PENERAPAN ALGORTIMA DIFFIE-HELLMAN PADA STEGANOGRAFI LEAST SIGNIFICANT BIT

Ignatius Rivaldo Lie[1*], Derry Alamsyah[2]
[1,2]Program Studi Informatika, Fakultas Ilmu Komputer dan Rekayasa, Universitas Multi Data Palembang
[1]ignatiusrivaldolie@mhs.mdp.ac.id, [2]derry@mdp.ac.id

Kata kunci:
steganografi; kriptografi; PSNR; least significant Bits; MSE

Abstract: *Perkembangan teknologi informasi berkembang begitu pesat seiring berjalannya waktu. Saat ini, informasi sering dipertukarkan melalui Internet dan karena itu rentan terhadap pencurian informasi. Banyak jenis informasi yang menggunakan pengamanan khusus seperti pin, kata sandi, dan data diri. Sehingga rentan terhadap penyadapan data melalui ruang bertukar informasi publik. Dalam penelitian ini dilakukan penerapan algoritma Diffie-hellman untuk steganografi least significant bits. Steganografi citra adalah proses penyembunyian pesan rahasia dalam citra digital dan Kriptografi adalah studi tentang metode komunikasi yang aman antara dua pihak. Pada penelitian ini algoritma yang digunakan yaitu Diffie-hellman, Advanced Encryption Standard sebagai media penerapan Diffie-hellman dan steganografi dengan teknik least significant bits. Pengujian dilakukan dengan menggunakan gambar high contrast dan low contrast untuk melihat Peak Signal to Noise Ratio (PSNR) dan Means Square Error (MSE) sebelum dan sesudah proses steganografi. Hasil pengujian didapatkan bahwa nilai rata-rata PSNR gambar high contrast sebesar 96,539692 dan rata-rata MSE gambar high contrast sebesar 0,0000159. Pengujian gambar low contrast didapatkan nilai rata-rata PSNR sebesar 96,7335291 dan rata-rata nilai MSE sebesar 0,0000173.*

Abstrak: Perkembangan teknologi informasi berkembang begitu pesat dari waktu ke waktu. Saat ini, informasi sering dipertukarkan melalui Internet dan karenanya rentan terhadap pencurian informasi. Banyak jenis informasi menggunakan pengamanan khusus seperti pin, kata sandi, dan data pribadi. Sehingga rentan terhadap penyadapan data melalui ruang pertukaran informasi publik. Pada penelitian ini penerapan algoritma *Diffie-Hellman* dilakukan untuk *steganografi least significant bits*. *Image Steganography* adalah proses menyembunyikan pesan rahasia dalam gambar digital dan Kriptografi adalah studi tentang metode komunikasi yang aman antara dua pihak. Pada penelitian ini, algoritma yang digunakan adalah *Diffie-Hellman*, *Advanced Encryption Standard* sebagai media aplikasi *Diffie-Hellman* dan *steganografi* dengan teknik *least significant bits*. Pengujian dilakukan dengan menggunakan citra high contrast dan low contrast untuk melihat Peak Signal to Noise Ratio (PSNR) dan Means Square Error (MSE) sebelum dan sesudah proses steganografi. Hasil pengujian menunjukkan bahwa rata-rata nilai PSNR citra kontras tinggi adalah 96,539692 dan rata-rata MSE citra kontras tinggi adalah 0,0000159. Pengujian citra kontras rendah diperoleh nilai PSNR rata-rata 96,7335291 dan nilai MSE rata-rata 0,0000173.

Lie, Alamsyah. (2023). Penerapan Algortima Diffie-Hellman pada Steganografi Least Significant Bit. *MDP Student Conference* 2023

PENDAHULUAN

Perkembangan teknologi informasi berkembang begitu pesat seiring berjalannya waktu. Saat ini, informasi sering dipertukarkan melalui Internet dan karena itu rentan terhadap pencurian informasi. Banyak jenis informasi yang menggunakan pengamanan khusus seperti pin, kata sandi, dan data diri. Dengan berkembangnya teknologi informasi, kejahatan siber juga ikut berkembang dan bertambah seiring waktu berjalan. Di antara berbagai kejahatan siber, salah satu jenis kejahatannya adalah penyadapan data. Penyadapan data sering terjadi di ruang pertukaran informasi publik, terutama di perangkat Android, di mana berbagi informasi satu sama lain mudah ditukarkan secara cepat. Salah satu cara bagi pengguna Android untuk berbagi informasi adalah dengan mengirim pesan pribadi dari satu pengguna ke pengguna lainnya menggunakan aplikasi android seperti WhatsApp, Facebook, Telegram, dan E-Mail [1].

Berbagai cara ditempuh agar bisa mengamankan informasi yang ditukarkan di ruang publik sebagai contohnya yaitu steganografi dan kriptografi. Steganografi adalah jenis komunikasi tersembunyi, yang secara harfiah berarti "tulisan tertutup" [2]. Tidak seperti kriptografi, steganografi tidak bertujuan untuk mengamankan komunikasi, tapi menyembunyikan keberadaannya [3].

Adapun beberapa penelitian terkait dari penelitian ini seperti penelitian [13] dalam penerapan *Advanced Encryption Standard* pada perankat *Smartphone* didapatkan bahwa algoritma rijandael lebih unggul dari algoritma lain dengan waktu enkripsi 0,025 ms dan deskripsi 0,022 ms. Pada penelitian [14] dalam penerapan kriptografi kunci simetris pada enkripsi video didapatkan bahwa video hasil dari enkripsi membuat *frame* video menjadi kurang jelas atau berbeda dengan *frame* aslinya dan penerapannya berhasil dijalankan.

Penelitian ini dikembangkan sistem steganografi dengan enkripsi *Advanced Encryption Standard* dengan algoritma *Diffie-Hellman*. Sistem ini dirancang bertujuan untuk mencegah penyadapan yang terjadi pada saat pertukaran data pada publik. Penerapan dilakukan dengan cara menerapkan *Advanced Encryption Standard (AES)* dengan algoritma *Diffie-Hellman* pada teknik Steganografi *Least Significant Bit*. Sistem akan dirancang dalam aplikasi berbasis android. Pengujian dilakukan dengan cara menghitung *Peak Signal-to-Noise Ratio (PSNR)* dan menghitung *Mean Square Error* (MSE) pada citra yang sudah disisipkan citra rahasia.

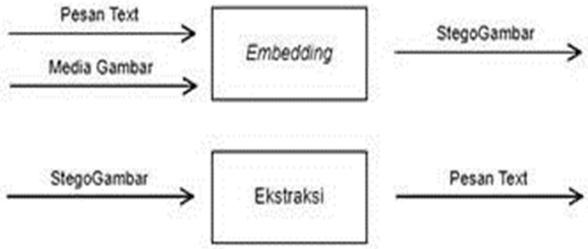
METODE

Penulis menggunakan metode penelitian dalam berbagai tahap yaitu studi literatur, perancangan, implementasi, pengujian dan evaluasi.

Studi Literatur

Pada tahapan ini, penulis mencari beberapa referensi yang digunakan untuk mendukung penelitian ini dari berbagai sumber seperti jurnal, dan buku yang terkait dengan topik pembahasan penelitian ini.

Steganografi citra adalah proses penyembunyian pesan rahasia dalam citra digital [6]. Tujuan utama steganografi adalah untuk meningkatkan keamanan komunikasi dengan menyisipkan pesan rahasia ke dalam gambar digital dan dengan memodifikasi piksel gambar digital digital agar tidak berarti [1].

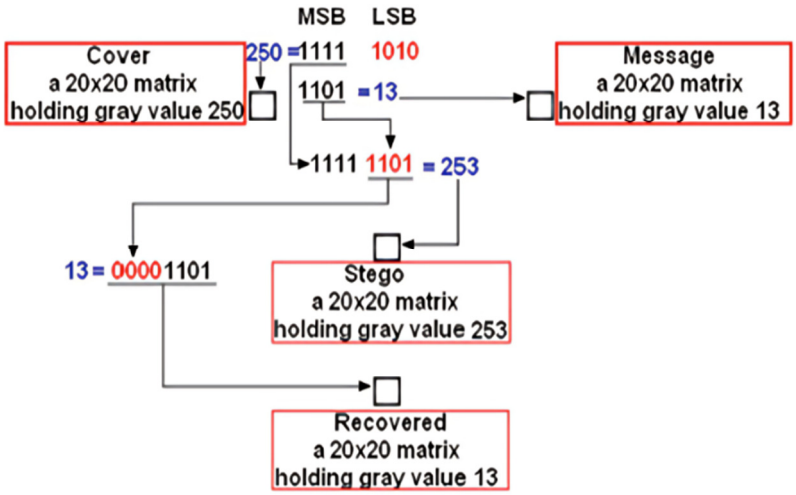


Gambar 1. Proses Penyisipan dan Ekstraksi Data pada Steganografi

Gambar 1 Memperlihatkan proses penyisipan pesan *Text* ke dalam media gambar, dimana hasil keluaran yang dihasilkan dari proses tersebut adalah sebuah *stegoGambar* (gambar yang telah disisipi pesan *Text*) dan pada Gambar 1 juga dapat dilihat proses ekstraksi pesan *Text* dari *stegoGambar*, dimana hasil keluaran dari proses tersebut adalah pesan teks [1].

Kriptografi adalah studi tentang metode komunikasi yang aman antara dua pihak. Biasanya, ada dua pihak yang ingin saling berkirim pesan, tetapi mereka ingin menghindari kemungkinan pihak ketiga memahami pesan-pesan ini seharusnya mereka jatuh ke tangan yang salah [7]. Kriptografi sering digunakan untuk meningkatkan keamanan suatu sistem informasi agar tidak terjadi kebobolan data maupun penyadapan data di saat pertukaran informasi.

LSB merupakan salah satu teknik steganografi yang paling banyak digunakan dan memiliki tingkat kesenyapan yang tinggi. Skema LSB bekerja dengan mengubah *redundant image bits* yang tidak berpengaruh secara signifikan terhadap bit-bit dari pesan rahasia. Gambar 2 menunjukkan mekanisme metode LSB pada citra 8 bit dengan menggunakan 4 bit LSB [4].



Gambar 2. Mekanisme LSB[4]

Diffie–Hellman adalah salah satu algoritma enkripsi kunci publik pertama yang tercatat, digunakan untuk mentransfer data dari satu pengguna ke pengguna lain dengan tetap menjaga integritas dan keamanan data. [8] Karena algoritma *Diffie–Hellman* yang ada dapat dipecahkan dengan mudah melalui logaritma diskrit, perantara, dan *brute force*, teknik yang diusulkan layak karena menggunakan banyak operasi kompleks untuk menghasilkan kunci umum untuk semua pengguna jaringan, sehingga membuatnya jauh lebih baik dari sebelumnya dan menciptakan saluran yang aman dan terjamin [8].

Dalam skema algoritma *Diffie–Hellman* yang ada awalnya kami memilih bilangan prima besar 'p' dan generator 'g' dari bilangan prima, di mana 'g' kurang dari 'p dan kekuatan 'g' harus menghasilkan semua nomor bervariasi dari '1' hingga 'p-1'. (2) Dalam algoritma *Diffie– Hellman*, pengguna pertama harus memilih kunci privat acak k1' sendiri sehingga kunci publiknya dihitung dengan menggunakan persamaan (1) sebagai berikut: Demikian pula, pengguna lain juga akan memilih kunci pribadi rahasianya 'k2'. Kunci publik dari pengguna kedua akan diberikan dengan cara yang sama seperti yang ditunjukan pada persamaan (2).

$$PublicKey = g^{(k2)} mod\ p \quad (2)$$

Kedua pengguna kemudian akan berbagi kunci publik masing-masing satu sama lain. Masing-masing pengguna kemudian akan menggunakan kunci publik dari pengguna lain dan kunci pribadinya sendiri untuk menghitung kunci umum simetris, *Commonkey* dapat dihitung menggunakan persamaan (3) sebagai berikut:

$$CommonKey = g^{(k1 * k2)} mod\ p \quad (3)$$

Dengan demikian, dengan bantuan algoritma yang ada, kedua pengguna dapat berkomunikasi dengan cara yang aman karena sekarang *plain text* dapat dikirim dalam bentuk terenkripsi. Selanjutnya, karena 'K1 ' dan 'K2' adalah kunci pribadi dari masing-masing pengguna dan nilai lainnya, 'p', 'g', 'PK(1)', dan 'PK(2)' bersifat publik, musuh bebuyutan harus menggunakan logaritma diskrit, untuk menentukan kunci rahasia. Misalnya, untuk menemukan nilai kunci pengguna A, musuh harus menghitung nilainya menggunakan persamaan (4).

$$'K1' = dlog_{a_q}\ (publickey(1)) \quad (4)$$

dan untuk kunci pribadi pengguna B, musuh harus menghitung nilainya sebagai:

$$'K2' = dlog_{a_q}\ (publickey(2)) \quad (5)$$

sama, kunci umum rahasia 'K' dapat ditentukan dengan cara yang sama seperti yang ditunjukan di persamaan (5) [8].

Algoritma AES adalah algoritma blok cipher simetris yang dipilih oleh National Institute of Standards and Technology (NIST) pada tahun 2001 untuk menggantikan *Data* Enkripsi *Standard* (DES) [9]. Enkripsi dilakukan pada transmisi dengan mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan pada penerimaan dengan mengubah data rahasia menjadi data asli. Oleh karena itu, informasi yang dikirim selama transmisi bersifat rahasia, sehingga informasi asli tidak dapat diakses oleh orang yang tidak berhak. Hanya penerima yang dapat mengetahui data asli dengan kunci rahasia. Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi *byte*, yaitu *SubBytes*, *ShiftRows*, *Mixcolumns*, dan *AddRoundKey*. Pada awal proses enkripsi, *input* yang telah disalin ke dalam *state* akan mengalami transformasi *byte AddRoundKey*. Setelah itu, *state* akan menjalani *Subbytes*, *ShiftRows*, *MixColumns*, dan *AddRoundKey* berubah sebanyak Nr. Proses dalam algoritma AES disebut fungsi putaran. Babak terakhir agak berbeda dengan babak sebelumnya dimana pada babak terakhir *state* tidak mengalami transformasi *MixColumns*. Transformasi *cipher* dapat dibalik dan dilakukan dalam arah yang berlawanan untuk menghasilkan invers *cipher* yang mudah dipahami untuk algoritma AES. Transformasi *byte* yang digunakan pada inverse cipher adalah *InvShiftRows*, *InvSubBytes*, InvMixColumns, dan AddRoundKey [10].

Setiap putaran mencakup empat operasi yang disebutkan sebelumnya. Jumlah putaran adalah 10 untuk kunci 128-bit, 12 untuk kunci 192-bit, dan 14 untuk kunci 256-bit. Setelah putaran terakhir, matriks yang dihasilkan ditambahkan ke kunci untuk menghasilkan *ciphertext*. Membalikkan semua operasi yang disebutkan sebelumnya menghasilkan pesan teks asli [9].

Mean Squared Error (MSE) adalah model metrik evaluasi yang sering digunakan dengan model regresi. Kesalahan kuadrat rata-rata dari model sehubungan dengan set tes adalah rata-rata kesalahan prediksi kuadrat atas semua contoh dalam set pengujian. Kesalahan prediksi adalah perbedaan antara nilai sebenarnya dan nilai prediksi untuk sebuah *instance*. [11]. Nilai MSE dapat dihitung menggunakan persamaan (6) sebagai berikut

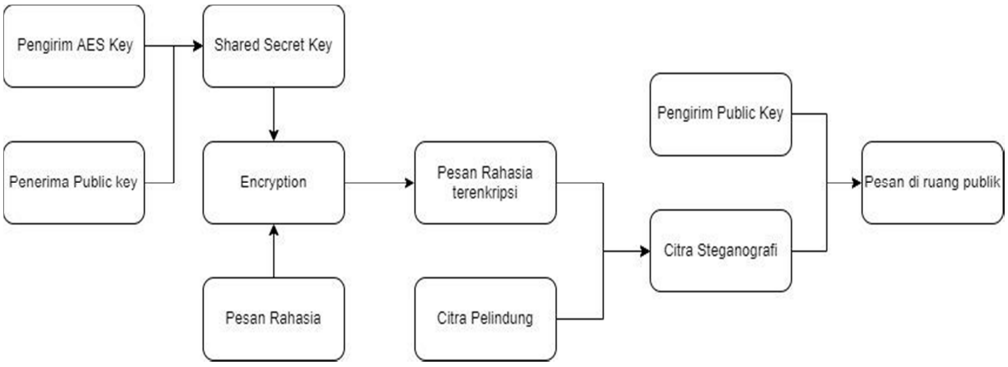
$$MSE = \frac{1}{M\ x\ N\ x\ O}\sum_{x=1}^{M}\ \sum_{y=1}^{N}\ \sum_{z=1}^{O}\ \left[\left(I_{(x,y,z)} - I'_{(x,y,z)}\right)\right]^2 \quad (6)$$

Peak Signal to Noise Ratio (PSNR) dihasilkan dari perhitungan logaritma *Mean Square Error* (MSE) suatu citra. Dimana MSE secara tradisional menggunakan metode penjumlahan sebagai komponen utamanya. Pada citra MSE *grayscale* dihitung berdasarkan dimensi $M \times N$, sedangkan pada citra warna RGB MSE, citra RGB dapat dihitung berdasarkan dimensi $M \times N \times O$[12]. Nilai PSNR dapat dihitung menggunakan persamaan (7) dengan menggunakan nilai MSE yang didapatkan pada persamaan sebelumnya.

$$PSNR = 10log10\left(\frac{max^2}{MSE}\right) \quad (7)$$

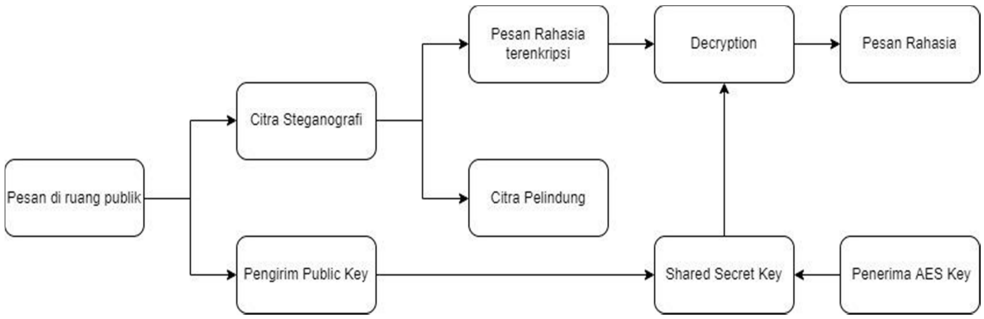
Perancangan

Pada tahap ini dibahas perancangan suatu sistem untuk digunakan sebagai media steganografi berserta enkripsi Algoritma *Diffie-Hellman*. Aplikasi dibuat untuk platform android dengan fungsi-fungsi aplikasi sebagai berikut:



Gambar 3. Proses Enkripsi

Proses enrkipsi ditujukan pada gambar 3. Proses enkripsi dimulai dari sistem melakukan proses untuk menghasilkan kunci publik. Pengirim memasukan kunci AES yang telah dikirim oleh penerima sebagai alamat yang dituju sehingga pesan tidak dapat dibuka tanpa kunci publik kedua belah pihak. Kunci AES dan kunci publik di proses menggunakan persamaan (3) menjadi kunci bersama atau *shared secret key*. Setelah proses tersebut maka dilakukan enkripsi AES dengan menggunakan kunci bersama tersebut lalu pesan rahasia terenkripsi melewati proses steganografi dengan citra pelindung yang bertindak sebagai media penyimpanan. Hasil dari proses tersebut adalah citra steganografi. Citra steganografi dikirimkan ke penerima bersama kunci publik pengirim melewati ruang publik.



Gambar 4. Proses Deskripsi

Proses deskripsi ditujukan pada gambar 4. Proses deskripsi dimulai dengan penerima menerima citra steganografi dan kunci publik pengirim. Penerima memasukan citra steganografi dan kunci publik pengirim ke dalam aplikasi. Citra steganografi melalui proses steganografi balik sehingga proses tersebut menghasilkan citra pelindung dan pesan rahasia terenkripsi. Kunci AES penerima dan kunci publik pengirim diproses menggunakan persamaan (5) sehingga dihasilkan kunci bersama yang sama dengan proses enkripsi pada gambar 5. Sistem melakukan proses deskripsi menggunakan kunci bersama maka didapatkan pesan rahasia yang dikirimkan oleh pengirim.

Implementasi

Pada tahap ini, penulis menerapkan teori-teori yang sudah didapatkan ke dalam bentuk aplikasi berbasis android menggunakan bahasa pemrograman *java*. Aplikasi memiliki 3 jenis masukan yaitu kunci publik penerima, pesan rahasia dan gambar citra pelindung. Aplikasi memiliki 3 tombol yaitu *Encode* yang melakukan proses enkripsi, *Decode* yang melakukan proses deskripsi dan *save* yang digunakan untuk menyimpan gambar yang sudah melewati proses enkripsi. Keluaran dari aplikasi ini adalah citra steganografi sebagai gambar yang di simpan menggunakan tombol *save* dan pesan rahasia jika proses deskripsi dilakukan.

Gambar 5. Tampilan Aplikasi Steganografi AES Diffie-Hellman

Pengujian

Pada tahap ini dilakukan pengujian dengan cara menghitung distorsi gambar steganografi dan citra pelindung menggunakan MSE dan PSNR.

Evaluasi

Evaluasi dilakukan dengan cara menghitung tingkat distorsi gambar *high contrast* dan *low contrast* yang sudah disteganografi maupun sebelum disteganografi lalu membandingkan hasil yang didapat.

HASIL DAN PEMBAHASAN

Pengujian program dilakukan menggunakan 2 jenis gambar yaitu gambar *High Contrast* dan *Low Contrast.* Gambar *High Contrast* adalah gambar yang memiliki tingkat kecerahan dan kegelapan yang tinggi. Gambar *Low Contrast* adalah gambar yang memiliki tingkat kecerahan dan kegelapan yang rendah. Perbedaan dari kedua jenis gambar yaitu, tingkat kejelasan gambar terutama warnanya. Pengujian dilakukan menggunakan 2 jenis gambar tersebut masing-masing 30 gambar.

Gambar tersebut berperan sebagai citra pelindung dengan pesan rahasia yang acak. Gambar sebelum steganografi dan setelah steganografi dibandingkan dengan cara menghitung perbedaan nilai PSNR dan MSE. Hasil dari pengujian tersebut dapat dilihat pada tabel 1 untuk gambar *high contrast* dan tabel 2 untuk gambar *low contrast*.

Tabel 1. Hasil Pengujian Gambar High Contrast

No	Kunci Publik Anda	Kunci Publik Teman	Common Key	PSNR	MSE
1	a883aab867	75769881c5	a5833c81c5	93.42699252	2.95E-05
2	ac57a393a9	acb199b771	91513333a1	97.78827528	1.08E-05
3	ac57a393a9	a63963a3c1	9c19a93911	95.15401438	1.98E-05
4	975b5c98b8	a91bb86819	39175c9811	95.73093533	1.74E-05
5	538719a598	ab733acac7	c983131c18	98.02288743	1.03E-05
6	58ba53cc11	579659c3a6	883a831111	93.63888551	2.81E-05
7	a1b19517a7	53c6655838	c1c1981898	96.39498716	1.49E-05
8	a1b19517a7	7376361173	a1b13811a3	96.91070691	1.32E-05
9	a1b19517a7	a61839191b	911131191b	97.96511259	1.04E-05
10	a1b19517a7	5c56aa99c6	c1513c1916	96.85885544	1.34E-05
11	a1b19517a7	7ca8aa9a1a	a1413c1a1a	94.70196849	2.20E-05
12	79763891a5	711c8b86c9	711c181111	92.52754639	3.63E-05
13	79763891a5	a76b163cb7	a962153145	95.99602742	1.63E-05
14	79763891a5	513ab7a8a6	513a983198	96.96361955	1.31E-05
15	79763891a5	511855a738	5115153195	96.61786627	1.42E-05
16	79763891a5	5a1ccb8c31	531c181191	99.17596426	7.86E-06
17	79763891a5	5336981989	53373811c1	100.3772267	5.96E-06
18	5867ca18c5	a8b6bc5931	c826c11111	96.77205435	1.37E-05
19	5867ca18c5	a33a911173	c13a1111c1	96.391823	1.49E-05
20	5867ca18c5	5ccc5b1815	8cccc5b1815	100.4693408	5.84E-06
21	5867ca18c5	733c9931a9	513c131111	96.023348	1.62E-05
22	5867ca18c5	a85c876931	c88cca1111	100.1989422	6.21E-06
23	5867ca18c5	7a3b1a65b1	5c3b1915c1	93.54437984	2.88E-05
24	97b3b68c85	78aa835b88	9849835c85	98.59434	8.99E-06
25	97b3b68c85	53791c763b	13b31c8c15	95.77436694	1.72E-05
26	97b3b68c85	a33a911173	3399311181	94.13837258	2.51E-05
27	97b3b68c85	568aca135a	1689ca115c	97.51125517	1.15E-05
28	97b3b68c85	a791c73b37	3731c61c15	96.63654224	1.41E-05
29	aa17937bba	5767931c6c	ca17991c21	96.00877313	1.63E-05

30	a1abab7aa8	a979333b6a	91a39934ac	96.84294238	1.35E-05

Tabel 2. Hasil Pengujian Gambar Low Contrast

No	Kunci Publik Anda	Kunci Publik Teman	Common Key	PSNR	MSE
1	5175577a17	7761363768	5161163a18	97.99424044	1.03E-05
2	5175577a17	a1839a339a	c1811a391a	98.43602616	9.32E-06
3	5175577a17	78567c6bb8	51585c6418	98.11851577	1.00E-05
4	5175577a17	51585c6418	81a8c37318	99.01982712	8.15E-06
5	5175577a17	a69b157118	c185157118	97.89092007	1.06E-05
6	5a7a35c738	77cb973a9c	5ac4351a3c	100.1240146	6.32E-06
7	5a7a35c738	a69b157118	ca9418c118	98.2080642	9.82E-06
8	5a7a35c738	551671b988	8c1a31c918	94.8387168	2.13E-05
9	5a7a35c738	785979565c	5c5331c61c	94.99380272	2.06E-05
10	5a7a35c738	a67a71c9c3	ca79311911	99.75471983	6.88E-06
11	971b89758c	7788c9bc98	9718c9bc1c	95.39347189	1.88E-05
12	971b89758c	a75a197776	371419758c	98.1187566	1.00E-05
13	7a7a55bb53	53731a91c1	59791c31c1	94.98524426	2.06E-05
14	7a7a55bb53	a75a197776	aa5911bb53	97.15887552	1.25E-05
15	7a7a55bb53	9a51c833c5	9951c599c1	95.08724908	2.02E-05
16	7a7a55bb53	59bbaacc79	53b4cccc53	99.61991957	7.10E-06
17	7a7a55bb53	a7386b6671	aa3c852251	96.84488546	1.34E-05
18	aa8ba719ac	7b5c397959	a45c9919c1	96.02095819	1.63E-05
19	aa8ba719ac	a671b75c76	9a814711ac	98.7106092	8.75E-06
20	aa8ba719ac	a979c78b85	93831713cc	98.91740575	8.34E-06
21	a9c695c8b9	7183638559	a1c391c559	95.36496328	1.89E-05
22	a9c695c8b9	75b9575691	a1c915c531	97.98839922	1.03E-05
23	a179b6b388	a77739c5b5	917999c185	92.73068998	3.47E-05
24	a179b6b388	79813c9513	a1819c3111	93.13663684	3.16E-05
25	a179b6b388	9755a11156	3151411155	98.37903945	9.44E-06
26	73cacc8a58	516c7b1771	51c1cc1a51	97.50643796	1.15E-05
27	73cacc8a58	58b998717b	51c31c8158	97.20048003	1.24E-05
28	73cacc8a58	5189999c18	51c3111118	95.75049382	1.73E-05
29	73cacc8a58	a17ab537a7	a1c9cc1ac8	87.87338553	0.000106106
30	73cacc8a58	a8cc6ab7c5	a111c18ac5	95.83912236	1.69E-05

Berdasarkan hasil uji coba steganografi pada *low contrast* dan *high contrast* dapat dilihat bahwa gambar *low contrast* ke 29 memiliki nilai PSNR paling rendah dari 60 data yang diujikan dengan nilai 87.873385532736 dan MSE paling tinggi dengan nilai 0.000106 yang dapat dilihat dari Tabel 2.

Gambar 6. Hasil Uji Low Contrast 29

Dapat dilihat juga gambar *high contrast* ke 20 memiliki nilai PSNR paling tinggi dari 60 data yang diujikan dengan nilai 100.4693408 dan MSE paling rendah 5.84E-06 dapat dilihat di Tabel 1.

Gambar 7. Hasil Uji Gambar High Contrast 20

SIMPULAN

Berdasarkan hasil uji coba diatas penulis mengambil kesimpulan bahwa gambar *high contrast* memiliki nilai rata-rata PSNR 96,539692 dan nilai rata-rata MSE 0,0000159 sedangkan gambar *low contrast* memiliki nilai rata-rata nilai PSNR yaitu 96,7335291 dan rata-rata nilai MSE yaitu 0,0000173.

DAFTAR PUSTAKA

[1] Assafli, H. T., Hashim, I. A., & Naser, A. A. 2021. *Advanced Encryption Standard (AES) Acceleration and Analysis Using Graphical Processing Unit (GPU). Applied Nanoscience (Switzerland).* https://doi.org/10.1007/s13204-021-01985-3

[2] Aziz Fikhri, A. 2018. *Implementasi Steganografi Text To Image Menggunakan Metode One BIT Least Significant BIT Berbasis Android. Jurnal Infomedia*, *3*(1).

[3] Kaur, S., Bansal, S., & Bansal, R. K. 2021. *Image Steganography For Securing Secret Data Using Hybrid Hiding Model. Multimedia Tools and Applications*, *80*(5), 7749–7769. https://doi.org/10.1007/s11042-020-09939-7

[4] Khaldi, A. 2021. *Hellman Key Exchange Through Steganographied Images Dialogos* (Issue 1).

[5] Laila, N., & Rms, A. S. 2018. *Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra Implementation of LSB Steganography with Vigenere Cipher Encryption in Image*. *Computer Science Informatics Journal*, *1*(2).

[6] Manoj, I. V. S. 2010. *Cryptography And Steganography*. Kluwer Academic.

[7] Muttaqin, K., & Rahmadoni, J. 2020. *Analysis and Design of File Security System AES (Advanced Encryption Standard) Cryptography Based.* Dalam *Journal of Applied Engineering and Technological Science* (Vol. 1, Issue 2).

[8] Purohit, K., Kumar, A., Upadhyay, M., & Kumar, K. 2019. *Symmetric Key Generation andDistribution Using Diffie-HellmanAlgorithm*. http://www.springer.com/series/11156

[9] Rubinstein-Salzedo, S. 2018. Cryptography. *Springer International Publishing AG*. http://www.springer.com/series/3423

[10] Siswanto, A., Arta, Y., Kadir, E. A., & Bimantara. 2021. *Text File Protection Using LeastSignificant Bit (LSB) Steganographyand Rijndael Algorithm*. http://www.springer.com/series/15179

[11] Sammut, Claude, dan Geoffrey I. Webb. 2011. *Encyclopedia of Machine Learning*.

[12] Setiadi, De Rosal Igantius Moses. 2021. *"PSNR vs SSIM: Imperceptibility Quality Assessment for Image Steganography." Multimedia Tools and Applications* 80(6):8423–44. doi: 10.1007/s11042-020-10035-z.

[13] A. Farisi, *"Analisis Kinerja Algoritma Kriptografi Kandidat Advanced Encryption Standard (AES) pada Smartphone,"* 2018.

[14] E. Suryadi, M. Subli, and K. Nurwijayanti, *"Penerapan Sistem Keamanan Video Menggunakan Kriptografi Algoritma Kunci Simetris," Jurnal Teknik Informatika dan Sistem Informasi*, Vol. 9, 2022.