Perancangan Sistem Steganografi Berbasis Transformasi Wavelet Diskrit Terintegrasi Algoritma Rijndael dan QR-Code

I Putu Rizky Pratama Putra[a1], Gst. Ayu Vida Mastrika Giri[a2],

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam,
Universitas Udayana
Jalan Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung, Bali, Indonesia
[1]puturizky098@email.com
[2]vida@unud.ac.id

Abstract

The advancement of technology has been the primary driving force behind the transformative shifts across various domains of human life, spanning from the era of industrial revolution to the present digital age. Within the digital epoch, the pivotal role of information and communication technology in shaping the global societal framework is unequivocal. Nonetheless, the rapid progression of technology introduces novel challenges such as safeguarding personal data integrity and combating unauthorized access to individual information. Addressing these challenges entails the adoption of sophisticated techniques, including compression methodologies like Discrete Wavelet Transform (DWT), renowned for its efficacy in multimedia data compression with high rates. Furthermore, cryptographic algorithms such as Rijndael offer viable solutions to enhance data security through a series of encryption operations, encompassing substitution, permutation, and iterative rounds applied to each block. The amalgamation of DWT and Rijndael culminates in data representation via QR codes. Additionally, this research encompasses the development of a user interface design to facilitate the seamless implementation and utilization of the system, ultimately aiming to fortify data security effectively.

Keywords: *Discrete Wavelet Transform, multimedia data, Rijndael algorithm, QR-code, user interface*

1. Pendahuluan

Teknologi telah menjadi pendorong utama perubahan dalam berbagai aspek kehidupan manusia, mulai dari era revolusi industri hingga era digital. Di era digital ini, teknologi informasi dan komunikasi memainkan peran kunci dalam membentuk struktur masyarakat global[1]. Namun, seiring dengan kemajuan yang pesat, teknologi juga membawa tantangan baru, seperti kasus pencurian data pribadi atau akses ilegal terhadap informasi seseorang. Dalam konteks di mana pesan sensitif perlu dikomunikasikan melalui saluran yang mungkin rentan terhadap pemantauan atau penyadapan, distribusi dokumen rahasia, atau akses terhadap data sensitif di jaringan, konten digital dapat mengalami perubahan atau pembajakan secara illegal. Untuk mengatasi tantangan tersebut, diperlukan penerapan teknik khusus, salah satunya adalah steganografi. Steganografi merupakan metode untuk menyisipkan pesan ke dalam media data multimedia dengan tujuan mengelabui pihak yang ingin mencuri data atau pesan. Salah satu metode yang sering dibahas dalam penelitian adalah metode LSB (Least Significant Bit), yang menyisipkan pesan ke dalam piksel-piksel dengan hasil uji coba menunjukkan efektivitasnya dalam penyisipan pesan atau data dan menjaga hasilnya menyerupai bentuk aslinya. Kelebihan metode ini adalah proses penyisipan dan ekstraksi yang cepat, serta citra sebelum dan sesudah penyisipan pesan memiliki resolusi yang sama, dan ukuran citra asli dan citra berisi pesan sama. Namun, metode ini juga memiliki beberapa kelemahan yang signifikan, seperti tingkat ketahanan pesan terhadap perubahan kontras citra yang buruk, rentan terhadap pemrosesan gambar seperti pemotongan dan kompresi, serta kapasitas pesan yang terbatas [2]. Dikarenakan pengamanan data atau pesan tidak hanya berfokus pada pengelabuan pesan saja, tetapi juga pada keamanan pesan

tersebut dari serangan, solusi yang dapat digunakan adalah metode Discrete Wavelet Transform (DWT). Metode ini memiliki keunggulan dalam mengamankan pesan atau file yang disembunyikan dengan memiliki nilai PSNR (Peak Signal-to-Noise Ratio) yang tinggi, sehingga citra hasil steganografi dapat menyerupai citra aslinya. Selain itu, metode ini juga memiliki keamanan yang baik dan cocok untuk menyisipkan pesan dengan kapasitas besar. Dengan menggabungkan steganografi dengan kriptografi, dan menggunakan QR-code sebagai media penyimpanan hasil dari kombinasi tersebut, diharapkan dapat meningkatkan performa keamanan. Kriptografi digunakan untuk mengenkripsi pesan sehingga hanya penerima yang sah yang dapat membacanya. Penggunaan QR-code juga dapat meningkatkan keamanan karena memiliki tingkat keamanan yang cukup tinggi [2]. Salah satu algoritma kriptografi yang umum digunakan adalah Algoritma Rijndael, yang menggunakan teknik substitusi dan permutasi dalam beberapa putaran. Dengan demikian, perancangan teknologi ini diharapkan dapat memberikan informasi yang lebih terkait dengan metode yang telah digunakan sebelumnya serta dapat diimplementasikan di masa yang akan datang untuk menjaga kerahasiaan pesan dan data yang bersifat pribadi dengan lebih efektif [3].

2. Metode Penelitian

2.1. Pengumpulan Data

Metode pengumpulan data merujuk pada pendekatan atau teknik yang digunakan untuk mengumpulkan informasi atau data dalam sebuah penelitian atau studi. Dalam penelitian ini, metode yang diterapkan adalah pengumpulan data secara kualitatif melalui studi literatur. Pengumpulan data dilakukan dengan mencari sumber-sumber dari berbagai referensi, seperti buku, jurnal, dan riset yang relevan. Bahan pustaka yang diperoleh dari berbagai sumber tersebut kemudian dianalisis secara kritis dan mendalam guna mendukung proposisi dan gagasan yang diusulkan.

2.2. Metode *Discrete Wavelet Transform* (DWT)

Discrete Wavelet Transform (DWT) adalah metode kompresi gambar yang memiliki tingkat kompresi tinggi. DWT membagi sinyal menjadi bagian frekuensi tinggi dan rendah, di mana bagian frekuensi tinggi berisi informasi tentang komponen yang mencolok, sementara bagian frekuensi rendah berisi informasi lebih halus. Dalam proses kompresi, DWT membagi gambar menjadi sub-image yang lebih kecil, dengan sub-image frekuensi tinggi mengandung informasi yang mencolok, dan sub-image frekuensi rendah mengandung informasi halus. DWT juga digunakan dalam audio dan video steganografi untuk menyisipkan data ke dalam koefisien *wavelet* [4].

(a) (b)

Gambar 1. Perbedaan bentuk *wavelet* (a) dan *wave* (gelombang) (b)

Persamaan umum untuk Transformasi Gelombang Diskrit (DWT) dapat ditemukan dalam formulasi berikut:

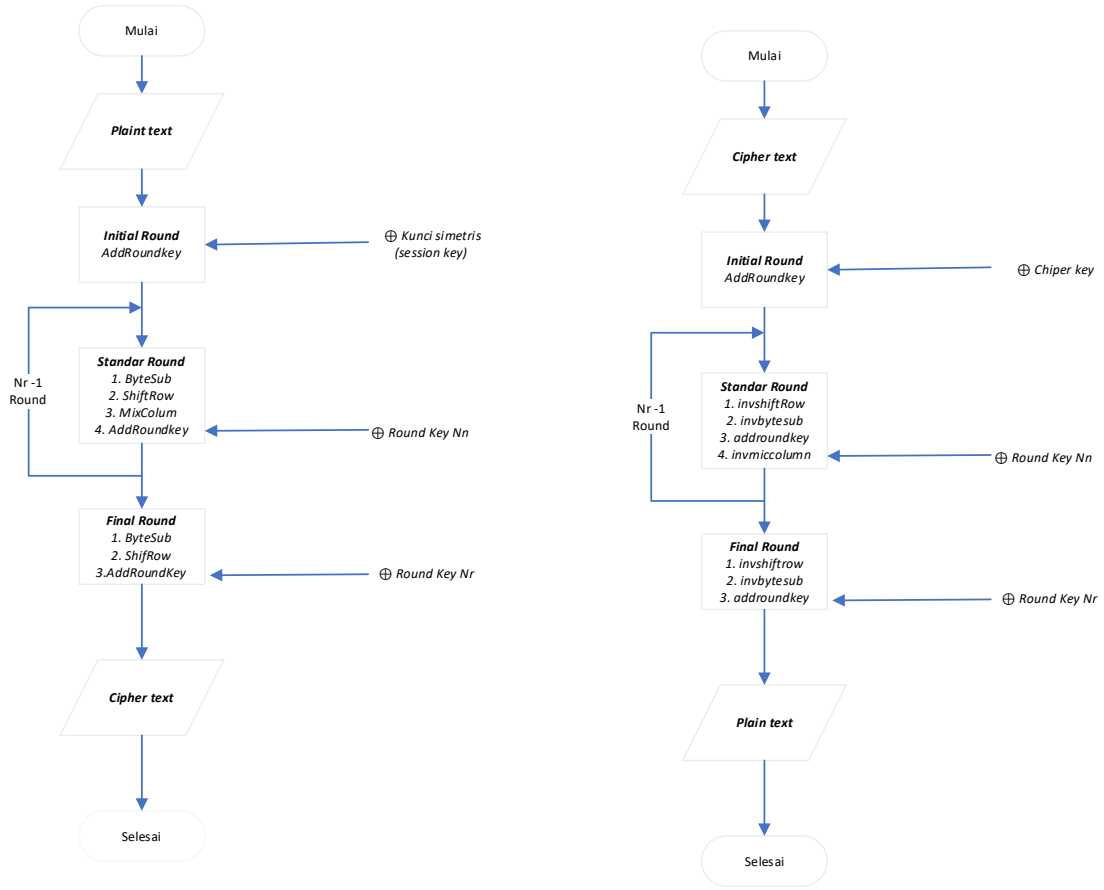
$$\text{DWT}\ \{f(t)\} = W_{\emptyset}\ (j_{\emptyset}, k) + W_{\emptyset}\ (j, k) \quad (1)$$

Di mana (f(t)) merupakan fungsi sinyal, *j* dan *k* merupakan indeks yang mengontrol skala dan posisi, dan $W_{\emptyset}$ merupakan koefisien transformasi gelombang untuk level atau resolusi tertentu [2]. Dalam implementasi DWT, sinyal digital dibagi menjadi frekuensi tinggi dan rendah menggunakan highpass filter dan lowpass filter. Dekomposisi DWT level 1 membagi frame menjadi empat frekuensi: Low-low frequency (LL), low-high frequency (LH), high-low frequency (HL), dan high-high frequency (HH). Dalam analisis sinyal DWT, penggunaan filter highpass dan lowpass menghasilkan koefisien detail dan koefisien aproksimasi [5].

p-ISSN: 2986-3929
e-ISSN: 3032-1948

2.3. Algoritma Kriptografi *Rijndael*

Rijndael, sebuah algoritma kriptografi kunci simetris dalam kategori block cipher, dikembangkan oleh Vincent Rijmen dan John Daemen sebagai respons terhadap kompetisi algoritma pengganti DES yang diadakan oleh National Institute of Technology (NIST)[6]. Rijndael terpilih sebagai pemenang kompetisi tersebut, dan kemudian dikenal sebagai Advanced Encryption Standard (AES). Algoritma ini menerapkan operasi substitusi, permutasi, dan serangkaian putaran pada setiap blok yang akan dienkripsi, dengan menggunakan kunci yang berbeda pada setiap putaran, yang disebut sebagai round key. Rijndael mendukung panjang kunci dan ukuran blok dari 128-bit hingga 256-bit dengan kelipatan 32-bit. Sebagai block cipher, Rijndael dapat dioperasikan dalam berbagai mode operasi, termasuk ECB, CBC, dan CFB. Rijndael beroperasi pada orientasi byte, di mana setiap elemen array state diisi dengan 8-bit teks dalam notasi HEX. Ukuran blok dan panjang kunci yang digunakan mempengaruhi jumlah putaran yang terjadi pada proses enkripsi dan dekripsi. Algoritma ini memiliki tiga parameter utama: Plaintext, Ciphertext, dan Key, yang masing-masing berukuran 16 byte[7] .



Gambar 1. Enkripsi dan Dekripsi Algoritma *Rijndael*

Cara kerja enkripsi:

a. Key Expansion: Ekspansi kunci dilakukan sesuai dengan panjang kunci dan ukuran blok yang digunakan, menghasilkan Roundkey.

b. Addroundkey: Melakukan XOR antara state awal (plaintext) dengan kunci utama pada tahap awal, dan dengan hasil ekspansi kunci pada putaran berikutnya.

c. Putaran (Nr) sebanyak Nr-1: Setiap putaran terdiri dari beberapa tahapan:

- Sub Bytes: Melakukan substitusi menggunakan tabel S-box.
- ShiftRows: Menggeser baris array state sesuai aturan tertentu.
- MixColumns: Mengacak data dalam kolom array state menggunakan operasi matriks.
- Addround key: Melakukan XOR antara array state sebelumnya dengan round key.

d. Putaran Akhir (Final round): Terdiri dari tahapan SubBytes, ShiftRows, dan AddRoundKey.

Cara kerja dekripsi:

a. Key Expansion: Dilakukan ekspansi kunci untuk dekripsi.
b. AddRoundKey: Proses XOR antara state awal (ciphertext) dengan kunci terakhir hasil ekspansi.
c. Putaran (Nr) sebanyak Nr-1: Setiap putaran terdiri dari beberapa tahapan, seperti InvShiftRow, InvByteSub, AddRoundKey, dan InvMixColumn.
d. Putaran Akhir (Final round): Terdiri dari tahapan InvShiftRow, InvSubByte, dan AddRoundKey.

2.4. QR-Code

Kode QR adalah kode batang dua dimensi yang mampu mengkodekan berbagai jenis data, seperti biner, numerik, dan alfanumerik, dalam bentuk citra digital. Penggunaan kode QR sebagai media penyimpanan data semakin meningkat seiring dengan popularitas perangkat mobile yang dilengkapi kamera dan koneksi internet. Untuk mengakses informasi dalam kode QR, pengguna perlu memindai kode tersebut menggunakan pemindai tertentu, seperti kamera pada smartphone. Proses pemindaian kode QR dapat dilakukan dengan cepat karena struktur kode QR memiliki elemen yang memberikan referensi pada kamera terkait orientasi objek, sehingga informasi dapat diterjemahkan oleh kamera meskipun sudut pembacaan objek dua dimensi kurang optimal [3].

2.5. Analisis dan Perencanaan Sistem

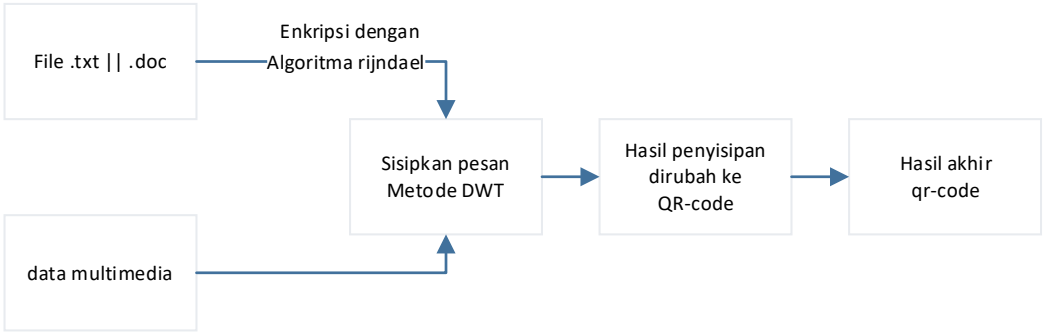
Permasalahan yang terkait dengan aplikasi steganografi untuk penyisipan pesan adalah integrasi pesan ke dalam data multimedia. Penyisipan pesan dilakukan dengan menyematkannya ke dalam kolom yang telah ditentukan. Dalam pengumpulan data, pendekatan studi pustaka digunakan, di mana informasi diperoleh dari sumber-sumber seperti buku teks, jurnal ilmiah, dan sumber informasi di internet yang relevan dengan perancangan steganografi tersebut. Pada tahap ini, sistem akan dikembangkan menggunakan diagram alir atau flowchart untuk merancang arsitektur keseluruhan. Selain itu, perancangan antarmuka pengguna akan dibuat untuk memastikan interaksi yang intuitif dan efektif bagi pengguna.

3. Hasil dan Diskusi

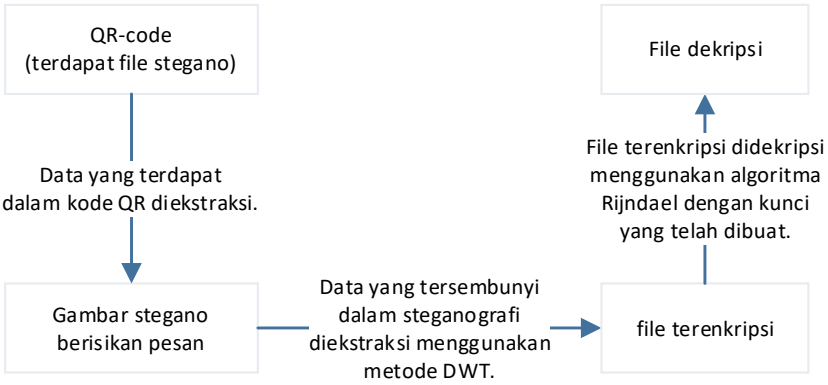
3.1. Arsitektur Sistem

Arsitektur sistem yang digunakan dalam penelitian ini melibatkan serangkaian tahapan. Tahap pertama melibatkan penyisipan pesan ke dalam data multimedia menggunakan metode *Discrete Wavelet Transform* (DWT) dengan algoritma *Rijndael*. Setelah itu, pesan dienkripsi dengan algoritma *Rijndael* sebelum disisipkan ke dalam data multimedia menggunakan metode DWT. Hasil dari proses penyisipan tersebut kemudian diubah menjadi *QR-code*. Untuk mengembalikan pesan, hasil akhir dalam bentuk *QR-code* dapat didekripsi dengan menggunakan dekoder yang sesuai. Diagram blok sistem secara umum dari arsitektur sistem pada proses penyisipan pesan dapat dilihat pada Gambar 1 dan 2.

p-ISSN: 2986-3929
e-ISSN: 3032-1948

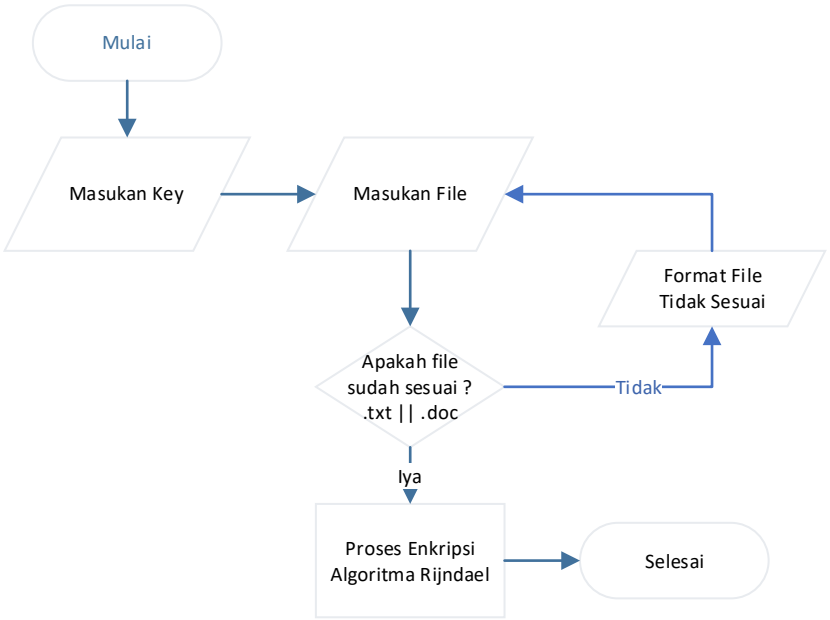


Gambar 1. Enkripsi Penyisipan Pesan



Gambar 2. Deskripsi penyisipan pesan

a. Diagram alir untuk proses enkripsi pesan.
Dalam sistem enkripsi yang menggunakan algoritma *Rijndael*, pengguna akan memasukkan pesan dalam bentuk berkas .txt atau .doc ke dalam sistem. Sistem akan memulai proses enkripsi pada pesan tersebut sesuai dengan algoritma *Rijndael*, dengan menggunakan kunci untuk melaksanakan proses enkripsi. Informasi lebih lanjut mengenai implementasi ini dapat dijelaskan secara rincian dalam Gambar 3.



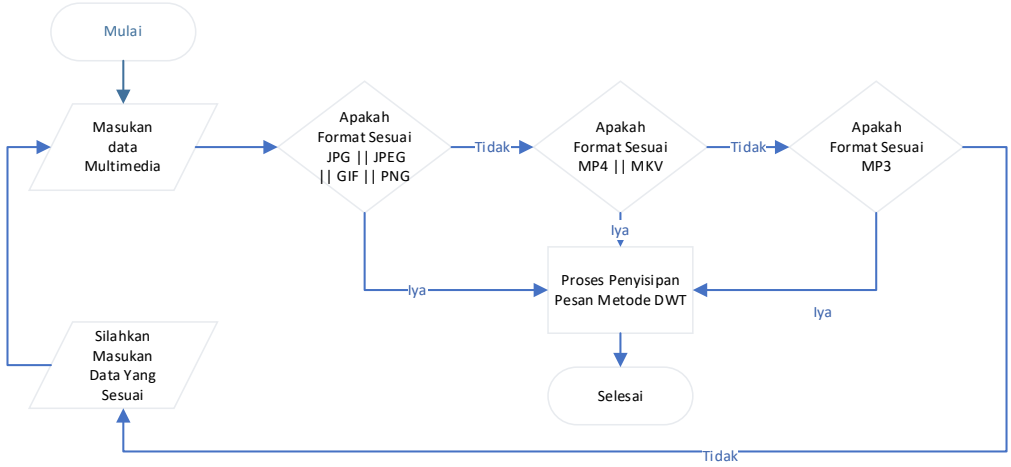
Gambar 3. Diagram alir proses enkripsi pesan

p-ISSN: 2986-3929
e-ISSN: 3032-1948

Penjelasan diagram alir proses enkripsi pesan:

- Inisiasi Program dan Permintaan Masukan File: Program dimulai dengan menyajikan pesan kepada pengguna untuk memasukkan file yang akan dienkripsi. Format file yang diterima dapat berupa. file atau .text.
- Pengguna Memasukkan Kunci *(Key)*: Pengguna diminta untuk memasukkan kunci *(key)* yang akan digunakan dalam proses enkripsi. Kunci ini harus disimpan secara rahasia dan memiliki tingkat kekuatan yang memadai untuk meningkatkan keamanan proses enkripsi.
- Kesesuaian File: Program menampilkan pesan konfirmasi kepada pengguna, meminta pengguna untuk memastikan apakah file yang akan dienkripsi sudah sesuai.
- Proses Enkripsi dengan Algoritma *Rijndael*: Program menggunakan algoritma *Rijndael* untuk melakukan proses enkripsi terhadap file yang dimasukkan, dengan menggunakan kunci yang telah diberikan. Proses ini melibatkan beberapa tahapan, termasuk pengaturan blok data, penggunaan kunci untuk substitusi dan permutasi, serta iterasi putaran enkripsi. Algoritma *Rijndael* mentransformasi blok data asli menjadi blok data terenkripsi, dan proses ini diulang hingga seluruh file terenkripsi.

b. Diagram alir untuk proses penyisipan pesan.
Dalam sistem penyisipan pesan, output dari enkripsi pesan akan disematkan ke dalam salah satu media data multimedia menggunakan metode *Discrete Wavelet Transform* (DWT). Informasi lebih lanjut mengenai implementasi ini dapat dijelaskan secara rinci dalam Gambar 4.



Gambar 4. diagram alir proses penyisipan pesan

Penjelasan diagram alir proses penyisipan pesan:

- Masukan Data Multimedia: Pengguna diminta untuk memasukkan data multimedia, seperti gambar, video atau audio, yang akan digunakan sebagai media penyisipan.
- Kesesuaian File: Program akan menghasilkan pesan kesalahan yang ditampilkan kepada pengguna, mengajukan permintaan agar pengguna memastikan kelayakan file yang akan digunakan, apabila terdeteksi adanya kesalahan dalam proses tersebut.
- Penyisipan Pesan Menggunakan Metode DWT: Data multimedia yang dipilih sebagai media penyisipan akan diubah ke dalam domain *wavelet* menggunakan metode DWT.

    - DWT pada Gambar: Pada gambar, biasanya terdiri dari dua dimensi, yaitu tinggi dan lebar (x dan y). Proses DWT pada gambar akan membagi gambar menjadi beberapa level resolusi yang berbeda. Proses dimulai dengan membagi gambar menjadi dua bagian, yaitu bagian detail (informasi tinggi) dan bagian aproksimasi (informasi rendah). Setiap bagian kemudian diubah lagi menjadi dua bagian lagi, dan proses ini berlanjut sampai mencapai level resolusi yang diinginkan. Proses DWT pada gambar dapat

p-ISSN: 2986-3929
e-ISSN: 3032-1948

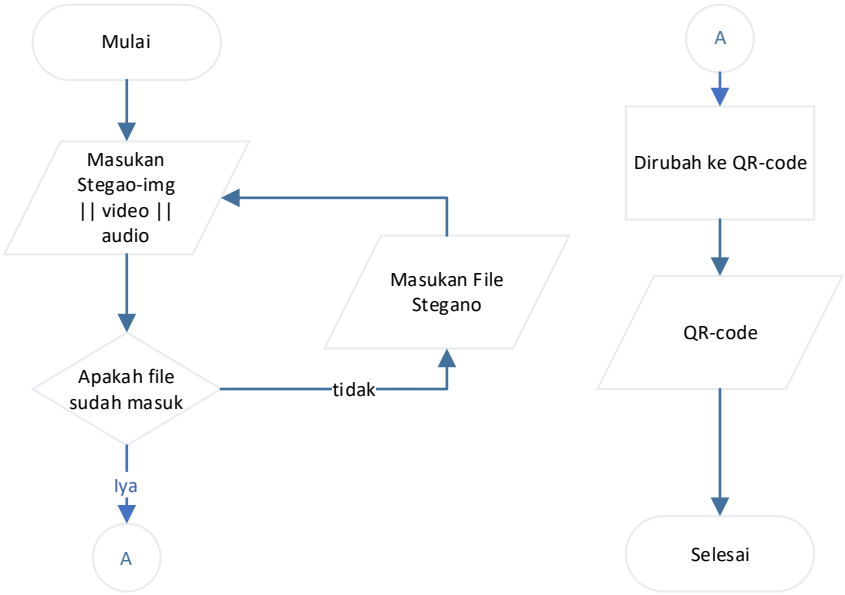
digunakan untuk kompresi gambar dengan mempertahankan informasi penting dalam bentuk detail dan aproksimasi pada berbagai level resolusi.

- DWT pada Video: DWT pada video melibatkan penggunaan DWT pada setiap frame video secara terpisah. Setiap frame video dipecah menjadi dua bagian, detail dan aproksimasi, menggunakan proses yang mirip dengan DWT pada gambar. Hal ini memungkinkan kompresi video dengan mempertahankan detail penting pada setiap frame, sehingga memungkinkan pengurangan ukuran file tanpa kehilangan kualitas video yang signifikan.
- DWT pada Audio: Pada audio, DWT sering digunakan untuk melakukan analisis spektral dan kompresi. Audio sering kali dipecah menjadi rentang frekuensi yang berbeda menggunakan DWT, yang kemudian dapat dianalisis atau diolah lebih lanjut. Proses DWT pada audio memungkinkan pengurangan redundansi informasi dan pemampatan data audio tanpa mengorbankan kualitas audio yang signifikan.

Dalam semua aplikasi ini, DWT memungkinkan representasi sinyal dalam domain frekuensi dan domain waktu secara bersamaan, yang memungkinkan analisis dan pengolahan sinyal yang lebih baik, serta kompresi data dengan efisien.

c. Diagram alir untuk proses memasukkan hasil dari tahap penyisipan dan enkripsi ke dalam *QR-code*.

Dalam sistem terakhir, pesan yang telah dienkripsi dan telah disisipkan ke dalam gambar akan melalui tahap akhir dengan penempatan di dalam *QR-code*. Informasi lebih lanjut mengenai implementasi ini dapat dijelaskan secara rinci dalam Gambar 5.



Gambar 5. Diagram alir proses memasukan hasil kedalam *QR-code*

Penjelasan diagram alir proses memasukan hasil kedalam *QR-code*:

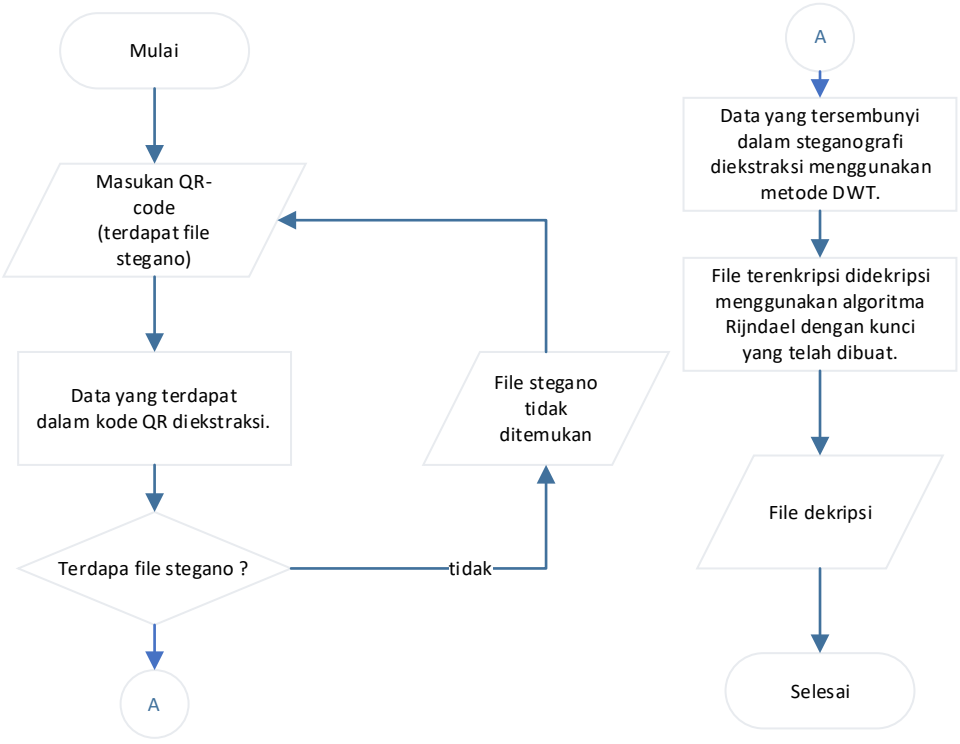
- Masukan file stegano : Pengguna diminta untuk memasukkan file stegano yang sudah dibuat
- Kesesuaian File: Program menampilkan pesan konfirmasi kepada pengguna, meminta pengguna untuk memastikan apakah file yang akan digunakan sudah terinput atau belum.
- Kesesuaian File: Program akan menghasilkan pesan kesalahan yang ditampilkan kepada pengguna, mengajukan permintaan agar pengguna memastikan file stegano yang akan digunakan, apabila terdeteksi adanya kesalahan dalam proses tersebut.

p-ISSN: 2986-3929
e-ISSN: 3032-1948

- Hasil akhir dari proses ini adalah *QR-code* yang mengandung pesan yang telah disisipkan sebelumnya, memungkinkan untuk distribusi atau penyimpanan informasi dengan cara yang tidak mencolok atau terlihat secara langsung.

d. Diagram alir untuk proses dekripsi pesan.

Jika pengguna menginginkan untuk melihat pesan, pesan tersebut akan dideskripsikan dengan memasukkan hasil akhirnya, yaitu QR code. Informasi lebih lanjut mengenai implementasi ini dapat dijelaskan secara rinci dalam Gambar 6.



Gambar 6. Diagram alir proses dekripsi pesan

Penjelasan diagram alir proses dekripsi pesan:

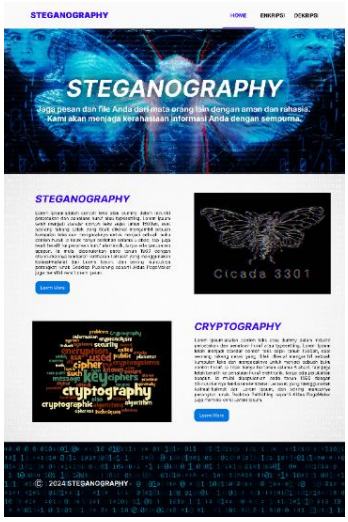
- Masukkan file *QR-code*: Pengguna diminta untuk menyediakan dan memasukkan file *QR-code* yang berisi data steganografi.
- Data yang tertanam dalam kode *QR-code* diekstraksi.
- Pengguna diminta untuk memeriksa keberadaan file stegano. Jika tidak ditemukan, akan muncul pemberitahuan bahwa stegano tidak ditemukan. Namun, jika ada, proses akan dilanjutkan.
- Data yang tersembunyi dalam steganografi diekstraksi menggunakan metode *Discrete Wavelet Transform* (DWT).
- File yang terenkripsi akan didekripsi menggunakan algoritma *Rijndael* dengan kunci yang telah dibuat sebelumnya.
- Setelah proses dekripsi selesai, pesan dalam file dapat dibaca.

3.2. Antarmuka pengguna

a. Tampilan awal

Pada antarmuka awal, terdapat pemaparan mengenai steganografi dan kriptografi, dengan kemungkinan tambahan artikel-artikel yang relevan.

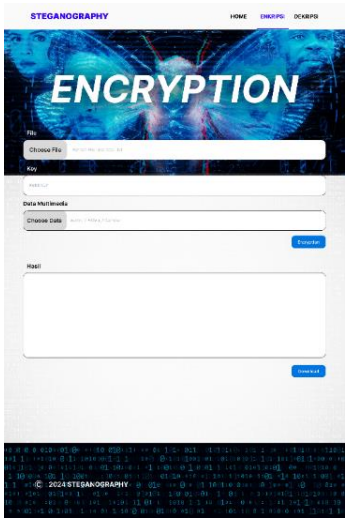
p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 7. Tampilan awal

b. Tampilan enkripsi

Pada antarmuka enkripsi, terdapat sebuah formulir yang memfasilitasi proses enkripsi serta menampilkan hasil enkripsi. Pengguna diminta untuk memasukkan *file* dalam format .txt atau .doc pada bagian yang disediakan untuk *file*, dan memasukkan kunci pada bagian *key* enkripsi. Kunci dapat dibuat dengan berbagai kombinasi angka, huruf, dan simbol. Setelahnya, pengguna dapat mengunggah berbagai jenis data multimedia, seperti video, gambar, atau audio, dan memilih salah satunya setelah semua bidang terisi. Proses enkripsi dimulai dengan menekan tombol *"encryption",* yang akan menghasilkan sebuah *QR-code. QR-code* tersebut menyimpan *file* steganografi, di mana *file* terenkripsi telah terdapat di dalamnya.

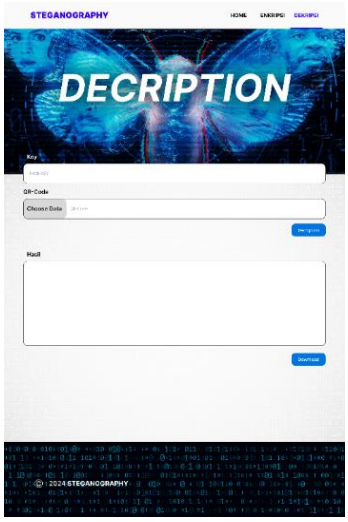


Gambar 8. Tampilan enkripsi

c. Tampilan dekripsi

Pada antarmuka dekripsi, terdapat sebuah formulir yang memfasilitasi proses dekripsi serta menampilkan hasil dekripsi, yakni berupa file yang sebelumnya telah dimasukkan pada tahap enkripsi. Proses dekripsi dilakukan dengan memasukkan kunci yang telah dibuat dan memasukkan *QR-code* yang telah dibuat, yang mengandung informasi tersembunyi (steganografi).

p-ISSN: 2986-3929
e-ISSN: 3032-1948



Gambar 9. Tampilan dekripsi

4. Kesimpulan

Penelitian ini menghasilkan kesimpulan bahwa penerapan steganografi menggunakan metode *Discrete Wavelet Transform* (DWT) bersama dengan algoritma *Rijndael* merupakan salah satu strategi yang dapat diimplementasikan dalam mengamankan pesan rahasia dalam data multimedia. DWT memiliki kemampuan untuk memisahkan sinyal menjadi komponen frekuensi tinggi dan rendah, yang menggambarkan karakteristik yang signifikan dan detail halus dari data tersebut. Di sisi lain, algoritma *Rijndael*, sebagai representasi algoritma simetris, mengandalkan operasi substitusi, permutasi, dan iterasi pada blok yang dienkripsi, dengan penerapan kunci yang berubah pada setiap iterasi, meskipun dalam implementasi praktis, satu kunci tunggal sering digunakan untuk setiap blok enkripsi. Penggunaan *QR-code* sebagai *cover* tempat stegano disimpan diharapkan dapat mengurangi risiko penghapusan tidak disengaja oleh pengguna. Desain antarmuka pengguna yang simpel dirancang untuk memfasilitasi implementasi dan penggunaan sistem ini.

Daftar Pustaka

[1] A. U. Albab and D. Darmaji, “Pengamanan Pesan Menggunakan Kombinasi Kriptografi dan Steganografi Audio Berbasis Transformasi Wavelet Diskrit,” *Jurnal Sains dan Seni ITS*, vol. 11, no. 3, pp. A92–A95, 2023.

[2] A. P. Ratnasari and F. A. Dwiyanto, “Metode steganografi citra digital,” *Sains, Apl. Komputasi dan Teknol. Inf*, vol. 2, no. 2, p. 52, 2020.

[3] Y. Situmeang, A. Situmorang, and P. Lumbanraja, “Implementasi Algoritma AES Rijndael Pada QR Code Untuk Validasi dan Keamanan Data Penerima Bantuan Sosial di Kelurahan Padang Bulan Selayang II,” *METHOTIKA: Jurnal Ilmiah Teknik Informatika*, vol. 3, no. 2, pp. 21–30, 2023.

[4] D. C. Antono, H. N. Palit, and R. Adipranata, “Implementasi Enkripsi AES Cipher dan Discrete Wavelet Transform Dalam Metode Steganografi,” *Jurnal Infra*, vol. 8, no. 1, pp. 285–288, 2020.

[5] A. S. Pratama and I. M. Suartana, “Analisis Kualitas Stego Video dalam Penyisipan Data Memanfaatkan Metode DCT-DWT,” *Journal Information Engineering and Educational Technology) ISSN*, vol. 2549, p. 869X, 2021.

[6] T. Yuniati, “Pengembangan Aplikasi Penyandian Data Menggunakan Algoritma Rijndael,” *Jurnal TIMES*, vol. 11, no. 2, pp. 25–33, 2022.

[7] R. Siringoringo, “Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File,” *Kumpulan Artikel Karya Ilmiah Fakultas Ilmu Komputer*, vol. 2, no. 1, pp. 31–42, 2020.