Steganografi Citra Digital Menggunakan Pendekatan *Least Significant Bit* dan *Discrete Cosine Transform*

Rizkia Fahmi Noviansyah Imanudin[1], Iwan Kustiawan[2*], Siscka Elvyanti[3]

[1,2,3] *Program Studi Teknik Elektro UPI*
Jl. Dr. Setiabudhi No. 207 Bandung 40154 INDONESIA
rfnoviansyah@student.upi.edu[1], iwan_kustiawan@upi.edu[2*], sisckael@upi.edu[3]

Intisari— **Keamanan siber adalah salah satu aset terpenting yang harus dijaga selama proses transmisi data melalui Internet. Salah satu strategi untuk melindungi informasi penting adalah steganografi yang merupakan teknik penyembunyian informasi ke dalam multimedia seperti teks, audio, gambar digital, dan video. Penelitian ini bertujuan untuk mengimplementasikan metode steganografi pada file citra digital menggunakan skema *Least Significant Bit* (LSB) dan *Discrete Cosine Transform* (DCT). Parameter uji kinerja yang diukur adalah *Peak Signal-to-Noise Ratio* (PSNR), ketahanan terhadap kompresi, dan transparansi file yang disisipkan pesan dengan menghitung *Mean Opinion Score* (MOS). Kami menggunakan pendekatan *water fall* dalam penelitian ini. Hasil penelitian menunjukkan bahwa nilai PSNR dengan metode LSB mendapatkan hasil yang lebih baik dibandingkan dengan metode LSB lainnya. Sedangkan dari segi ketahanan terhadap kompresi, file citra digital memiliki ketahanan terhadap kompresi karena pesan yang diekstrak dalam file tidak mengalami perubahan. Berdasarkan pengolahan data MOS, metode LSB mengungguli persepsi pengguna dibanding metode lainnya. Hal ini diakibatkan karena metode DCT menghasilkan sedikit distorsi pada citra digital yang berpengaruh pada kejernihan dari berkas.**

Keywords— **Steganografi, least significant bit, discrete cosine transform, peak signal-to-noise ratio.**

I. PENDAHULUAN

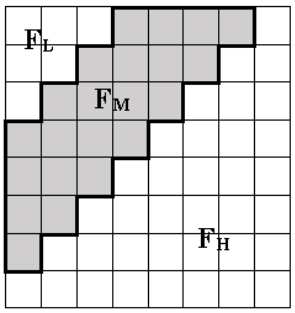
Beberapa metode untuk melindungi informasi penting sedang dikembangkan baru-baru ini. Salah satu metode yang sedang dikembangkan adalah Steganografi. Steganografi dan kriptografi melayani tujuan yang sama, tetapi keduanya digunakan dan cara kerjanya sedikit berbeda. Kriptografi melindungi data yang dikirim, sedangkan steganografi menyembunyikan data dalam multimedia seperti teks, gambar, video, dan audio hingga tidak ada [1]. Steganografi telah digunakan sejak abad ke-5 SM, misalnya pada tato kulit kepala. Steganografi memiliki kegunaan baru dalam ilmu pengetahuan seiring berkembangnya teknologi digital [2]. Metode LSB dan DCT merupakan salah satu implementasi dari pendekatan setganografi dengan parameter utama uji kinerja meliputi transparansi, robustness, dan rasio nilai signal to noise atau PSNR [3]-[6].

Terdapat sejumlah kriteria utama dalam proses steganografi yang baik. Antara lain, *fidelity*, kualitas berkas yang digunakan sebagai *host* tidak mengalami banyak perubahan setelah penyematan pesan. *Imperceptible* yang berarti berkas hasil steganografi sulit dibedakan dengan berkas *host* yang asli sehingga pesan tidak dapat terasa keberadaannya secara inderawi. *Recovery* yaitu pesan yang sudah disematkan kedalam *host* dapat diekstrak atau dimunculkan kembali[8].

Satu *byte* berisi delapan bit. Ada 2 macam bit yaitu Most Significant Bit (MSB) dan Least Significant Bit (LSB). Misalnya pada byte 10010110, bit pertama yang merupakan angka 1 adalah bit MSB, dan bit terakhir yang merupakan angka 0 adalah bit LSB. Metode ini hanya mengubah bit LSB [9]. DCT banyak digunakan sebagai teknik transformasi frekuensi dalam pemrosesan sinyal dan citra dimana contoh penggunaannya adalah steganografi dan kompresi sinyal [10]. DCT mengubah citra dari domain spasial menjadi domain frekuensi. Penyematan data menggunakan DCT memiliki keuntungan yaitu data dapat disimpan dalam bit-bit koefisien yang tidak penting. Citra hasil transformasi dengan DCT dibagi menjadi blok-blok dengan ukuran 8 x 8 terlebih dahulu. Setiap blok ditransformasikan dengan persamaan (1) dan menghasilkan blok dengan dimensi yang sama yang dinyatakan dalam domain frekuensi [11].

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7}f(x,y)\cos\left[\frac{\pi(2x+1)u}{16}\right]\cos\left[\frac{\pi(2x+1)v}{16}\right] \quad (1)$$

Frekuensi bagian tengah dari citra dijadikan tempat menyembunyikan informasi rahasia karena frekuensi bagian tengah tahan dari sebuah komrpesi atau gangguan lainnya. Daerah host yang dinyatakan sebagai frekuensi bagian tengah dari 8x8 blok DCT ditunjukkan pada Gambar 1.



Gambar 1. Tata letak sebuah host DCT

F_L (frequency low) dinyatakan sebagai komponen frekuensi terendah, dan F_H (frequency high) dinyatakan sebagai komponen tertinggi, sementara F_M (frequency middle) adalah daerah dengan ketahanan tambahan terhadap teknik pengurangan pemampatan dengan tujuan mencegah perubahan yang signifikan pada citra sampul [12]. Setelah citra digital

menjadi bentuk frekuensi, penyematan data dilakukan dengan menggunakan proses LSB pada frekuensi menengah yang memiliki sifat *lossy*[13].

Citra merupakan hasil dari sistem perekam data. Citra dapat bersifat optik berupa foto, bersifat analog yang mempunyai rupa sinyal-sinyal pada video di monitor televisi, atau bersifat digital yang disimpan pada suatu media penyimpanan. Citra yang bersifat digital mudah untuk dimanipulasi contohnya seperti, modifikasi warna dan kecerahan setiap warna, merubah ukuran dari citra dan lain-lain [14]. Secara matematis, fungsi kontinyu dengan intensitas cahaya pada bidang dua dimensi adalah citra. Komputer dapat mengolah citra dengan cara merepresentasikan suatu citra secara numerik dengan nilai-nilai diskrit. Citra digital umumnya dapat dibagi menjadi 3, warna image atau RGB (Red, Green, Blue) yang memiliki warna pada masing masing pikselnya berupa warna merah, hijau, dan biru. Citra digital yang kedua adalah citra digital hitam dan putih atau *grayscale* yang mempunyai warna gradasi dari putih sampai hitam pada setiap pikselnya, dan citra digital Binary Image yang hanya memiliki warna hitam atau putih pada setiap pikselnya [15].

Format .JPEG atau Joint Photographic Experts Group merupakan sebuah standar kompresi internasional. Dibuat untuk mendukung penggunaan citra digital *grayscale* ataupun berwarna dan grafis yang memiliki kualitas tinggi pada perangkat digital. Format .JPEG mulai dikembangkan sejak tahun 1982 merupakan format citra digital yang populer [16]. PNG atau Portable Network Graphic, merupakan citra digital yang menggunakan kompresi *lossless*, format ini sudah didukung transparansi dan portable. Format ini mempunyai kemampuan untuk menangani warna sampai 48 bit [17].

PSNR merupakan perbandingan nilai maksimum dari sinyal yang diukur dengan besar derau dan berpengaruh terhadap sinyal tersebut. Biasanya PSNR diukur dalam satuan decibel. Citra yang baik memiliki PSNR antara 20 dB ~ 40 dB. PSNR bisa ditentukan dengan menggunakan rumus:

$$PSNR = 10\ log\left(\frac{MAXi^2}{\sqrt{MSE}}\right)$$
$$= 20\ log\left(\frac{MAXi}{\sqrt{MSE}}\right)$$
$$= 20\log(MAX) - 10\log(MSE)$$

dengan:

- PSNR = nilai PSNR (dalam dB)
- MAXi = nilai maksimum piksel i
- $MSE = \frac{\sum_{y=1}^{m}\sum_{x=1}^{n}[I(x,y)-I'(x,y)]2}{mn}$

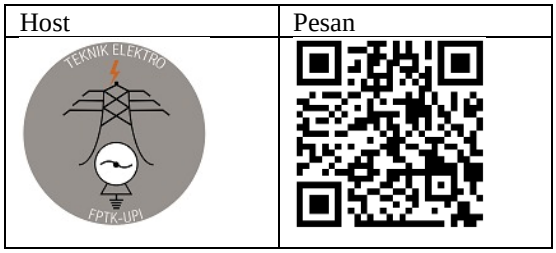
m dan *n* adalah baris citra dan kolom citra, untuk *I* dan *I'* adalah citra asli dan citra rekonstruksi [18].

International Telecommunication Union (ITU) telah menentukan skor opini sebagai nilai pada skala yang telah ditentukan yang diberikan subjek untuk mengetahui pendapat tentang suatu sistem. MOS adalah rata-rata dari nilainya. MOS sudah sukses dalam menilai kualitas suara, dan MOS semakin populer digunakan sebagai penilai kualitas media lainnya seperti konten audio, citra, dan video. Skala nilai MOS menggunakan poin dari 1 – 5 (*Excellent, Good, Fair, Poor, Bad*) [12].

II. METODE

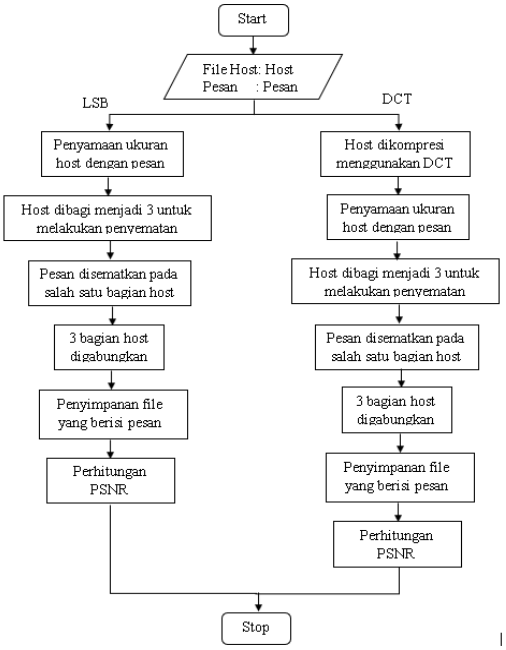
Penelitian ini menggunakan metode *waterfall* karena metode ini memiliki tahapan yang dilakukan berurutan dan berkelanjutan. Tahapan yang dilakukan diantaranya studi literatur, analisis kebutuhan, pengumpulan *resources* (source code, pesan yang akan disisipkan, file gambar untuk *host)*, penyusunan algoritma, pengujian dan analisis hasil percobaan.

Untuk melakukan proses steganografi dibutuhkan 2 gambar, yaitu untuk *host* dan untuk pesan. Gambar yang digunakan untuk *host* merupakan sebuah logo, dan gambar yang digunakan untuk pesan merupakan sebuah QRcode. Gambar percobaan ditampilkan seperti pada Gambar 2. Gambar yang digunakan untuk host dan pesan ini memiliki ukuran 300x300 piksel dengan format .JPG, dan .PNG untuk mengukur kualitas ketahanan terhadap steganografi.

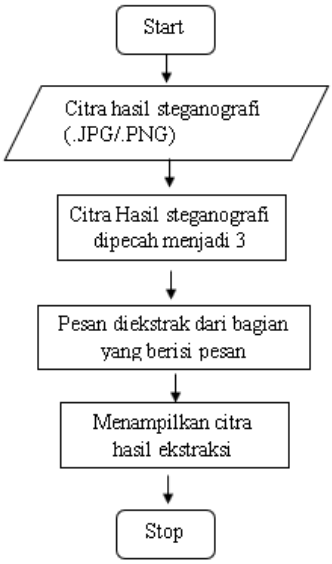


Gambar 2. Gambar yang digunakan untuk host dan pesan

Berikutnya adalah penyusunan algoritma yang terdiri algoritma penyisipan pesan dan ekstraksi pesan. Algoritma penyisipan pesan dan ekstraksi pesan ditunjukkan pada Gambar 3 dan Gambar 4.



Gambar 3. Algoritma penyisipan pesan



Gambar 4. Algoritma ekstraksi pesan

Untuk mendapat nilai opini subjektif dari responden, dilakukan perhitungan MOS terhadap perbandingan berkas citra digital yang asli dengan citra digital hasil steganografi. MOS merupakan nilai rata-rata dari data opini yang didapat. Pengambilan data dilakukan dengan menggunakan angket secara daring yang disebar ke responden. Bobot nilai yang digunakan merupakan poin dari 1 – 5.

Tabel 1 Skala MOS penilaian berkas citra digital

Skala MOS	Kualitas	Implementasi pilihan jawaban dalam kuisioner
5	Sangat Baik	Perbedaan tidak terlihat
4	Baik	Ada perbedaan tetapi tidak terlalu terlihat
3	Cukup	Sedikit berbeda
2	Kurang	Berbeda
1	Buruk	Sangat berbeda

Penilaian dilakukan dengan membandingkan berkas citra digital yang asli dengan citra digital hasil steganografi. Berkas citra digital diperlihatkan pada form asesmen, lalu responden menjawab pertanyaan yang telah dibuat. Data yang didapat dari hasil uji coba, dan uji terhadap responden dianalisis dengan cara membandingkan setiap hasil dari format .JPG dan .PNG.

III. HASIL DAN PEMBAHASAN

Proses penyisipan pesan dilakukan dengan menggunakan *software* MATLAB. Proses ini dibagi berdasarkan metode LSB dan DCT terhadap *host* sebagai sampul dengan jenis format .JPG dan .PNG. PSNR dihitung untuk mengetahui kualitas sinyal dari berkas berdasarkan tingkat rasio sinyal puncak terhadap derau. Perbandingan nilai PSNR setiap berkas citra digital ditampilkan pada Tabel 2. PSNR setiap berkas memiliki nilai yang berbeda. Nilai PSNR pada berkas dengan format .JPG mempunyai selisih 0,041 dB, dengan proses steganografi menggunakan metode LSB menghasilkan PSNR yang lebih besar dibandingkan metode DCT. Nilai PSNR pada berkas dengan format .PNG mempunyai selisih 0.793 dB, dengan proses steganografi menggunakan metode LSB menghasilkan PSNR yang lebih besar dibandingkan metode DCT. Hasil ini menunjukkan, proses steganografi dengan metode LSB memiliki nilai PSNR yang lebih besar dibandingkan metode DCT.

Tabel 2. Hasil perhitungan nilai PSNR

No.	**Metode**	**Format**	**Nilai PSNR (dB)**
1.	LSB	.JPG	32,7761
2.		.PNG	33,3950
3.	DCT	.JPG	32,7351
4.		.PNG	32,6020

Untuk mengukur ketahanan terhadap kompresi dilakukan proses konversi atau kompresi pada format berkas citra digital .JPG menjadi .PNG. Jika pesan diekstrak dari berkas yang sudah dikompresi tidak sesuai dengan aslinya, maka berkas yang menjadi *host* tidak dapat menahan kompresi.

Tabel 3 Hasil Ekstraksi Pesan

No.	Metode	Gambar Asli	Gambar Hasil Ekstraksi
1.	LSB		
2.	DCT		
3.	LSB		
4.	DCT		

Hasil ekstraksi pesan untuk setiap berkas citra digital sama dengan pesan aslinya (Tabel 3). Hal ini menjadi bukti bahwa berkas citra digital hasil steganografi tahan terhadap kompresi .PNG. Hasil steganografi citra digital yang dinilai responden berjumlah empat buah dengan format dan metode steganografi yang diterapkan berbeda satu sama lain. Jawaban yang didapat dari 30 orang responden dikonversi menjadi skor nilai dengan rentang 1-5. Nilai MOS diperoleh dari rata-rata jawaban responden (Tabel 4).

Tabel 4 Hasil perhitungan MOS

No.	Metode	Pertanyaan	Format	Nilai PSNR (dB)	Klasifikasi
1.	LSB	1	.JPG	2,8333	Kurang
2.	DCT	2		2,7666	Kurang
3.	LSB	3	.PNG	3,133	Cukup
4.	DCT	4		3,1	Cukup

Citra digital yang telah melalui proses steganografi metode LSB dan DCT dibandingkan kualitasnya berdasarkan tiga faktor yaitu kualitas dari berkas dengan mengukur PSNR, ketahanan terhadap kompresi, dan transparansi dengan mengukur MOS.

Tabel 5 Perbandingan berkas hasil steganografi

No.	Metode	Format	PSNR (dB)	MOS	Ketahanan	Hasil Ekstraksi
1.	Least Significant Bit (LSB)	.JPG	32,7761	2,8333	Ada	Sama
2.	Discrete Cosine Transform (DCT)		32,7351	2,7666	Ada	Sama
3.	Least Significant Bit (LSB)	.PNG	33,3950	3,133	Ada	Sama
4.	Discrete Cosine Transform (DCT)		32,6020	3,1	Ada	Sama

Perbandingan kualitas berkas hasil steganografi ditunjukkan oleh Tabel 5. Pada parameter PSNR, metode berpengaruh terhadap nilai PSNR dimana nilai PSNR dari berkas yang melalui metode LSB memiliki nilai yang lebih baik dibandingkan metode DCT. Nilai MOS dari berkas yang melalui metode LSB lebih baik dibandingakan dengan metode DCT, hal ini diakibatkan karena metode DCT menghasilkan sedikit distorsi pada citra digital yang berpengaruh pada kejernihan dari berkas. Ketahanan pada berkas diuji dengan melakukan ekstraksi pesan setelah melalui proses konversi berkas dengan kompresi .PNG. Pesan yang diekstrak dari setiap berkas citra digital berformat .JPG maupun format .PNG tidak mengalami perubahan dari pesan asli, hal ini disebabkan karena kompresi .PNG memiliki sifat kompresi *lossless*.

Hasil yang diperoleh sejalan dengan penelitian yang dilakukan oleh [12][19] yang mendapat nilai PSNR untuk mengukur parameter *fidelity* atau kualitas dari citra pada metode LSB lebih baik daripada metode DCT. Adapun penelitian yang dilakukan oleh [20] berbeda dengan penelitian yang dilakukan oleh M Khalaf dkk. [13] yang mendapatkan hasil PSNR pada metode DCT lebih besar dibandingkan metode LSB. Hal demikian karena adanya perbedaan langkah penyematan pesan kedalam host.

IV. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, proses steganografi dengan berkas *host* dan pesan berupa citra digital menggunakan metode LSB dan DCT berjalan dengan baik. Nilai PSNR pada berkas hasil steganografi dengan metode LSB lebih unggul dibandingkan hasil steganografi dengan metode DCT. Dari segi ketahanan terhadap kompresi, metode LSB dan DCT memiliki kesesuaian pesan ketika diekstrak, lalu ketika dilakukan kompresi .PNG juga pesan yang diekstrak sesuai dengan pesan aslinya. Nilai MOS digunakan untuk mengukur transparansi, metode LSB memiliki nilai yang lebih baik dibandingkan metode DCT. Faktor yang menyebabkan perbedaan pada hasil steganografi antara metode LSB dan DCT adalah format berkas citra digital yang menjadi *host* dan kompresi yang dilakukan dalam proses steganografi dengan metode DCT.

REFERENSI

[1] A. El-Sayed, G. Attiya, And A. Fkirin, "Steganography Literature Survey, Classification and Comparative Study," Communications on Applied Electronics, Vol. 5, No. 10, Pp. 13–22, 2016, Doi: 10.5120/Cae2016652384.

[2] M. Kwiatkowska And L. Swierczewski, "Steganography-Coding and Intercepting the Information from Encoded Pictures in The Absence of Any Initial Information," 2014.

[3] F. G. Beram, "Effective Parameters of Image Steganography Techniques," International Journal of Computer Applications Technology and Research, Vol. 3, No. 6, Pp. 361–363, 2014, Doi: 10.7753/Ijcatr0306.1009.

[4] D. C. Prabhu, S. R. Nivedha, A. Kumar, S. K, And A. D, "Multiple Image Steganography Using Lsb-Dct Technique," International Journal of Engineering Research & Technology (Ijert), Vol. 4, No. 22, Pp. 1–5, 2016.

[5] K. Amarendra, V. N. Mandhala, B. C. Gupta, G. G. Sudheshna, And V. V. Anusha, "Image Steganography Using Lsb," International Journal of Scientific and Technology Research, Vol. 8, No. 12, Pp. 906–909, 2019.

[6] M. D. Khatavkar And A. S. Mali, "A Image Security With Image Steganography Using Dct Coefficient And Encryption," International Journal Of Innovations In Engineering Research And Technology [Ijiert, Vol. 3, No. 9, Pp. 1–8, Sep. 2016.

[7] S. Kundra And N. Madaan, "A Comparative Study of Image Steganography Techniques," Vol. 3, No. 4, Pp. 293–297, 2014.

[8] Rihartanto, D. S. B. Utomo, And A. Rizal, "Implementasi Image Tilling Pada Penyembunyian Pesan Menggunakan Lsb," Proceeding Sintak, Pp. 186–192, 2019.

[9] H. P. Winasih, E. Hari Rachmawanto, C. A. Sari, And D. Rosal Ignatius Moses Setiadi, "Implementation of Lsb-Rsa Algorithm for The Authenticity of The Jpg File Certificate," In Proceedings - 2020 International Seminar on Application for Technology of Information and Communication: It Challenges for Sustainability, Scalability, And Security in The Age of Digital Disruption, Isemantic 2020, Sep. 2020, Pp. 40–44. Doi: 10.1109/Isemantic50169.2020.9234254.

[10] A. Sheidaee And L. Farzinvash, "Novel Image Steganography Methode Based on Dct And Lsb," 9th International Conference on Information and Knowledge Technology (Ikt 2017)9, Pp. 116–123, 2017.

[11] M. Baziyad And M. S. Obaidat, "On the Importance of The Dct Phase for Image Steganography Schemes," In 2020 Ieee 5th International Conference on Computing Communication and Automation, Iccca 2020, Oct. 2020, Pp. 791–795. Doi: 10.1109/Iccca49541.2020.9250849.

[12] N. A. Amrullah, "Perbandingan Algoritma Lsb Dan Dct Pada Steganografi," 2008.

[13] A. A. M Khalaf Et Al., "Hiding Data in Images Using Dct Steganography Techniques with Compression Algorithms Machine Learning and Prediction Techniques for Biomedical Signal (Prediction Behavior Technique) View Project Secure Decentralized Energy Systems View Project Hiding Data in Images Using Steganography Techniques with Compression Algorithms," Telkomnika, Vol. 17, No. 3, Pp. 1168–1175, 2019, Doi: 10.12928/Telkomnika.V17i3.

[14] D. Zalukhu, "Aplikasi Otentikasi Citra Digital Dengan Metode Adaptive Data Hiding," Means (Media Informasi Analisa Dan Sistem), Vol. 2, No. 2, Pp. 109–116, 2017, [Online]. Available: Http://Ejournal.Ust.Ac.Id/Index.Php/Jurnal_Means/Http://Www.Stmik-Budidarma.Ac.Id//

[15] R. D. Kusumanto And A. N. Tompunu, "Pengolahan Citra Digital Untuk Mendeteksi Obyek Menggunakan Pengolahan Warna Model Normalisasi Rgb," 2011.

[16] A. Ardiansyah, N. Hardi, And W. Gata, “Identifikasi Dan Recovery File Jpeg Dengan Metode Signature-Based Carving Dalam Model Automata,” Komputika : Jurnal Sistem Komputer, Vol. 9, No. 1, Pp. 75–83, Apr. 2020, Doi: 10.34010/Komputika.V9i1.2733.
[17] Hendri, “Kompresi Citra Dari Format Bmp Ke Format Png,” Jurnal Time, Vol. Iii, No. 1, Pp. 27–31, 2014.
[18] N. Arif, A. Amrullah, U. D. Nuswantoro, And J. N. I. No, “Perbandingan Algoritma Lsb Dan Dct Pada Steganografi,” Pp. 1–9, 2008.
[19] D. Singla And R. Syal, “Data Security Using Lsb & Dct Steganography in Images,” International Journal of Computational Engineering Research, Vol. 2, No. 2, Pp. 359–364, 2012.
[20] D. W. Sari and I. Pratama, “Analisis Dan Perbandingan Teknik Steganografi Citra Digital Algoritma Lsb Dan Dct Dengan Menggunakan Algoritma Kriptografi Rc4,” 2019, [Online]. Available: Https://Www.Researchgate.Net/Publication/338124748.