Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

Watermarking Citra Digital DFT Dan Kriptografi Algoritma RSA Pada Sistem Berbasis Web

Nur Wulan[1], Herlina Harahap[2], Yunita Sari Siregar[3]

[1,2,3] Fakultas Teknik dan Komputer, Program Studi Teknik Informatika , Universitas Harapan Medan, Medan, Indonesia

Email: [1]nurwulanstth@gmail.com, [2]Herlina_Hrp@yahoo.com, [3] yunitasarisiregar1990@gmail.com
Email Penulis Korespondensi: yunitasarisiregar1990@gmail.com

Abstrak– Dalam perkembangan teknologi informasi yang sangat meningkat terdapat tantangan dalam memastikan keamanan dan perlindungan hak cipta khususnya dalam citra digital. Penggunaan citra digital dilakukan pada berbagai bidang seperti bidang pendidikan, kesehatan, bisnis dan lainnya. Citra digital menjadi sangat rentan dalam penyalahgunaan seperti plagiarisme, manipulasi, dan distribusi illegal yang dapat merugikan orang lain. Oleh karena itu diperlukan teknologi yang dapat melindungi integritas dan kepemilikan citra digital secara efektif. Watermarking adalah salah teknologi yang dapat digunakan untuk melindungi hak cipta tanpa merusak kualitas citra digital. Salah satu metode watermarking yaitu Discrete Fourier Transform (DFT), dengan mengubah citra ke domain frekuensi, sehingga watermark yang ditanamkan lebih efektif terhadap berbagai manipulasi maupun kompresi. Selain itu, kriptografi mempunyai fungsi dalam neningkatkan keamanan watermarking. Salah satu algoritam kriptografi adalah Rivest Shamir Adleman (RSA), dengan mengenkripsi dana mendeskripsi data menggunakan kunci publik dan kunci privat. Dalam proses watermarking, RSA akan melindungi watermark dengan mengenkripsi sebelum proses penyisipan dilakukan, sehingga pihak yang memiliki kunci privat dapat membaca watermark tersebut. Platform web memberikan fleksibilitas bagi pengguna untuk mengunggah, menyisipkan, atau memverifikasi watermark dengan mudah. Penggabungan metode DFT dan algoritma RSA dalam sistem berbasis web akan memberikan perlindungan yang lebih kuat terhadap pelanggaran hak cipta citra digital

Kata Kunci: Watermarking; Discrete Fourier Transform (DFT); Kriptografi; Rivest Shamir Adlmenan (RSA); Sistem: Web

1. PENDAHULUAN

Di era digital, kemajuan teknologi memungkinkan penyebaran informasi, termasuk citra digital, terjadi dengan sangat cepat. Namun, perkembangan ini juga membawa risiko seperti penyalahgunaan, pelanggaran hak cipta, hingga manipulasi citra digital. Masalah ini menimbulkan kebutuhan akan solusi yang dapat melindungi hak kepemilikan dan keaslian citra digital secara efektif. Salah satu teknologi yang berkembang untuk menjawab tantangan ini adalah watermarking citra digital dan kriptografi dalam menjaga integritas data. Watermarking citra digital menjadi salah satu metode yang umum digunakan untuk menjaga keaslian dan memberikan perlindungan hak cipta pada citra digital. Dengan menyisipkan informasi tertentu (watermark) ke dalam citra digital, pemilik dapat membuktikan kepemilikan suatu citra jika terjadi pelanggaran. Namun, agar watermarking dapat efektif, watermark harus bersifat tahan terhadap berbagai gangguan, seperti kompresi, pemotongan, atau modifikasi citra. Dalam hal ini, metode Discrete Fourier Transform (DFT) digunakan karena memiliki kemampuan unggul dalam domain frekuensi, yang membuat watermark lebih sulit dihilangkan atau dirusak tanpa memengaruhi kualitas citra secara signifikan. Tedapat beberapa penelitian yang telah dilakukan dalam pemanfaatan watermarking Discrete Fourier Transform (DFT) dan Kriptografi Algoritma Rivest Shamir Adleman (RSA) antara lain: metode yang tahan terhadap serangan *compress* ialah metode DFT, untuk gambar bertipe *biner*, metode yang tahan terhadap serangan *compress* ialah metode DFT (Solikhin et al., 2022), Implementasi Algoritma kriptografi RSA dalan sistem informasi perputakaan (Dairi et al., 2022),

Citra digital merupakan citra yang telah disimpan dalam bentuk file sehingga dapat diolah dengan menggunakan komputer (Setyansyah et al., 2019). Citra mempunyai karakteristik yang tidak dimiliki oleh data teks, yaitu citra kaya dengan informasi (Ramadhani et al., 2018). Watermarking citra digital merupakan teknik yang digunakan untuk memberi tanda kepemilikan atau informasi hak cipta tanpa terlihat dalam media digital. Menurut (Wahyuningsih et al., 2017), Fidelity adalah mutu citra penampung tidak jauh berubah. Pengamat tidak mengetahui kalau di citra tersebut terdapat data rahasia. Watermarking (M Khairani & Nurwulan, 2018), merupakan aplikasi dari steganografi, namun ada perbedaan antara keduanya. Jika pada steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apa, maka pada watermarking justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian label hak cipta atau watermark. Terdapat dua proses utama di dalam watermarking citra digital, yaitu proses penyisipan (embedding) dan ekstraksi (extraction) (Umar & Darwis, 2019). Adapun metode watermarking yang diguanakan adalah Discreat Fourier Transform (DFT), merupakan prosedur matematika yang digunakan untuk menentukan harmonik atau frekuensi yang merupakan isi dari urutan sinyal diskrit. Urutan sinyal diskrit adalah urutan nilai yang diperoleh dari sampling periodik sinyal kontinu dalam domain waktu (Ariyanto et al., 2018).

Menurut terminologi kriptografi adalah ilmu dan seni menjaga keamanan pesan ketika pesan dikirim dari satu tempat ke tempat lain. Jika Anda bertukar pesan (seperti surat) dengan orang lain, maka Anda tentu ingin agar pesan yang Anda kirim sampai ke pihak yang dituju dengan aman (Mufida Khairani et al., 2022). Kriptografi adalah cara untuk mengacak informasi ke dalam berbagai bentuk yang tidak dapat dibaca sebelum diterjemahkan (Mido & Ujianto, 2022). Pengaman data dengan teknik kriptografi dilakukan dengan merubah data yang akan dirahasiakan (plaintext)

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

menjadi data yang disandikan (ciphertext) (Rahmatsyah et al., 2024). Algoritma RSA merupakan algoritma kunci publik yang dalam proses pengerjaannya membutuhkan konsep matematika, yaitu Faktor PersekutuanTerbesar (FPB), algoritma Euclid, relatif prima, bilangan prima, aritmetika modular, dan kekongruenan. Keamanan algoritma RSA dilihat dari susahnya memfaktorkan bilangan-bilangan prima besar dari proses pembangkitan sepasang kunci. Hasil dari algoritma ini adalah kunci publik $(e,)$ yang digunakan untuk enkripsi dan kunci pribadi $(d,)$ yang digunakan untuk dekripsi dengan e, d, dan n merupakan bilangan bulat positif. Kunci yang digunakan pada enkripsi dan dekripsi pada pesan biasa berbeda dengan kunci yang digunakan pada tanda tangan digital. Pada tanda tangan digital, kunci pribadi $(d,)$ digunakan untuk mengenkripsikan pesan dan kunci publik $(e,)$ digunakan untuk mendekripsi pesan (HR et al., 2021). Algoritma RSA menggunakan pemfaktoran bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk menemukan kunci privat (Rizki & Ariyani, 2021)

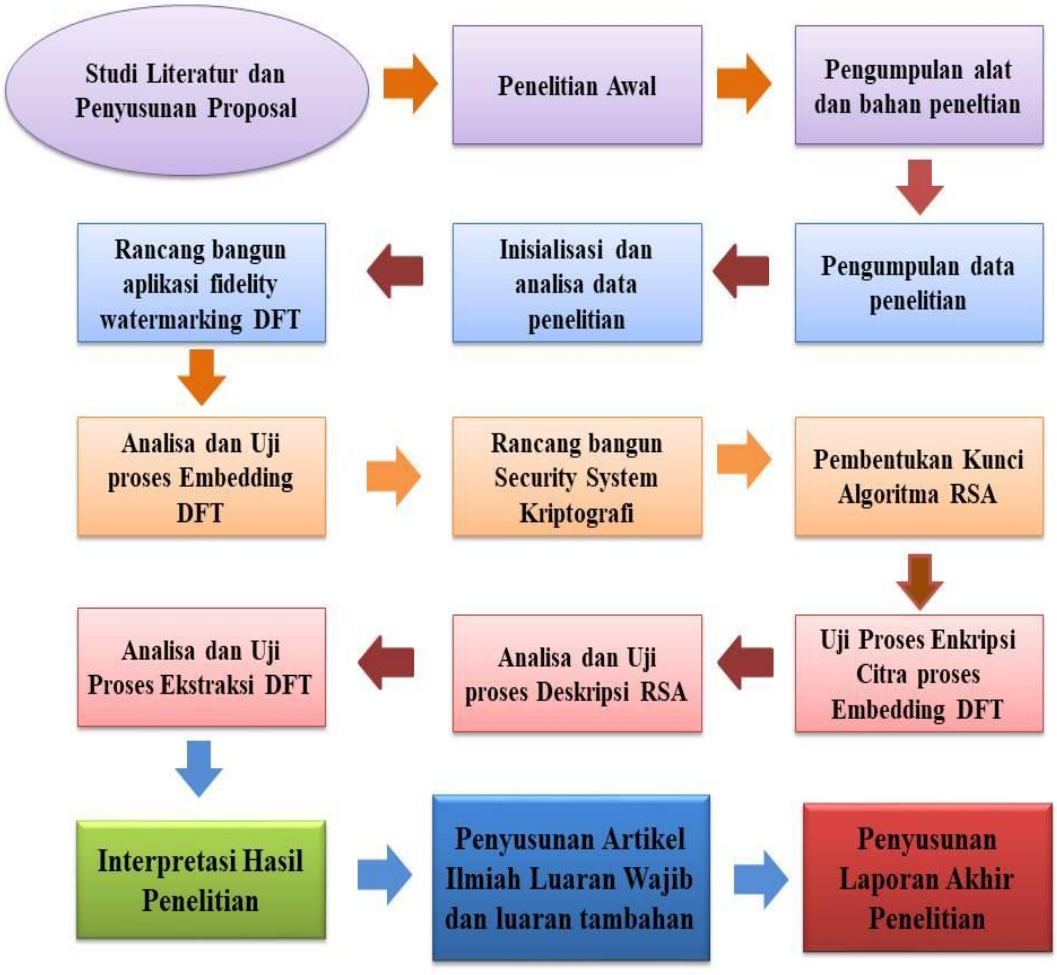
Ada empat tujuan mendasar dalam ilmu kriptografi ini yang juga merupakan aspek keamanan informasi, yaitu(Azhar & Yuliany, 2019)

1. Kerahasiaan (confidentiality). Kerahasiaan adalah layanan yang ditujukan untuk menjaga agar pesan atau informasi tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data (data integrity). Integritas data adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman
3. Autentikasi (authentication). Autentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihakpihak yang berkomunikasi (user autehentication).
4. Non-repudiasi atau nirpenyangkalan. Non repudiasi atau nirpenyangkalan adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan.

2. METODE PENELITIAN

2.1 Kerangka Dasar Penelitian

Terdapat beberapa tahapan metodologi penlitian yang akan digambarkan pada kerangka kerja penelitia pada gambar 1 dibawah ini



Gambar 1. Kerangka Kerja Penelitian

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

2.2 Tahapan Penelitian

Berdasarkan kerangka kerja penelitian diatas, terdapat beberapa tahapan sebagai berikut :

1. Watermarking Metode Discrete Fourier Transform (DFT)

Watermarking merupakan salah satu bentuk dari *steganography,* yang dapat diartikan sebagai suatu teknik penyembunyian data atau informasi ke dalam suatu data lainnya.(Gani & Setiyono, 2019). *Descrete Fourier Transform* (DFT) merupakan metode transformasi matematis untuk mengubah sinyal dari domain waktu ke dalam domain frekuensi dan sebaliknya domain frekuensi dapat di kembalikan ke domain waktu dengan menggunakan Invers DFT (Elawati et al., 2022). Discrete Fourier Transform berasal dari fungsi Transformasi Fourier X(f) yang didefinisikan dalam persamaan 1:

$$X(f) = \int_{\infty}^{\infty} x[t].e^{-f2\pi ft}\,dt \quad (1)$$

Dimana:

N = Jumlah sampel input
X(m) = Urutan ke-m komponen output DFT (X(0), X(1),…,X(N-1))
m = Indeks output DFT dalam domain frekuensi (0,1,…,N-1)
x(n) = Urutan ke-n sampel input (x(0),x(1),…,x(N-1))
n = Indeks sampel input dalam domain waktu (0,1,…,N-1)
j = Bilangan imajiner (√−1)
π = Derajat (180°)
e = Logaritma natural (2.718281828459)

Dalam bidang pemrosesan sinyal kontinu, Persamaan 1 digunakan untuk mengubah fungsi domain waktu kontinu x(t) menjadi fungsi domain frekuensi kontinu X(f). Fungsi X(f) memungkinkan untuk menentukan kandungan isi frekuensi dari beberapa sinyal dan menjadikan beragam analisis sinyal dan pengolahan yang dipakai di bidang teknik dan fisika. Dengan munculnya komputer digital, ilmuwan di bidang pengolahan digital berhasil mendefenisikan DFT sebagai urutan sinyal diskrit domain frekuensi X(m), dimana:

$$F(x) = \sum_{n=0}^{N-1} x(n).e^{-f2\pi nm/N} \quad (2)$$

Dimana:

N = Jumlah sampel input
X(m) = Urutan ke-m komponen output DFT (X(0), X(1),…, X(N-1))
m = Indeks output DFT dalam domain frekUensi (0, 1,…, N-1)
x(n) = Urutan ke-n sampel input (x(0), x(1),…, x(N-1))
n = Indeks sampel input dalam domain waktu (0, 1,…, N-1)
j = Bilangan imajiner (√−1)
π = Derajat (180°)

Kemudian hubungkan dengan rumus Euler e^{-jo} = cos (o) – j sin (0) sehingga setara dengan persamaan 3:

$$X(m) = \sum_{n=0}^{N-1} x(n).\left[\cos\left(\frac{2\pi nm}{N}\right) - j\sin\left(\frac{2\pi nm}{N}\right)\right] \quad (3)$$

Dimana:
N = Jumlah sampel input
X(m) = Urutan ke-m komponen output DFT(X(0), X(1),…, X(N-1))
m = Indeks output DFT dalam domain frekUensi (0, 1,…, N-1)
x(n) = Urutan ke-n sampel input (x(0),x(1),…,x(N-1))
n = Indeks sampel input dalam domain waktu (0,1,…,N-1)
j = Bilangan imajiner (√−1)
π = Derajat (180°)

Meski lebih rumit daripada Persamaan 2, Persamaan 3 lebih mudah untuk dipahami. Konstanta j = √−1 hanya membantu membandingkan hubungan fase di dalam berbagai komponen sinusoidal dari sinyal. Nilai N merupakan parameter penting karena menentukan berapa banyak sampel masukan yang diperlukan, hasil domain frekuensi dan jumlah waktu proses yang diperlukan untuk menghitung N-titik DFT. Diperlukan N-perkalian kompleks dan N-1 sebagai tambahan. Kemudian, setiap untuk menghitung seluruh nilai N (X(0), X(1), …, X(N-1)) memerlukan N2 perkalian. Hal ini menyebabkan perhitungan DFT memakan waktu yang lama jika jumlah sampel yang akan diproses dalam jumlah besar. Transformasi Fourier Diskrit (DFT) 2 Dimensi adalah tranformasi fourier diskrit yang dikenakan pada fungsi 2D (fungsi dengan dua variabel bebas), yang didefinisikan persamaa 4 sebagai berikut :

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

$$F(u,v) = \frac{1}{MN} \sum_{y=0}^{M-1} \sum_{Y=0}^{N-1} f(y,x) \begin{pmatrix} \cos\left(2\pi \left(\frac{ux}{N} + \frac{vy}{M}\right)\right) \\ -j \sin\left(2\pi \left(\frac{ux}{N} + \frac{vy}{M}\right)\right) \end{pmatrix} \quad (4)$$

2. Kriptografi Algoritma Rivest Shamir Adleman (RSA)

Kriptografi adalah suatu ilmu yang mempelajari penulisan secara rahasia. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut Cryptology. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah (Azhar & Yuliany, 2019). RSA menggunakan dua kunci public dan satu kunci private, proses enkripsi pada RSA menggunkan kunci private dan satu kunci publik, sedangkan untuk deskripsinya RSA menggunakan dua kunci publik (Sutejo, 2021)

a. Proses pembentukan kunci

Algoritma RSA memiliki kunci publik dan kunci *private*. Kunci publik diketahui semua orang dan digunakan untuk mengenkripsi pesan. Pesan yang dienkripsi dengan kunci publik hanya dapat didekripsi menggunakan kunci *private*. Algoritma kriptografi RSA menggunakan kunci asimetris. Pada proses enkripsi menggunakan kunci publik sedangkan dekripsi menggunakan kunci privat. *Generate* kunci atau pembangkitan kunci dilakukan pada awal sebelum melakukan proses enkripsi dimana membutuhkan 2 bilangan (*integer*) prima secara acak, dalam hal ini diharuskan menggunakan sebuah pembangkit yang secara otomatis generasi bilangan tersebut dikarenakan angka-angka tersebut cukup besar dan banyak untuk memperoleh keamanan yang lebih tinggi dan lebih baik. Selanjutnya terdapat juga proses pengecekan apakah bilangan tersebut bilangan prima atau tidak sehingga akan terjadi *lopping* yang cukup lama sampai menemukan nilai prima yang sesuai dengan syarat (Sutejo, 2021). Berikut ini cara untuk membentuk kunci publik dan kunci *private* menggunakan RSA sebagai berikut:

1) Pilih bilangan prima secara acak sebanyak dua buah untuk nilai (p) dan (q). Bilangan ini harus cukup besar yaitu minimal 3 digit.
2) Hitung nilai (n), kemudian nilai (n) disebut sebagai parameter sekuriti pada persamaan 4

$$n = p \times q \quad (4)$$

3) Pilih secara acak bilangan kunci public (e) dengan syarat bilangan tersebut tidak memiliki faktor pembagi yang sama dengan Φ(n) atau (p-1) (q-1) selain bilangan 1 atau bersifat relatif prima.
4) Bentuk kunci *private* (d) dengan menggunakan sebuah algoritma yang disebut algoritma Euclid akan menghitung nilai d pada persamaan 5 dan 6.

$$e \times d = 1 \ (mod\ \Phi(n)) \quad (5)$$

atau

$$e \times d = (1 + k\ \Phi\ (n))\ (3) \quad (6)$$

Dikarenakan kedua rumus diatas bersifat ekivalen, maka d dapat dihitung menggunakan rumus, dengan syarat nilai k merupakan bilangan bulat yang dapat menghasilkan kunci dekripsi bernilai bilangan bulat juga persamaan 7.

$$d = \frac{(1+k\ \Phi\ (n))}{e} \quad (7)$$

5) Nilai n dan e dapat diketahui publik, sedangkan nilai p dan q dirahasiakan agar tidak diketahui publik. Kunci publik terdiri dari nilai (n, e), kemudian kunci *private* terdiri dari nilai (d, n)

b. Proses Enkripsi

Dalam proses enkripsi data, penyandian dilakukan menggunakan kunci publik (n, e) awalnya data berupa *plaintext* dimasukkan kemudian akan diubah kedalam bentuk ASCII pada setiap karakternya, selanjutnya *plaintext* (P) akan dienkripsikan dengan kunci public menggunakan perhitungan persamaan 8.

$$C = P^{\,e}\ (mod\ n) \quad (8)$$

c. Proses Dekripsi Data

Pada proses dekripsi data yang sudah dienkripsi sebelumnya (*ciphertext*) dengan menggunakan kunci publik (e, n) akan dikembalikan menjadi pesan awal (*plaintext*) menggunakan kunci *privat* (d, n), proses pertama yang dilakukan adalah memasukkan data *ciphertext* (C) kemudian data tersebut didekripsikan kebentuk bilangan ASCII pada setiap karakternya menggunakan perhitungan persamaan 9.

$$P = C^{\,d}\ (mod\ n) \quad (9)$$

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

3. HASIL DAN PEMBAHASAN

Analisis Sistem suatu teknik atau metode pemecahan masalah dengan cara menguraikan *system* ke dalam komponen-komponen pembentuknya untuk mengetahui bagaimana komponen-komponen tersebut bekerja dan saling berinteraksi satu sama lain untuk mencapai tujuan system.

3.1 Penerapan Metode

Penerapan metode *Discrete Fourier Transform* (DFT) dan Algoritma Kriptografi *Rivest Shamir Adleman* (RSA) dalam watermarking citra digital merupakan kombinasi teknik yang bertujuan untuk meningkatkan keamanan dan kualitas watermark yang disisipkan. DFT adalah sebuah metode matematis yang mengubah data dari domain spasial ke domain frekuensi, sehingga memungkinkan watermark disisipkan pada komponen frekuensi citra. Dengan menyisipkan watermark di domain frekuensi, citra menjadi lebih tahan terhadap serangan seperti kompresi, rotasi, atau noise, yang sering terjadi pada citra digital. Watermark yang tersembunyi di frekuensi tertentu lebih sulit untuk dideteksi atau dihapus tanpa mempengaruhi kualitas keseluruhan citra.

3.1.1 Metode Discrete Fourier Transform (DFT)

Discrete Fourier Transform (DFT) adalah metode matematis yang digunakan untuk mengubah data dari domain waktu atau spasial menjadi domain frekuensi. DFT memetakan sinyal atau citra yang diwakili oleh nilai-nilai piksel atau sampel data ke dalam bentuk komponen frekuensi, yang merepresentasikan frekuensi-frekuensi dasar yang membentuk sinyal atau citra tersebut. Pada citra digital, DFT digunakan untuk menganalisis dan memproses informasi frekuensi dari citra, sehingga memungkinkan manipulasi dan analisis yang lebih kompleks. Dalam konteks citra digital, penerapan DFT pada citra 2D memecah citra menjadi sejumlah sinyal frekuensi, di mana frekuensi rendah biasanya mengandung informasi utama citra seperti bentuk dan kontur, sementara frekuensi tinggi berisi detail halus seperti tepi. Salah satu keuntungan utama menggunakan DFT dalam watermarking adalah kemampuannya untuk menyisipkan watermark pada komponen frekuensi tertentu, sehingga watermark menjadi lebih tahan terhadap serangan atau modifikasi seperti kompresi JPEG, pemotongan, rotasi, atau noise. Dengan mengoperasikan watermark di domain frekuensi, watermark tersebut lebih sulit dihapus atau diubah tanpa mengubah kualitas keseluruhan citra secara signifikan.

3.1.2 Metode Rivest Shamir Adleman (RSA)

Algoritma RSA merupakan penerapan dari kriptografi asimetri, yaitu jenis kriptografi yang menggunakan dua kunci yang berbeda: kunci publik (p*ublic key*) dan kunci pribadi (*private key*). Adapun tingkat kerahasian dari besaran besaran pada algoritma RSA diantaranya adalah besaran besaran yang digunakan pada algoritma RSA menurut (Octafiani & Rosita. 2021):

1. p dan q bilangan prima (rahasia)
2. N = p . q (tidak rahasia)
3. Φ(n) =(p–1) (q–1) (rahasia)
4. e=(kunci enkripsi) (tidak rahasia)
5. d=(kunci dekripsi) (rahasia)
6. X (plainteks) (rahasia)
7. Y (cipherteks) (tidak rahasia)

3.2 Perancangan Sistem

Setelah mealakukan analisa, selanjutnya dilakukan perancangan terhadap system tersebut dalam peracangan system ini ada beberapa tahapan-tahapan yang harus dilakukan. Adapun tahapan-tahapan dalam perancangan sistem yang dilakukan adalah *use case diagram*, data flow diagram (DFD), perancangan antarmuka sistem dan peracangan *database* menggunakan *eloquent*.

3.2.1 Usecase Diagram

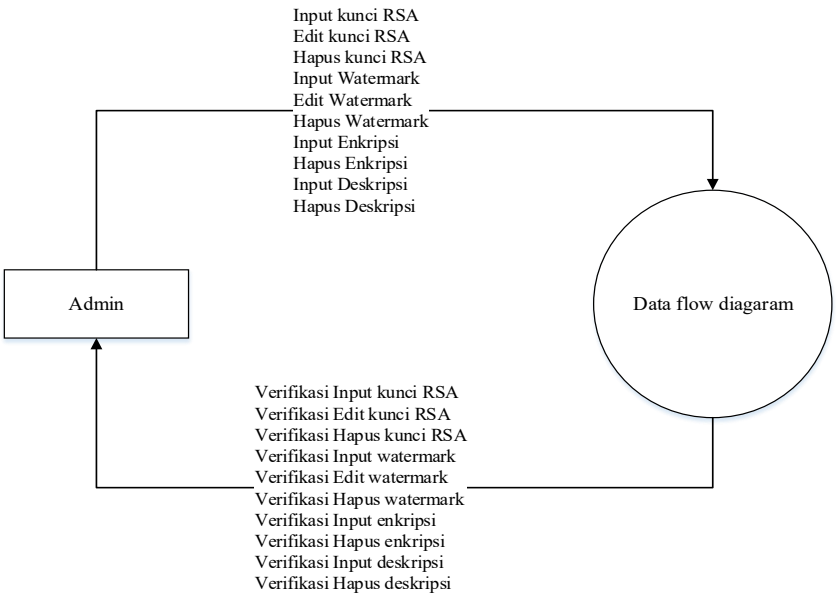
Secara garis besar, bisnis proses sistem yang akan dirancang digambarkan dengan *usecase diagram* yang terdapat pada Gambar 2.

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

Gambar 2. Use Case Diagram

3.2.2 Data Flow Diagram

Data flow diagaram merupakan suatu pemodelan proses data yang dibuat untuk menggambarkan proses darimana suatu data berasal, dapat dilihat pada gambar 3. Data Flow Diagram level 0 atau yang sering disebut dengan diagram konteks dari system yang dirancang.



Gambar 3. DFD level 0 Diagram Konteks

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

3.3 Desain Basis Data

Desain basis data terdiri dari tahap merancang kamus data, merancang struktur tabel. Selanjutnya yang dikerjakan yaitu merancang struktur tabel pada basis data sistem yang akan dibuat, berikut ini merupakan rancangan struktur tabel tersebut.

1. Struktur Tabel Akun
   Tabel akun digunakan untuk menyimpan data akun login, selengkapnya mengenai struktur tabel ini dapat dilihat pada gambar 4.

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id_akun	int(11)			No	None		AUTO_INCREMENT	Change Drop More
2	nama_lengkap	varchar(50)	utf8mb4_general_ci		No	None			Change Drop More
3	username	varchar(50)	utf8mb4_general_ci		No	None			Change Drop More
4	password	varchar(30)	utf8mb4_general_ci		No	None			Change Drop More

Gambar 4. Tabel Akun

2. Struktur Tabel Kunci
   Tabel data kunci digunakan untuk menyimpan data kunci, selengkapnya mengenai struktur tabel ini dapat dilihat pada gambar 5.

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id_kunci	int(11)			No	None		AUTO_INCREMENT	Change Drop More
2	tgl_kunci	date			No	None			Change Drop More
3	nm_kunci	varchar(50)	utf8mb4_general_ci		No	None			Change Drop More
4	kunci_private	text	utf8mb4_general_ci		No	None			Change Drop More
5	kunci_public	text	utf8mb4_general_ci		No	None			Change Drop More

Gambar 5. Tabel Kunci

3. Struktur Tabel Watermark
   Tabel data watermark digunakan untuk menyimpan data watermark, selengkapnya mengenai struktur tabel ini dapat dilihat pada gambar 6.

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id_watermark	int(11)			No	None		AUTO_INCREMENT	Change Drop More
2	id_kunci	int(11)			No	None			Change Drop More
3	tgl_watermark	date			No	None			Change Drop More
4	watermark	text	utf8mb4_general_ci		No	None			Change Drop More
5	en_watermark	text	utf8mb4_general_ci		No	None			Change Drop More

Gambar 6. Tabel Watermark

4. Struktur Tabel Enkripsi
   Tabel data enkripsi digunakan untuk menyimpan data enkripsi, selengkapnya mengenai struktur tabel ini dapat dilihat pada gambar 7.

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id_enkripsi	int(11)			No	None		AUTO_INCREMENT	Change Drop More
2	id_watermark	int(11)			No	None			Change Drop More
3	tgl_enkripsi	date			No	None			Change Drop More
4	in_gambar	text	utf8mb4_general_ci		No	None			Change Drop More
5	out_gambar	text	utf8mb4_general_ci		No	None			Change Drop More

Gambar 7. Tabel Enkripsi

5. Struktur Tabel Deskripsi

   Tabel data deskripsi digunakan untuk menyimpan data deskripsi, selengkapnya mengenai struktur tabel ini dapat dilihat pada gambar 8.

#	Name	Type	Collation	Attributes	Null	Default	Comments	Extra	Action
1	id_deskripsi	int(11)			No	None		AUTO_INCREMENT	Change Drop More
2	tgl_deskripsi	date			No	None			Change Drop More
3	in_gambar	text	utf8mb4_general_ci		No	None			Change Drop More
4	out_watermark	text	utf8mb4_general_ci		No	None			Change Drop More

Gambar 8. Tabel Deskripsi

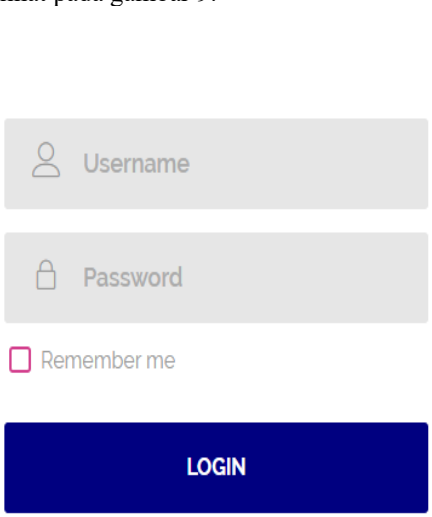
Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

3.4 Implementasi

Implementasi dan pengujian sistem merupakan kelanjutan dari kegiatan perancangan sistem dan dapat dipandang sebagai usaha untuk mewujudkan *system* yang dirancang. Pada bab ini akan diuraikan cara dan Langkah-langkah untuk untuk mengimplementasikan rancangan sistem yang telah diuraikan pada bab sebelumnya. Implemnetasi sistem merupakan tahap akhir dari membuat sebuah sistem, diamana kegiatan implementasi meliputi implemnetasi antar muka sistem yang akan diterapkan pada *user* untuk kemudian diuji coba hingga diperoleh hasil yang sesuai diharapkan. Adapun hasil yang peneliti peroleh tersebut berupa tampilan hasil program dan hasil pengujian sistem.

1. Tampilan Menu Login

   Tampilan sistem menu login dapat dilihat pada gambar 9.

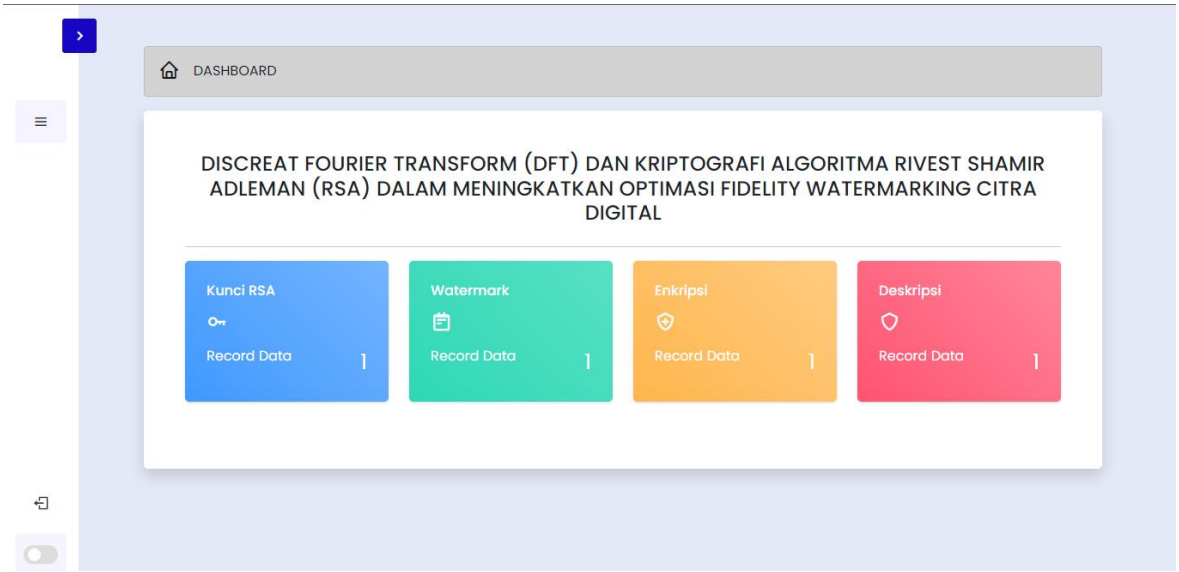


Gambar 9. Tampilan Menu Login

Berdasarkan gambar 9 menampilkan sebuah antarmuka *login* sederhana. Terdapat dua kolom *input* yang memungkinkan pengguna memasukkan *Username* dan *Password*. Di bawah kolom tersebut, terdapat kotak centang bertuliskan *Remember me*, yang berfungsi untuk mengingat informasi *login* pengguna di masa mendatang. Di bagian paling bawah, terdapat tombol *login* berwarna biru tua yang dapat diklik untuk masuk ke sistem atau aplikasi. Desain ini memberikan pengalaman login yang mudah dan intuitif bagi pengguna

2. Tampilan Menu Dashboard

   Tampilan sistem menu dashboard dapat dilihat pada gambar 10.

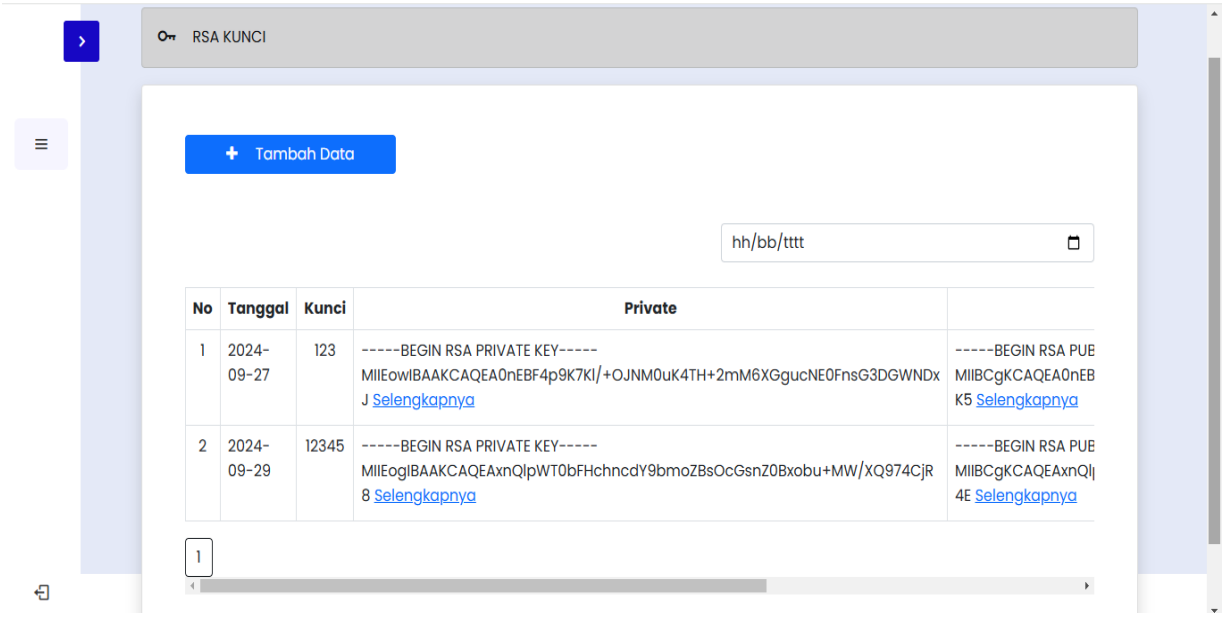


Gambar 10. Tampilan Menu Dashboard

Gambar 10 menampilkan antarmuka dashboard dari sistem menggunakan *Discrete Fourier Transform* (DFT) dan kriptografi *Rivest Shamir Adleman* (RSA) untuk optimasi watermarking citra digital. Terdapat empat fitur utama yang ditampilkan, yaitu Kunci RSA, Watermark, Enkripsi, dan Deskripsi, masing-masing dengan satu data yang dapat diakses. Desainnya sederhana dan berfokus pada pengelolaan data terkait watermarking dan enkripsi.

Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad

3. Tampilan Kunci RSA
Tampilan sistem Kunci RSA dapat dilihat pada gambar 11.



Gambar 11. Tampilan Kunci RSA

Gambar 11 menampilkan halaman RSA Kunci yang berisi daftar kunci RSA yang tersimpan. Terdapat tombol Tambah Data berwarna biru untuk menambahkan kunci baru, serta tabel yang menampilkan detail kunci, termasuk kolom tanggal, jenis kunci, dan kunci RSA pribadi serta publik. Pengguna dapat melihat rincian kunci dengan klik "Selengkapnya" yang tersedia di setiap baris

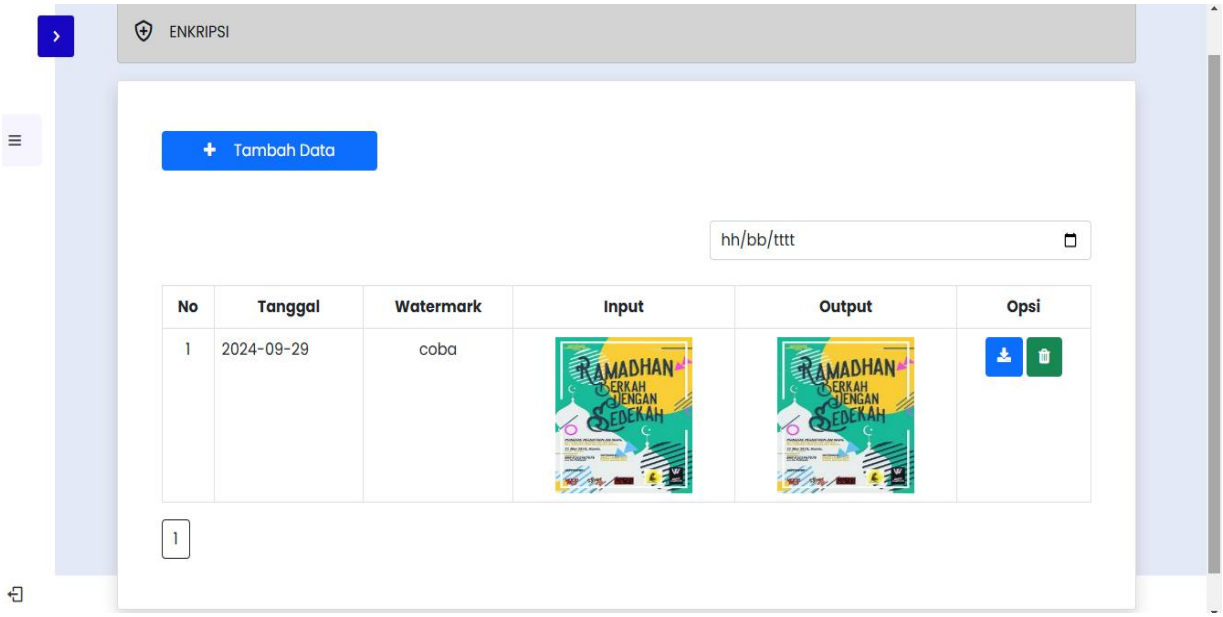
4. Tampilan Watermark
Tampilan sistem data watermark dapat dilihat pada gambar 12.

Gambar 12. Tampilan Watermark

Gambar 12 menampilkan halaman Watermark yang berisi daftar data watermark yang tersimpan. Terdapat tombol Tambah Data berwarna biru untuk menambahkan watermark baru, serta tabel yang menunjukkan informasi tanggal, nama watermark, dan detail watermark yang dienkripsi. Data yang ditampilkan saat ini memiliki satu entri dengan watermark.

5. Tampilan Enkripsi
Tampilan sistem data enkripsi dapat dilihat pada gambar 13.

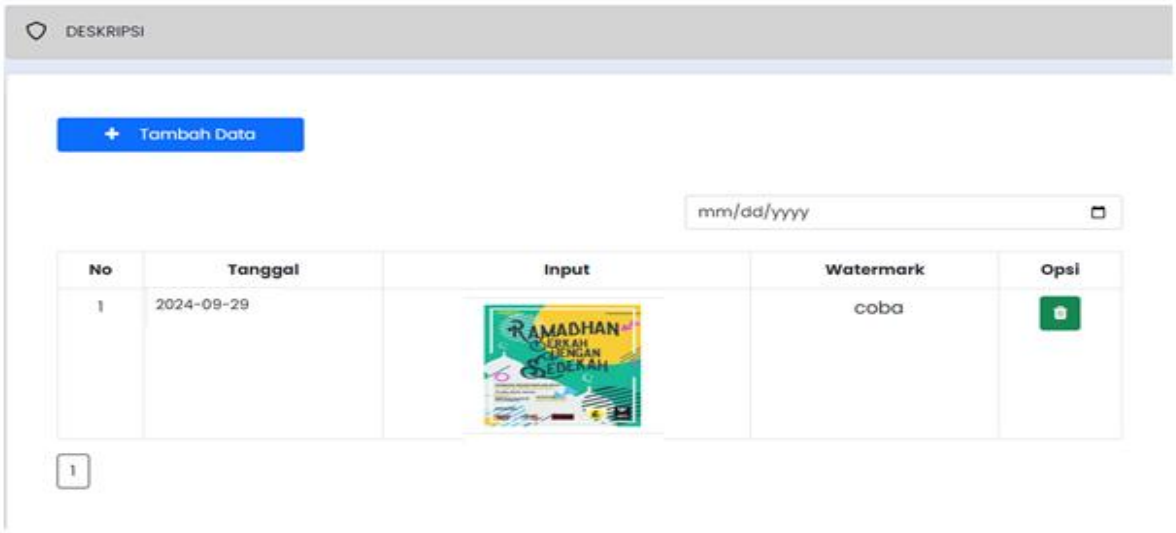
Prosiding Seminar Nasional Teknologi Inovasi dan Kolaborasi Disiplin Ilmu
Vol 1, No 1, Oktober 2024, Hal 244-255
ISSN 3090-3505 (Media Online)
Website https://journal.fkpt.org/index.php/sinekad



Gambar 13. Tampilan Enkripsi

Gambar 13 menunjukkan halaman Enkripsi yang menampilkan daftar hasil proses watermarking pada citra. Terdapat satu entri dengan watermark yang dilakukan. Tabel menampilkan gambar asli pada kolom Input dan gambar hasil watermarking pada kolom Output. Selain itu, terdapat opsi untuk mengunduh atau menghapus data tersebut dengan tombol yang disediakan

6. Tampilan Deskripsi
Tampilan sistem data deskripsi dapat dilihat pada gambar 14.



Gambar 14. Tampilan Deskripsi

Gambar 14 menampilkan halaman Deskripsi yang berisi satu entri data. Tabel tersebut mencakup kolom Tanggal, Input berupa gambar, Watermark, serta opsi untuk menghapus data dengan tombol berwarna hijau. Pengguna juga dapat menambah data baru melalui tombol Tambah Data yang terletak di bagian atas halaman.

3.5 Pembahasan

Setiap sistem memiliki kelebihan dan kekurangan, berikut ini adalah kelebihan dan kekurangan sistem yang telah dibuat.

1. Kelebihan Sistem
Kelebihan sistem ini diantaranya yaitu :
   a. Sistem menampilkan tata letak yang sederhana dengan tombol-tombol aksi yang jelas, memudahkan pengguna untuk memahami fungsi dari setiap fitur.

b. Data seperti kunci RSA, watermark, dan enkripsi diatur dengan baik dalam tabel yang mudah dibaca, membantu pengguna untuk mengelola dan mengakses informasi dengan efisien.
c. Setiap entri data dilengkapi dengan opsi seperti menambah, mengunduh, atau menghapus, memberikan fleksibilitas penuh kepada pengguna dalam mengelola data.

2. Kekurangan Sistem
Adapun kekurangan sistem yang telah dibuat diantaranya yaitu :\
a. Sistem tidak menampilkan adanya mekanisme keamanan tambahan seperti autentikasi dua faktor (2FA) atau enkripsi data di sisi antarmuka, yang dapat meningkatkan perlindungan data pengguna.
b. Sistem ini terlihat fokus hanya pada pengelolaan watermark dan enkripsi, sehingga kurang fleksibel untuk penggunaan lebih luas yang mungkin melibatkan jenis data atau proses lain
c. Desain visual sistem tampak statis, dengan sedikit elemen interaktif atau animasi yang dapat meningkatkan pengalaman pengguna secara keseluruhan

4. KESIMPULAN

Bedasarkan penelitian yang mengulas sistem yang dirancang. Maka terdapat beberapa kesimpulan mengenai sistem yang dirancang. Adapun kesimpulannya sebagai berikut :

1. Sistem ini berhasil menyediakan fitur dasar yang dibutuhkan untuk mengelola kunci RSA, watermark, dan enkripsi citra dengan tampilan antarmuka yang sederhana dan mudah digunakan.
2. Setiap data yang dikelola oleh sistem, seperti tanggal, kunci RSA, watermark, dan gambar, diatur dalam format tabel yang terstruktur, memudahkan pengguna dalam mengakses informasi.
3. Sistem ini masih memiliki keterbatasan dalam hal keamanan dan jenis data yang dapat dikelola, membuatnya lebih cocok untuk penggunaan yang spesifik pada pengelolaan watermark dan enkripsi

REFERENCES

Ariyanto, Y., Ardiansyah, R., & Paris, B. (2018). Steganografi Menggunakan Metode Discrete Fourier Transform (DFT). *Jurnal Informatika Polinema*, *4*(2), 87. https://doi.org/10.33795/jip.v4i2.151

Azhar, J. K., & Yuliany, S. (2019). *Implementasi Algoritma RSA (Rivest , Shamir dan*. *December*.

Dairi, M. S., Setiani Asih, M., & author, corespondent. (2022). Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaaan Implementation Of RSA Cryptographic Algorithms in Library Information System Applications. *Januari*, *2023*(2), 214–223. https://jurnal.unity-academy.sch.id/index.php/jirsi/index%0Ahttp://creativecommons.org/licenses/by-sa/4.0/

Elawati, Hayati, R., & Hanafi. (2022). Analisis Perbandingan Metode Descrete Fourier Transform Dan Metode Descrete Cosine Transform Pada Teknik Menyembunyikan Sinyal Suara. *Jurnal Tektro*, *6*(2), 74.

Gani, S., & Setiyono, B. (2019). Teknik Invisible Watermarking Digital Menggunakan Metode DWT (Discrete Wavelet Tarnsform). *Jurnal Sains Dan Seni ITS*, *7*(2). https://doi.org/10.12962/j23373520.v7i2.29845

HR, A. H., Khudzaifah, M., & Jauhari, M. N. (2021). Implementasi Fungsi Hash MD5 dan Kriptografi Algoritma RSA pada Pembuatan Tanda Tangan Digital. *Jurnal Riset Mahasiswa Matematika*, *1*(2), 51–63. https://doi.org/10.18860/jrmm.v1i2.13992

Khairani, M, & Nurwulan, N. (2018). Algoritma Blowfish Pada Watermarking Video Digital. *JURIKOM (Jurnal …*, *5*(4), 357–361. http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/842

Khairani, Mufida, Harahap, H., Siregar, Y. S., & Lubis, Y. F. A. (2022). Implementation Of Discrete Cosine Transform (DCT) And Blowfish Methods In Digital Video Security. *Sinkron : Jurnal Dan Penelitian Teknik Informatika*, *7*(1), 232–242.

Mido, A. R., & Ujianto, E. I. H. (2022). Analisis Pengaruh Citra Terhadap Kombinasi Kriptografi RSA dan STEGANOGRAFi LSB. *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *9*(2), 279. https://doi.org/10.25126/jtiik.2022914852

Rahmatsyah, I., Sari Siregar, Y., & Khairunnisa. (2024). Proteksi Keamanan Data dengan Menerapkan Algoritma Bacon Cipher dan ROT128. *Journal of Computer Science and Information Technology*, *4*(1), 34–41. https://journal.fkpt.org/index.php/Explorer/article/view/1099

Ramadhani, R., Siregar, D., & Siregar, Y. S. (2018). Implementasi Steganografi Menggunakan Algoritma Diversity Pada Citra Digital. *Jurnal Teknologi Dan Ilmu Komputer Prima (JUTIKOMP)*, *1*(1), 102–114. https://doi.org/10.34012/jutikomp.v1i1.337

Rizki, M., & Ariyani, P. F. (2021). Penerapan Kriptografi Dengan Menggunakan Algoritma Rsa Untuk Pengamanan Data Berbasis Desktop Pada Pt Trias Mitra Jaya Manunggal. *Skanika*, *4*(2), 1–6. https://doi.org/10.36080/skanika.v4i2.1991

Setyansyah, R., Siregar, Y. S., & Khairani, M. (2019). Noise Removal Pada Citra Digital Dengan Menggunakan Metode Active Contour. *ALGORITMA: Jurnal Ilmu Komputer Dan Informatika*, *5*(1), 978–979. http://www.seminar.ilkom.unsri.ac.id/index.php/ars/article/view/2130

Solikhin, M., Pratama, Y., Pasaribu, P., Rumahorbo, J., & Simanullang, B. (2022). Analisis Watermarking Menggunakan Metode Discrete Cosine Transform (DCT) dan Discrete Fourier Transform (DFT). *Jurnal Sistem Cerdas*, *5*(3), 155–170. https://doi.org/10.37396/jsc.v5i3.192

Sutejo. (2021). Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien. *INTECOMS: Journal of Information Technology and Computer Science*, *4*(1), 104–114. https://doi.org/10.31539/intecoms.v4i1.2437

Umar, F., & Darwis, H. (2019). Watermarking Citra Digital Berwarna Menggunakan Stationary Wavelet Transform (Swt). *ILKOM Jurnal Ilmiah*, *11*(1), 1–10. https://doi.org/10.33096/ilkom.v11i1.409.1-10

Wahyuningsih, S., Pandex, T. V. D., & Stefanny, V. (2017). Implementasi Visible Watermarking Dan Steganografi Least Significant Bit Pada File Citra Digital. *Jurnal TELEMATIKA MKOM*, *8*(2), 140–145.