InComTech: Jurnal Telekomunikasi dan Komputer
InComTech: Jurnal
vol.13, no.1, April 2023, 28-39
http://publikasi.mercubuana.ac.id/index.php/Incomtech
P-ISSN: 2085-4811 E-ISSN: 2579-6089

Enkripsi Data Teks Dengan AES dan Steganografi DWT

Chaerul Umam*, Muslih

Teknik Informatika, Universitas Dian Nuswantoro,
Jl. Imam Bonjol 207, Semarang 50131, Indonesia
*chaerul@dsn.dinus.ac.id

Abstrak :
Pertukaran data melalui internet rawan akan adanya pencurian informasi. Maka dari itu, sebagai upaya pencegahan terjadinya hal itu diperlukan sebuah sistem keamanan. Terdapat berbagai macam usaha perlindungan suatu data, misalnya dengan menggunakan teknik kriptografi dan steganografi. Pada penelitian ini, membahas bagaimana hasil data teks yang telah dienkripsi menggunakan algoritma Advanced Encryption Standard (AES) 128-Bit dilanjutkan dengan teknik steganografi pada sebuah citra menggunakan algoritma Discrete Wavelet Transform (DWT). Kemudian data hasil percobaan dianalisis kualitasnya menggunakan parameter Mean Signal Error (MSE) dan Peak- to-peak Signal to Noise Ratio (PSNR) sebagai alat ukurnya. Pada percobaan ini kualitas gambar stego menggunakan DWT tergolong cukup baik dengan menghasilkan nilai MSE 0.16-0.26 dB dan nilai PSNR nya 46.27-52.2 dB

Keywords:
Kriptografi;
Advanced Encryption Standard;
Steganografi;
Discerete Cosine Transform;
Imperceptibility;

Riwayat Artikel*:*
Diserahkan 04 Maret 2022
Direvisi 07 September 2022
Diterima 01 Februari 2023
Dipublikasi 30 April 2023

DOI:
10.22441/incomtech.v13i1.15059

1. PENDAHULUAN

Informasi telah menjadi salah satu perihal penting yang mempengaruhi kehidupan manusia. Media pertukaran informasi dapat mempermudah sekaligus mempercepat pertukaran informasi yang diinginkan, namun di sisi lain informasi bisa menjadi suatu ancaman yang membahayakan. Apabila pertukaran informasi tersebut dilakukan tanpa adanya pengamanan data yang ketat, maka data tersebut dapat dicuri oleh orang – orang yang tidak bertanggungjawab. Terdapat berbagai macam usaha perlindungan suatu data, misalnya dengan menggunakan teknik kriptografi [1], [2] dan steganografi [3], [4]. Proses menyembunyikan informasi ke dalam sebuah wadah pembawa dinamakan teknik steganografi, selain itu juga dapat ditambahkan teknik kriptografi untuk dilakukan pengacakan informasi dengan kunci tertentu sehingga informasi tidak diketahui artinya [5]. Pada dasarnya kriptografi terdiri dari dua proses, meliputi proses enkripsi dan proses dekripsi. Adalah proses mentransformasi pesan asli (plaintext) ke

dalam wujud pesan tersandi (ciphertext) disebut proses enkripsi [6].

Dalam penelitian ini, data teks yang digunakan dalam format *.txt yang akan dienkripsi menggunakan algoritma Advance Encryption Standard (AES). Algoritma tersebut adalah algoritma yang mampu digunakan sebagai metode mengamankan data informasi. Pada algoritma AES melakukan enkripsi (encryption) dan dekripsi (decryption) terhadap informasi menggunakan blockciphertext simetris [7]. Dimana proses enkripsi mengubah data yang tidak lagi bisa diartikan maknanya disebut ciphertext, berbanding terbalik dengan dekripsi prosesnya mengubah ciphertext kembali ke sebuah plaintext yaitu pesan/data bentuk semula. Algoritma AES menggunakan berbagai kunci kriptografi, diantaranya yaitu 128-bit, 192-bit, dan 256-bit [8]. Penulis memilih Algoritma Advanced Encryption Standard (AES) karena bit pada algoritma AES berorientasi pada cipher yang dihasilkan, sehingga implementasi algoritma ini memungkinkan untuk memperoleh hasil yang efisien terhadap perangkat lunak dan keras. Algoritma AES juga diunggulkan dalam kesolidan kode, kesederhanaan rancangan yang cepat dan sederhana dibanyak platform. Pada penelitian ini, peneliti menerapkan algoritma AES dengan kunci kriptografi 128 bit.

Hasil dari proses enkripsi (ciphertext) akan menghasilkan teks baru yang tidak dapat diterjemahkan informasinya. Hal ini akan menimbulkan kecurigaan bagi pihak lain yang ingin merusak atau menggunakan pesan rahasia tanpa ijin. Oleh karena itu ciphertext akan disembunyikan pada citra menggunakan teknik steganografi. Dalam hal penggunaannya, steganografi bekerja dengan menyisipkan pesan rahasia ke dalam sebuah informasi sehingga tidak menimbulkan kecurigaan dan keberadaannya tidak diketahui siapapun dalam pengirimannya. Pada penelitian ini hasil data teks yang telah dienkripsi menggunakan algoritma AES dilanjutkan dengan teknik steganografi pada sebuah citra. Algoritma yang diterapkan adalah algoritma Discrete Wavelet Transform (DWT). DWT merupakan algoritma orthogonal transform yang terbagi dalam 4 buah subband. Setiap Sub-band memiliki karakter masing-maisng yang berkaitan dengan *robustness* dan *imperceptibility* data [9], [10]. Sub-band DWT antara lain LL, LH, HL dan HH. Pada subband HH, diketahui bahwa imperceptibiloity citra cukup tinggi. Imperceptibility dapat diukur dengan Peak Signal to Noise Ratio (PSNR), dimana nilai PSNR lebih dari 40 dB dapat disimpulkan bahwa citra asli dan citra hasil operasi tidak jauh berbeda [11].

Dengan adanya kelebihan dan keunggulan yang dimiliki oleh algoritma AES (Advanced Encryption Standard) dalam mengenkripsi teks, dan juga algoritma DWT (Discrete Wavelet Transform) dalam menyisipkan teks pada gambar, maka dalam tugas akhir ini algoritma AES (Advanced Encryption Standard) digunakan untuk mengenkripsi teks terlebih dahulu, kemudian ciphertext hasil disisipkan pada citra digital menggunakan algoritma DWT (Discrete Wavelet Transform).

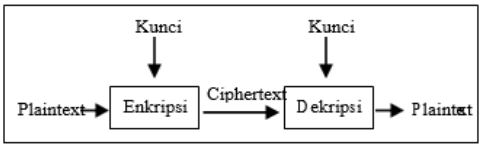
2. METODE

2.1 Citra Digital

Citra digital yang digunakan untuk menyembunyikan pesan pada dasarnya adalah Bitmap. Perihal kedalaman warna menjadi yang paling penting pada citra.jumlah bit per piksel yang berada dari wuatu warna bisa dijabarkan sebagai berikut, 4 bit sebagai16 warna (16 grayscale), 8 bit sebagai 256 warna (256 grayscale) dan 24 bit sebagai 16.777.216 warna [12]. Sebuah teori menyatakan bahwa jika citra mengandung semakin basnyak warna, maka keamanan yang dibutuhkan juga harus semakin tinggi dan ketat. Hal ini dikarenakan bitmap mempunyai area yang besar terhadap sebuah warna. Jika dinyatakan atas kedalaman warna, bitmap bisa mengambil beberapa data tersembunyi.

2.2. Kriptografi

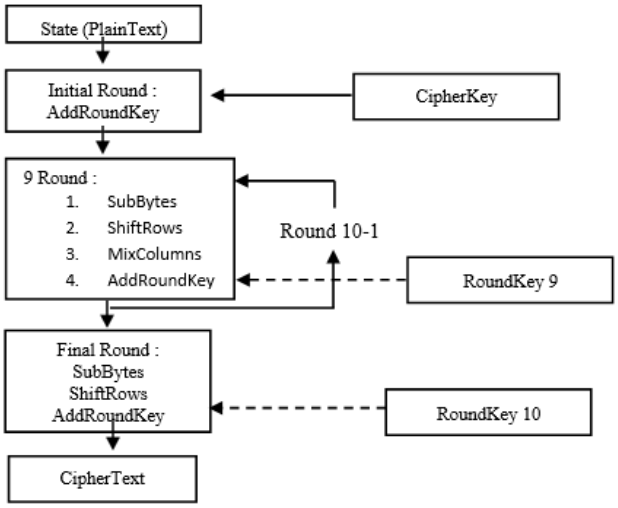
Kriptografi berarti ilmu yang berfungsi menjaga rahasia pada pesan yang mana prosesnya menyandikan pesan menjadi bentuk berbeda yang maknanya tidak bisa dipahami lagi. Kriptografi juga merupakan salah satu cara efektif untuk mengamankan berbagai informasi penting. Dalam kriptografi, terdapat proses yang wajib ada dalam implementasinya, yaitu proses enkripsi dan dekripsi. Pesan yang hendak dienkripsi dikenal dengan plaintext (teks biasa). Hal tersebut dikarenakan informasi bisa dibaca dan dipahami oleh siapapun [13], [14]. Algoritma ini terdiri dari proses enkripsi dan dekripsi pada plaintext yang membutuhkan penggunaan kunci. Kemudian pesan plaintext yang telah dienkripsi (atau tersandikan) disebut dengan ciphertext (teks sandi) seperti terlihat pada Gambar 1.



Gambar 1. Ilustrasi Mekanisme Kriptografi

2.3. *Advanced Encryption Standard (AES)*

Rijndael adalah cipher blok yang dikembangkan oleh Joan Daemen dan Vincent Rijmen. Algoritma ini fleksibel dalam mendukung setiap kombinasi data dan ukuran kunci 128, 192, dan 256 bit. Pada tanggal 22 Mei 2002 secara resmi Algoritma Rijndael diangkat menjadi standar algoritma kriptografi.



Gambar 2. Mekanisme Enkripsi AES-128 bit

AES merupakan salah satu dari algoritma terpopuler pada tahun 2006. Namun, AES hanya mengizinkan panjang data 128 bit yang dapat dibagi menjadi empat blok operasi

dasar. Blok-blok ini beroperasi pada array byte dan diatur sebagai matriks 4x4 yang disebut state. Untuk enkripsi penuh, data dilewatkan melalui putaran Nr (Nr = 10, 12, 14). Tiap jenisnya menyematkan kunci internal yang unik yaitu *round key* pada setiap proses putaran, seperti pada Gambar 2.

Prosedur enkripsi terdiri dari beberapa langkah seperti yang ditunjukkan oleh Gambar 2. Setelah addroundkey awal, fungsi bulat diterapkan ke blok data (terdiri dari bytesub, shiftrows, mixcolumns dan transformasi addroundkey, masing-masing). Ini dilakukan secara iteratif (Nr kali) tergantung pada panjang kunci. Struktur dekripsi memiliki urutan transformasi yang persis sama dengan yang ada di struktur enkripsi. Transformasi Inv-Bytesub, Inv-Shiftrows, Inv-Mixcolumns, dan Addroundkey memungkinkan bentuk skedul kunci identik untuk enkripsi dan dekripsi.

1. Transformasi bytesub: Merupakan Substitusi byte non linier, menggunakan tabel gardu (s-box), yang dibangun dengan invers perkalian dan transformasi affine. Gambar 2 menunjukkan langkah transformasi Bytesub.
2. Transformasi Shiftrows: Adalah transposisi byte sederhana, byte dalam tiga baris terakhir status digeser secara siklis; offset dari shift kiri bervariasi dari satu hingga tiga byte.
3. Transformasi mixcolumns: Setara dengan perkalian matriks kolom-kolom keadaan. Setiap vektor kolom dikalikan dengan matriks tetap. Perlu dicatat bahwa byte diperlakukan sebagai polinomial daripada angka.
4. Transformasi Addroundkey: Adalah XOR sederhana antara status kerja dan roundkey. Transformasi ini adalah kebalikannya sendiri.

Commented [x1]: Tidak ada referensi [15-16]

2.4. Steganografi

Steganografi adalah ilmu/seni yang mempelajari dan berfungsi sebagai menyembunyikan tulisan berupa pesan. Tujuan disembunyikannya sebuah pesan supaya pesan tidak dapat diketahui keberadaannya [17]. Steganografi mengulas tentang bagaimana menyembunyikan atau menyamarkan sebuah pesan.

2.5. *Discrete Wavelet Transform (DWT)*

Transformasi domain frekuensi yang kami terapkan dalam penelitian ini adalah Haar-DWT, DWT paling sederhana. Haar-DWT 2-dimensi terdiri dari dua operasi: Satu adalah operasi horizontal dan yang lainnya adalah operasi vertikal. Detail prosedur Haar-DWT 2-D dijelaskan sebagai berikut:

Langkah 1: Pertama, pindai piksel dari kiri ke kanan dalam arah horizontal. Kemudian, lakukan operasi penjumlahan dan pengurangan pada piksel-piksel yang bertetangga. Simpan jumlah di sebelah kiri dan selisih di sebelah kanan. Ulangi operasi ini sampai semua baris diproses. Jumlah piksel mewakili bagian frekuensi rendah (dilambangkan sebagai simbol L) sedangkan perbedaan piksel mewakili bagian frekuensi tinggi dari gambar asli (dilambangkan sebagai simbol H).

Langkah 2: Kedua, pindai piksel dari atas ke bawah dalam arah vertikal. Lakukan operasi penjumlahan dan pengurangan pada piksel tetangga dan kemudian simpan jumlah di atas dan selisihnya di bawah. Ulangi operasi ini sampai semua kolom diproses. Akhirnya kita akan mendapatkan 4 sub-band masing-masing dilambangkan sebagai LL, HL, LH, dan HH. Sub-band LL adalah bagian frekuensi rendah dan karenanya terlihat sangat mirip dengan gambar aslinya. Seluruh prosedur yang dijelaskan disebut orde pertama 2-D Haar-DWT [18],[19].

2.6. Pengumpulan Data

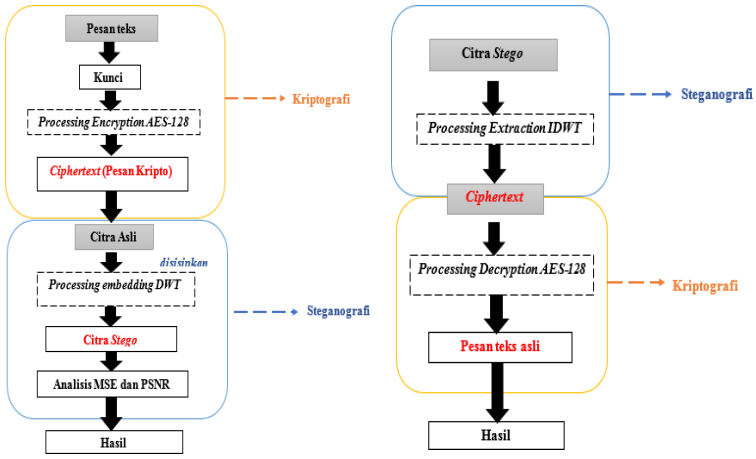
Dalam penelitian ini, peneliti memperoleh data, khususnya untuk citra diambil dari internet untuk membantu dalam proses eksperimen. Citra tersebut merupakan gambar berjenis RGB, seperti pada Tabel 1.

Tabel 1. Dataset Penelitian

Nama File	Ukuran File	Ukuran Pixel
airplane_128.jpg	15.2 KB	128x128
airplane_128.bmp	48.0 KB	128x128
airplane_512.jpg	197 KB	512x512
airplane_512.bmp	768 KB	512x512
joker_128.jpg	6.63 KB	128x128
joker_128.bmp	48.0 KB	128x128
joker_512.jpg	291 KB	512x512
joker_512.bmp	768 KB	512x512
sails_128,jpg	12.6 KB	128x128
sails_128.bmp	48.0 KB	128x128
sails_512.jpg	162 KB	512x512
sails_512.bmp	257 KB	512x512

2.7. Usulan Metode

Pada proses embedding, pesan teks yang dituliskan user dienkripsi sehingga menjadi ciphertext kemudian disisipkan pada citra. Berikut ini adalah skema proses embedding. Pada proses *extraction*, citra stego yang diperoleh dari proses *embedding* diekstrak sehingga dapat mengeluarkan pesan tersembunyi. Berikut ini adalah skema proses ekstraksi. Proses embedding dan extraction dapat dilihat apda Gambar 3.



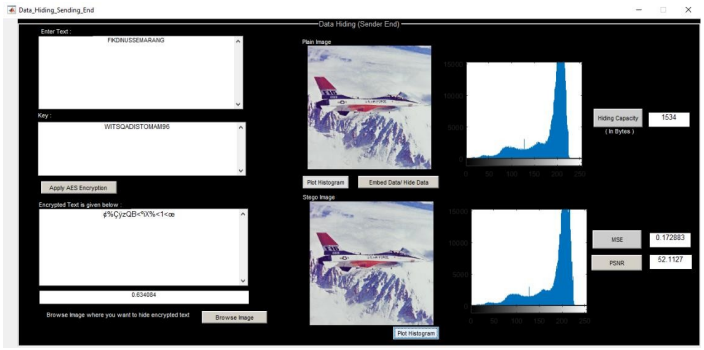
Gambar 3. Embedding dan Extraction Proses

2.8. Pengujian Metode

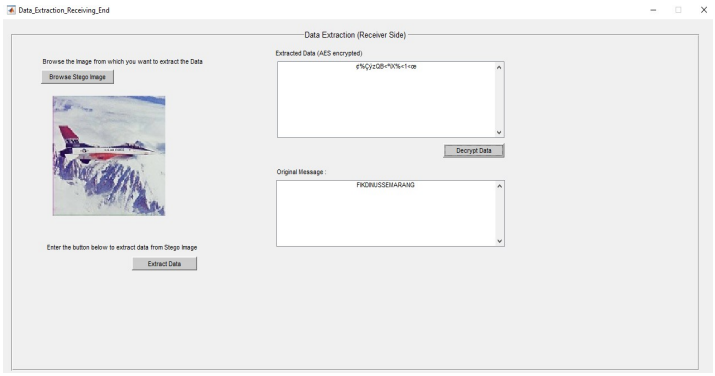
Pengujian penelitian diperoleh dari hasil pengukuran PSNR (*Peak Signal Noise Ratio*) dan MSE (*Mean Square Error*) terhadap citra stego yang dihasilkan. Semakin tinggi nilai PSNR,maka semakin kualitas citra stego semakin mirip dengan citra asli. Semakin rendah nilai MSE-nya, semakin baik kualitas citra stego. Sebelum mencari nilai PSNR, harus dilakukan perhitungan MSE terlebih dahulu untuk mengetahui tingkat kesalahan pada piksel citra *stego*terhadap citra asli.

3. HASIL DAN PEMBAHASAN

Implementasi yang dilakukan pada penelitian ini memanfaatkan *tools* Matlab yang menggunakan GUI sederhana. Terdapat dua tampilan program yang terpisah antara lain GUI *Data Hiding* dan *Data Extact.* Berikut merupakan hasil tampilan GUI implementasi *data hiding* seperti pada Gambar 4 dan Gambar 5.



Gambar 4. Tampilan aplikasi

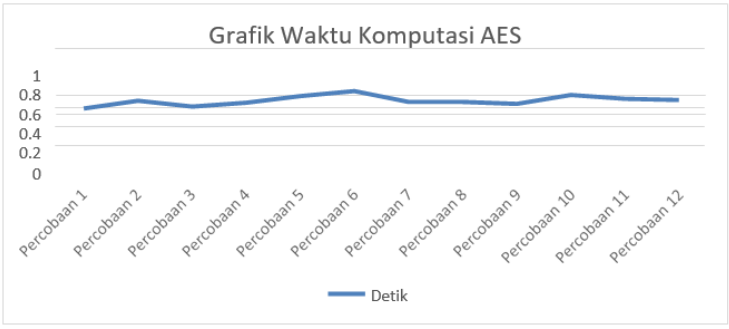


Gambar 5. Proses ekstraksi pesan

Pada Gambar 4, menu ini user dapat melakukan enkripsi teks dan penyisipan pada citra *cover*. Pertama-tama user diminta memasukkan pesan teks di dalam kolom *"Enter Text"* dan jugamemasukkan pesan kunci di kolom *"Key"*. Lalu klik tombol *"Apply AES*

Encryption" untuk melakukan enkripsi AES. Setelah itu akan diperoleh *ciphertext* dan dimunculkan pada kolom bawah beserta waktu proses enkripsi. Kemudian user diminta untuk memilih citra *cover* dengan mengeklik *"Browse Image"* dan akan muncul citra yang dimaksud pada kolom *"Plain Image"*. Terdapat tombol *"Plot Histogram"* untuk menampilkan grafik histogram terhadap citra *cover*. Tombol *"Hiding Capacity"* berfungsi untuk menampilkan kapasitas penyisipan pada citra *cover*. Untuk memulai embedding klik tombol *"Embed Data/ Hide data"* dan akan menampilkan hasil citra *stego* pada kolom *"citra stego"* dan user dapat melihat grafik histogram dengan mengeklik *"plot histogram"* di sebelah kanan citra *stego* untuk membandingkan perbedaan terhadap grafik histogram sebelumnya seperti pada Gambar 5. User bisa mendapatkan nilai MSE dan PSNR dari hasil pengujian ini.

Pada Gambar 5, menu ini user dapat melakukan proses ekstraksi gambar dan dekripsi pesan teks. User diminta untuk memilih citra stego pada file directory, kemudian citra stego akan muncul di kolom bawah. User mengeklik tombol "Extract Data" untuk mengektraksi citra tersebut untuk mendapatkan ciphertext yang telah disisipkan pada program sebelumnya. Untuk dekripsi teksnya user hanya butuh mengeklik tombol "Decrypt Data" dan akan muncul pesan asli di kolom bawah. Eksperimen pada implementasi AES 128 dilakukan untuk mengetahui hasil yang berupa ciphertext atau pesan rahasia yang telah diproses. Dan juga ditambahkannya fitur waktu komputasi sebagai tolak ukur kinerja pemrosesan algoritma terhadap objek penelitian seperti pada Gambar 6.



Gambar 6. Grafik waktu komputasi AES

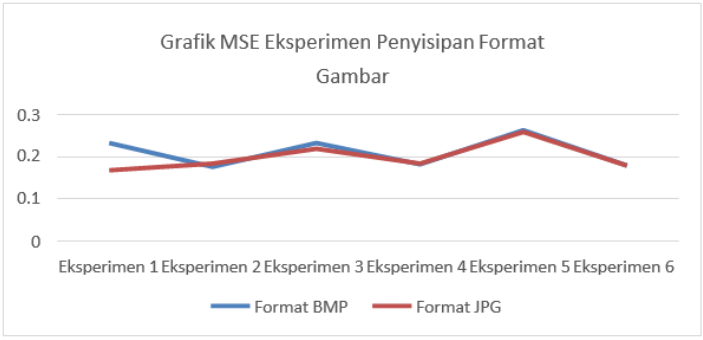
Dari Hasil Eksperimen Implementasi AES 128 telah didapatkan hasil eksperimen dari beberapa pesan teks dan kunci diantaranya seperti pada Tabel 2.

Tabel 2. Lama waktu penyisipan pesan menggunakan AES

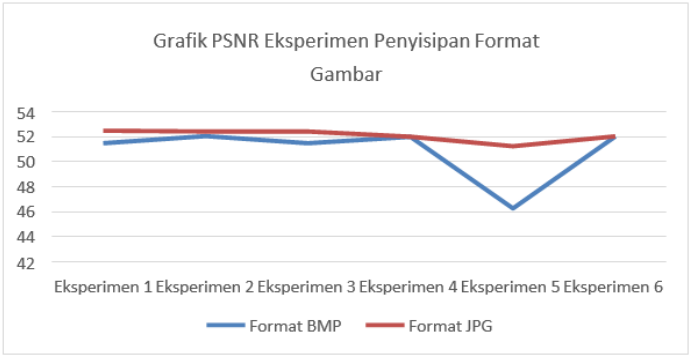
Eksperimen ke	Keterangan
1	Panjang pesan 19 karakter dengan panjang kunci 10 karakter mampu diproses selama 0.662056 detik
2	Panjang pesan 60 karakter dengan panjang kunci 10 karakter mampu diproses selama 0.740039 detik.
3	Panjang pesan 53 karakter dengan panjang kunci 16 karakter mampu diproses selama 0.687269 detik.
4	Panjang pesan 64 karakter dengan panjang kunci 16 karakter mampu diproses selama 0.728582 detik.
5	Panjang pesan 125 karakter dengan panjang kunci 14 karakter mampu diproses

	selama 0.793764 detik
6	Panjang pesan 149 karakter dengan panjang kunci 14 karakter mampu diproses selama 0.841142 detik
7	Panjang pesan 105 karakter dengan panjang kunci 8 karakter mampu diproses selama 0.739969 detik.
8	Panjang pesan 81 karakter dengan panjang kunci 8 karakter mampu diproses selama 0.733481 detik.
9	Panjang pesan 90 karakter dengan panjang kunci 9 karakter mampu diproses selama 0.719606 detik.
10	Panjang pesan 135 karakter dengan panjang kunci 9 karakter mampu diproses selama 0.802855 detik.
11	Panjang pesan 126 karakter dengan panjang kunci 10 karakter mampu diproses selama 0.768553 detik.
12	Panjang pesan 93 karakter dengan panjang kunci 10 karakter mampu diproses selama 0.754694 detik.

Pengujian non-attack merupakan eksperimen dengan menghitung nilai MSE dan PSNR citra stego untuk mengetahui kualitas citra stego dengan membandingkannya terhadap citra cover. Gambar 7 dan Gambar 8 merupakan grafik MSE dan PSNR dari eksperimen yang telah dilakukan.



Gambar 7. Grafik perolehan nilai MSE



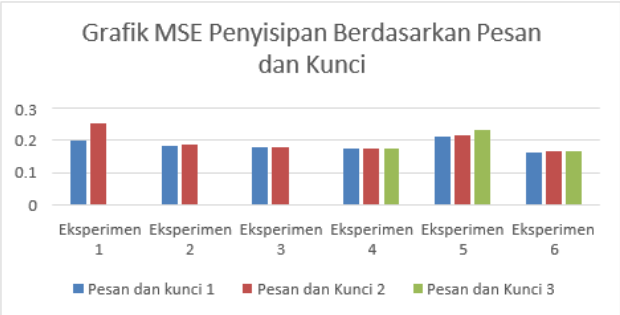
Gambar 8. Grafik perolehan nilai PSNR

Dari Hasil Eksperimen Penyisipan Berdasarkan Format Gambar pada percobaan dengan menggunakan pesan dan kunci yang sama namun format dan ukuran citra yang berbeda telah didapatkan hasil eksperimen dari beberapa citra uji seperti pada Tabel 3.

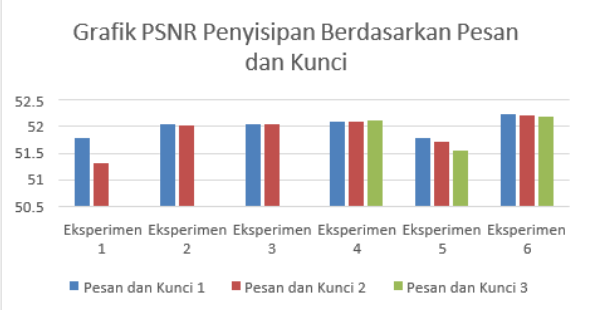
Tabel 3. Nilai MSE dan PSNR menggunakan AES

No	Eksperimen	Keterangan
1	Pesan teks 1 disisipkan citra 1	Percobaan pada citra pertama berformat *bmp menunjukkan hasil MSE 0.233826 dan PSNR 51.5049.
2	ukuran 128x128 piksel	Percobaan pada citra kedua berformat *jpg menunjukkanhasil MSE 0.168498 dan PSNR 52.0586.
3	Pesan teks 1 disisipkan citra 1	Percobaan pada citra pertama berformat *bmp menunjukkan hasil MSE 0.176538 dan PSNR 52.0713.
4	ukuran 512x512 piksel	Percobaan pada citra kedua berformat *jpg menunjukkan hasil MSE 0.184186 dan PSNR 52.4236.
5	Pesan teks 2 disisipkan citra 2	Percobaan pada citra pertama berformat *bmp menunjukkan hasil MSE 0.233826 dan PSNR 51.5049.
6	ukuran 128x128 piksel	Percobaan pada citra kedua berformat *jpg menunjukkan hasil MSE 0.219889 dan PSNR 52.4236.
7	Pesan teks 2 disisipkan citra 2	Percobaan pada citra pertama berformat *bmp menunjukkan hasil MSE 0.182939 dan PSNR 52.0378.
8	ukuran 512x512 piksel	Percobaan pada citra kedua berformat *jpg menunjukkan hasil MSE 0.184186 dan PSNR 52.0141.
9	Pesan teks 3 disisipkan citra 3	Percobaan pada citra pertama berformat *bmp menunjukkan hasil MSE 0.26385 dan PSNR 46.2758.
10	ukuran 128x128 piksel	Percobaan pada citra kedua berformat *jpg menunjukkan hasil MSE 0.259237 dan PSNR 51.2581.
11	Pesan teks 3 disisipkan citra 3	Percobaan pada citra pertama berformat *bmp menunjukkan hasil MSE 0.179893 dan PSNR 52.0465.
12	ukuran 512x512 piksel	Percobaan pada citra kedua berformat *jpg menunjukkan hasil MSE 0.179818 dan PSNR 52.0451.

Dari hasil di atas, diperoleh kesimpulan bahwa format *jpg lebih baik daripada format *bmp karena ukuran file *jpg lebih kecil daripada *bmp. Kemudian semakin besar jumlah piksel pada citra akan menghasilkan nilai MSE lebih kecil dan nilai PSNR lebih besar, yang berarti kualitas citra lebih baik. Gambar 9 dan Gambar 10 merupakan grafik nilai MSE dan PSNR berdasarkan pada tabel Hasil Eksperimen Penyisipan Berdasarkan Pesan dan Kunci.



Gambar 9. Grafik Perolehan MSE pada kunci yang berbeda



Gambar 10. Grafik Perolehan PSNR pada kunci yang berbeda

Pada percobaan dengan menggunakan pesan dan kunci yang berbeda telah didapatkan hasil eksperimen dari beberapa citra uji seperti Tabel 4.

Tabel 4. Nilai MSE dan PSNR pada kunci berbeda menggunakan AES

No	Eksperimen	Keterangan
1	Citra 1	Percobaan pada pesan pertama menunjukkan hasil MSE 0.205405 dan PSNR 51.7933.
2		Percobaan pada pesan kedua dengan kunci yang sama menunjukkan hasil MSE 0.254761 dan PSNR 51.3044.
3	Citra 2	Percobaan pada pesan pertama menunjukkan hasil MSE 0.185939 dan PSNR52.0425.
4		Percobaan pada pesan kedua dengan kunci yang sama menunjukkan hasil MSE 0.188502 dan PSNR 52.0136.
5	Citra 3	Percobaan pada pesan pertama menunjukkan hasil MSE 0.18047 dan PSNR 52.0403.
6		Percobaan pada pesan kedua dengan kunci yang sama menunjukkan hasil MSE 0.17917 dan PSNR 52.0546.
7	Citra 4	Percobaan pada kunci pertama menunjukkan hasil MSE 0.174868 dan PSNR52.1027.
8		Percobaan pada kunci kedua dengan pesan yang sama menunjukkan hasil MSE 0.175448 dan PSNR 52.0965.
9		Percobaan pada kunci ketiga dengan pesan yang sama menunjukkan hasilMSE 0.174018 dan PSNR 52.112.
10	Citra 5	Percobaan pada kunci pertama menunjukkan hasil MSE 0.210266 dan PSNR 51.7884.
11		Percobaan pada kunci kedua dengan pesan yang sama menunjukkan hasilMSE 0.21637 dan PSNR 51.7249.
12		Percobaan pada kunci ketiga dengan pesan yang sama menunjukkan hasil MSE 0.234334 dan PSNR 51.5465.
13	Citra 6	Percobaan pada kunci pertama menunjukkan hasil MSE 0.164026 dan PSNR52.2325.
14		Percobaan pada kunci kedua dengan pesan yang sama menunjukkan hasil MSE 0.16574 dan PSNR 52.2127.
15		Percobaan pada kunci ketiga dengan pesan yang sama menunjukkan hasilMSE 0.167614 dan PSNR 52.1908.

Dari hasil percobaan di atas, diperoleh kesimpulan bahwa penambahan karakter pada pesan teks dan kunci meningkatkan nilai MSE dan menurunkan nilai PSNR, dengan kata lain semakin banyak jumlah karakter yang disisipkan maka akan semakin buru citra yang

dihasilkan. Berdasarkan hasil eksperimen menunjukkan bahwa semakin banyaknya panjang karakter pesan teks dan kunci, maka akan semakin lambat waktu komputasi enkripsi. Rata- rata waktu komputasi yang ditempuh adalah 0.6-0.8 detik. Kemudian pada proses penyisipannya berdasarkan format dan ukuran citra menghasilkan rata-rata nilai MSE 0.16-0.26 dB dan nilai PSNR nya 46.27-52.07 dB. Diketahui bahwa format *jpg lebih baik daripada format *bmp dan juga diketahui bahwa semakin besar jumlah piksel pada citra akan menghasilkan nilai MSE lebih kecil dan nilai PSNR lebih besar, yang berarti kualitas citra lebih baik. Kemudian eksperimen penyisipan pada citra berdasarkan pesan teks dan kunci menghasilkan rata-rata nilai MSE 0.16-0.25 dB dan nilai PSNR 51.3-52.2 dB, diketahui semakin panjang karakter pesan atau kunci yang disisipkan maka semakin buruk citra stego nya.

4. KESIMPULAN

Metode kriptografi menggunakan algoritma AES 128 Bit berhasil diimplementasikan, hal ini ditunjukkan dengan pesan teks yang berhasil disandikan dengan baik dan dapat dikembalikan ke bentuk semula. Metode steganografi DWT berhasil diimplementasikan, hal ini ditunjukkan pada pesan teks yang disisipkan ke dalam citra digital dapat disembunyikan dengan baik sehingga tidak dapat dibedakan dengan citra aslinya secara kasat mata. Kualitas gambar stego menggunakan DWT tergolong cukup baik. Hal ini dapat dilihat dari hasil nilai MSE 0.16-0.26 dB dan nilai PSNR nya 46.27-52.2 dB. Semakin banyak karakter pada pesan yang disisipkan maka nilai PSNR semakin kecil dan nilai MSE semakin besar. Semakin kecil ukuran citra dan semakin besar piksel pada citra asli maka nilai PSNR semakin besar dan nilai MSE semakin kecil. untuk memperbaiki hasilm pad apenelitian selanjutnya dapat dilakukan proses penggabungan atau mengganti metode yang diusulkan penulis dengan metode yang berbeda dari teknik steganografi yang dapat mengetahui perbedaan dari kelebihan dan kekurangan setiap metode. Pesan yang digunakan sebagai pesan rahasia tidak hanya berupa pesan teks, yaitu dapat menggunakan pesan file gambar, file audio atau file video. Dalam pengembangan lebih lanjut dapat difokuskan bukan hanya media gambar melainkan pada audio atau video untuk media steganografi.

REFERENSI

[1] C. A. Sari, W. S. Sari, and B. Sugiarto, "IMPERCEPTIBLE KRIPTOGRAFI CITRA BERWARNA MENGGUNAKAN RIVEST SHAMIR ADLEMAN," in *Proceeding SENDIU 2021*, 2021, pp. 978–979.
[2] C. A. Sari and E. H. Rachmawanto, "Gabungan Algoritma Vernam Chiper Dan End of File," *Techno.COM*, vol. 13, no. 3, pp. 150–157, 2014.
[3] Muslih and E. Rachmawanto, "PENGAMANAN FILE MULTIMEDIA DENGAN METODE STEGANOGRAFI END OF FILE UNTUK MENJAGA," *Techno.COM*, vol. 15, no. 1, pp. 1–6, 2016.
[4] E. H. Rachmawanto and C. A. Sari, "Steganografi Pengamanan Data Gambar Penyakit dengan Hybrid SLT-DCT," in *SEMANTIK 2013*, 2013, vol. 2013, no. November, pp. 96–101.
[5] P. Chowdhuri, B. Jana, and D. Giri, "Secured steganographic scheme for highly compressed color image using weighted matrix through DCT," *Int. J. Comput. Appl.*, vol. 7074, pp. 1–12, Aug. 2018.
[6] S. D. Nasution, G. L. Ginting, M. Syahrizal, and R. Rahim, "Data Security Using Vigenere Cipher and Goldbach Codes Algorithm," *Int. J. Eng. Res. Technol.*, vol. 6, no. 01, pp. 360–363, 2017.
[7] Sangeeta and E. A. Kaur, "A Review on Symmetric Key Cryptography Algorithms," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 4, pp. 358–362, 2017.
[8] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, "A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish," *Procedia Comput. Sci.*, vol. 78, no. December 2015, pp. 617–624, 2016.
[9] S. Tyagi, H. V. Singh, and R. Agarwal, "Image watermarking using genetic algorithm in DCT domain," in *2017 International Conference on Inventive Systems and Control (ICISC)*, 2017, pp. 1–6.
[10] J. Wang and Z. Du, "A method of processing color image watermarking based on the Haar wavelet," *J.*

Vis. Commun. Image Represent., vol. 64, p. 102627, 2019.
[11] N. Ben Halima, M. A. Khan, and R. Kumar, "A Novel Approach of Digital Image Watermarking using HDWT-DCT," in *2015 Global Summit on Computer & Information Technology (GSCIT)*, 2015, no. June, pp. 1–6.
[12] S. K, "An Optimal RSA Encryption Algorithm for Secret Images," *Int. J. Pure Appl. Math.*, vol. 118, no. 20, pp. 2491–2500, 2018.
[13] E. J. Kusuma, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "An Imperceptible LSB Image Hiding on Edge Region Using DES Encryption," in *International Conference on Innovative and Creative Information Technology (ICITech)*, 2017, pp. 1–5.
[14] P. Bindlish, "Study of RSA, DES and Cloud Computing," *Int. J. Adv. Res. Comput. Sci.*, vol. 7, no. 3, pp. 211–215, 2016.
[15] C. A. Sari, G. Ardiansyah, D. R. I. Moses Setiadi, and E. H. Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 17, no. 5, 2019.
[16] Nurhayati and S. S. Ahmad, "Steganography for inserting message on digital image using least significant bit and AES cryptographic algorithm," in *2016 4th International Conference on Cyber and IT Service Management*, 2016, pp. 1–6.
[17] Lindawati and R. Siburian, "Steganography Implementation on Android Smartphone Using the LSB (Least Significant Bit) to MP3 and WAV Audio," *Proc. - ICWT 2017 3rd Int. Conf. Wirel. Telemat. 2017*, pp. 170–174, 2017.
[18] A. Goswami and S. Khandelwal, "Hybrid DCT-DWT Digital Image Steganography," *Int. J. Adv. Res. Comput. Commun. Eng. Vol.*, vol. 5, no. 6, pp. 228–233, 2016.
[19] R. Naoum, A. Shihab, and S. Alhamouz, "Enhanced Image Steganography System based on Discrete Wavelet Transformation and Resilient Back-Propagation," *Int. J. Comput. Sci. Netw. Secur.*, vol. 16, no. 1, pp. 114–122, 2016.