
f) Kurang mencurigakan dari mata manusia

Kekurangan teknik LSB [9]:

a. Mudah dicuri oleh orang ilegal.
b. Mengompresi gambar dapat mengakibatkan hilangnya data tersembunyi yang kurang kuat.
c. Tiga kelemahan- *Robustness, Tamper* dan *Resistance*.
d. Sangat sensitif terhadap segala jenis penyaringan.
e. *Scaling*, *Rotation*, *Cropping*, menambahkan *lead noise* ekstra untuk menghancurkan pesan rahasia.

2.2.9 Citra Digital

Citra adalah representasi (gambar), kemiripan, atau tiruan dari suatu objek. Gambar dibagi menjadi dua kategori: gambar *analog* dan gambar *digital*. Gambar *analog* adalah gambar yang berkesinambungan

seperti gambar pada monitor TV, *radiografi*, hasil *CT scan*, dll. Gambar *digital*, di sisi lain, adalah gambar yang dapat diproses oleh komputer. Format *file* gambar harus dapat menggabungkan kualitas gambar, ukuran *file*, dan kompatibilitas dengan berbagai aplikasi. Ada beberapa format *file* gambar standar yang digunakan saat ini. Format ini digunakan untuk menyimpan gambar dalam *file*. Setiap format memiliki karakteristiknya sendiri. Ini adalah contoh format umum, yaitu : *Bitmap (.bmp), tagged image format (.tif, .tiff), PortablNetwork Graphics (.png), JPEG (.jpg),* dll [18].

Ada dua jenis format *file* gambar yang biasa digunakan dalam pengolahan gambar, yaitu: gambar *bitmap* dan gambar *vektor*. Gambar *bitmap* ini sering disebut sebagai gambar *raster*. Citra *bitmap* ini menyimpan data kode citra secara digital dan lengkap (cara penyimpanannya adalah piksel). Gambar *bitmap* ini dapat direpresentasikan dalam bentuk matriks atau dipetakan menggunakan biner atau sistem bilangan lainnya. Gambar ini memiliki keuntungan dapat memanipulasi warna, tetapi lebih sulit untuk mengubah objek. Tampilan *bitmap* memungkinkan anda mengekspresikan rona halus dan gradasi warna dalam gambar. Namun saat tampilan diperbesar, gambar di monitor terlihat *corrupt* (kualitas gambar berkurang). Contoh format *file* citra antara lain adalah BMP, GIFF, TIF, JPG, dll.

Sedangkan format *file* gambar *vektor* adalah gambar *vektor* yang diperoleh dengan perhitungan matematis, tidak ada piksel, data disimpan dalam bentuk *vektor* posisi, dan hanya informasi *vektor* posisi yang disimpan dalam bentuk fungsi. Untuk gambar *vektor*, mengubah warna lebih sulit, tetapi mengubah nilai dan memahat objek itu mudah. Oleh karena itu, saat anda memperbesar atau memperkecil gambar, kualitas gambar tetap relatif baik dan tidak berubah. Citra vektor biasanya dibuat menggunakan aplikasi-aplikasi citra vektor seperti *CorelDRAW, Adobe Illustrator, Macromedia Freehand, Autocad,* dll [18].

Citra berwarna digital adalah salah satu tipe data yang paling umum digunakan karena alasan berikut [6]:

a. Kemudahan akses dan biaya rendah karena ketersediaan berbagai perangkat pencitraan digital
b. Pengolahan citra digital sederhana
c. Gambar besar yang menyediakan data dalam jumlah besar
d. Kemampuan untuk menyimpan gambar digital secara diam-diam
e. Nilai piksel sama dengan nilai ASCII

Citra warna digital diwakili oleh 3 matriks 2D, satu matriks untuk setiap warna (*Red*, *Green* dan *Blue*). *Matriks* warna dapat digunakan secara individual, dan isi dari setiap *matriks* dapat diekstraksi untuk membentuk kunci (atau kumpulan kunci) dengan panjang sembarang. Anda dapat mengubah ukuran *matriks* gambar berwarna menjadi *matriks* baris tunggal dengan sejumlah elemen tertentu..

2.2.10 *Black Box Testing*

Definisi pengujian *black-box* adalah metodologi pengujian yang berfokus pada spesifikasi fungsional perangkat lunak. Fokusnya adalah pada informasi domain karena pengujian mengabaikan struktur kontrol. Pengujian menggunakan pengujian *black box* memungkinkan perancang sistem untuk membuat sekumpulan kondisi masukan yang melatih semua kendala fungsional dari sistem.

Keuntungan menggunakan metode pengujian *black box* adalah bahwa pengujian tidak memerlukan pengetahuan tentang bahasa pemrograman tertentu. Karena pengujian dilakukan dari sudut pandang pengguna, pemrogram dan penguji saling bergantung.

Kekurangan dari metode pengujian *black box* adalah sulitnya merancang *test case* tanpa spesifikasi yang jelas. Anda dapat mengulangi tes yang sudah dilakukan oleh pengembang. bagian dari *backend* tidak diuji sama sekali [20].

Pengujian *black box* berupaya mendeteksi kategori [13] sebagai berikut:

a) Fungsi yang salah atau hilang

b) Kesalahan *interface*

c) Kesalahan dalam struktur data atau database eksternal

d) Kesalahan kinerja

e) Kesalahan inisialisasi dan terminasi