YAYASAN AKRAB PEKANBARU
Jurnal AKRAB JUARA
Volume 6 Nomor 1 Edisi Februari 2021 (30-40)

3

IMPLEMENTASI STEGANOGRAFI IMAGE PROCESSING DAN ENKRIPSI AES MENGGUNAKAN OPENSTEGO

Dewi Laksmiati
Universitas Bina Sarana Informatika
(Naskah diterima: 1 Januari 2021, disetujui: 30 Januari 2021)

Abstract

Nowadays digital communication is very common. With digital communication we can convey messages quickly and accurately. However, digital communication still carries the risk of tapping information. Therefore, we need a method of communication that can be done through digital media but with a higher level of data security and confidentiality. In this paper, we will discuss the application of hidden and encrypted messages, where messages are encrypted and inserted in a photo file. The encrypted secret message is embedded in image bits. To then be decrypted by the receiver. Hiding messages in secret is also called steganography, a science about hiding messages. And so that messages are more confidential, AES encryption is added. This process will be carried out using the OpenStego open source application
Keywords: *Secure Communication, Steganography, Encryption, OpenStego*

Abstrak

Saat ini komunikasi secara digital merupakan hal yang sangat umum. Dengan komunikasi digital kita dapat menyampaikan pesan secara cepat dan akurat. Namun komunikasi digital masih menyimpan resiko penyadapan informasi. Karenanya dibutuhkan sebuah metode komunikasi yang dapat dilakukan melalui media digital namun dengan tingkat keamanan data dan kerahasiaan yang lebih tinggi. Dalam penulisan ini akan dibahas penerapan pesan tersembunyi dan terenkripsi, dimana pesan dienkripsi dan disisipkan di dalam sebuah file foto. Pesan rahasia yang terenkripsi disisipkan dalam bit-bit gambar. Untuk kemudian didekripsi oleh penerima. Penyembunyian pesan secara rahasia ini disebut juga steganografi, sebuah ilmu tentang menyembunyikan pesan. Dan agar pesan lebih terjaga kerahasiaannya, ditambahkan enkripsi AES. Proses ini akan dilakukan menggunakan aplikasi open source OpenStego.
Kata Kunci: Keamanan Komunikasi, Steganografi, Enkripsi, OpenStego

I. PENDAHULUAN

Dalam komunikasi, pada beberapa keadaan tidak hanya membutuhkan kecepatan dan ketepatan komunikasi, namun juga komunikasi yang aman dan tersembunyi. Hal ini menyebabkan steganografi cukup menarik bagi sebagian pihak dika-

renakan kelebihannya dalam perlindungan keamanan komunikasi melalui internet.

Steganografi merupakan teknik menyembunyikan informasi dan memberikan tanda pengenal. Steganografi merupakan salah satu metode untuk menyembunyikan pesan rahasia yang aman dan sulit dideteksi oleh penglihatan manusia, pesan dapat berupa teks, gambar, audio, video dengan kualitas data yang terjaga. Kata steganografi berasal dari bahasa Yunani yang berarti surat tertutup atau tertutup, yang mencakup berbagai cara komunikasi rahasia yang sangat efisien.

Dalam pengamanan komunikasi, biasanya hanya satu pendekatan keamanan yang digunakan pada satu waktu oleh pengguna baik kriptografi atau steganografi. kombinasi teknik steganografi dan kriptografi adalah teknik keamanan yang paling berguna dan kuat, juga dapat memainkan peran yang sangat penting dalam bidang ini.

Awalnya, steganografi ini melibatkan penggunaan metode sederhana, misalnya membotakkan rambut pembawa pesan, lalu pesan ditulis di kulit kepala, kemudian setelah rambut tumbuh dan menutupi pesan di kulit kepala. Maka pembawa pesan pergi ke tujuan untuk membawa pesan rahasia yang disembunyikan di bawah rambut. Kemudian di tempat tujuan kembali dibotakkan untuk melihat pesan. Setelah pengetahuan lebih maju, digunakanlah tinta tak terlihat, pengaturan karakter. Kemudian pada era teknologi informasi digunakan tanda tangan digital, saluran komunikasi yang diacak, dan spektrum komunikasi yang tersebar. Penyisipan informasi rahasia memiliki peran penting dalam komunikasi data. Data dengan algoritma steganografi harus memiliki keamanan, kapasitas, transparansi dan ketahanan / elemen yang kuat.

Ada dua proses utama dalam steganografi, yaitu penyematan dan penggalian pesan atau informasi dalam media samaran. Embedding adalah proses memasukkan pesan atau informasi ke dalam media samaran, sedangkan ekstraksi adalah proses mengartikan pesan yang disembunyikan dalam gambar stego. Pesan yang akan tercakup menjadi gambar membutuhkan dua file. Pertama adalah gambar asli yang tidak dimodifikasi yang akan menangani pesan tertutup, yang disebut gambar sampul. File kedua adalah informasi pesan yang dicakup. Sebuah pesan dapat berupa teks biasa, teks chip, gambar lain, atau apapun yang dapat disematkan ke aliran bit .

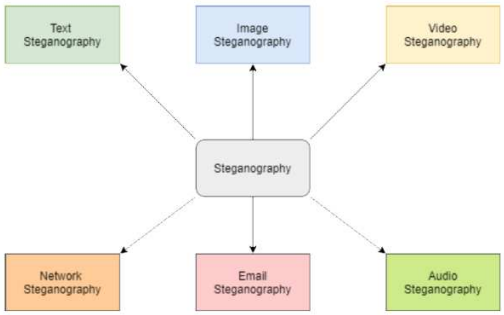
II. KAJIAN TEORI

Steganografi

Steganografi adalah proses penyembunyian pesan rahasia di dalam pesan yang lebih besar sedemikian rupa agar seseorang tidak menyadari keberadaan atau isi pesan yang disembunyikan tersebut. Tujuan Steganografi adalah untuk melindungi komunikasi rahasia pada dua pihak. Tidak seperti kriptografi, yang menyembunyikan isi pesan rahasia, steganografi menyembunyikan pesan yang dikomunikasikan. Meskipun steganografi tidak sama dengan kriptografi, terdapat banyak analogi pada keduanya, dan sebagian orang mengklasifikasikan steganografi sebagai bentuk kriptografi karena komunikasi tersembunyi termasuk bentuk pesan rahasia.

Steganografi menggunakan beberapa media perantara, diantaranya:

1. *Text Steganography*
2. *Image Steganography*
3. *Video Steganography*
4. *Audio Steganography*
5. *Network Steganography*

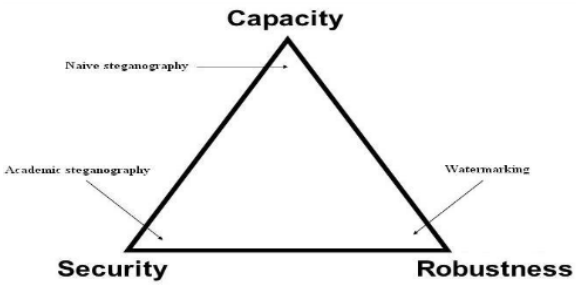


Gambar 1. Media perantara steganografi

Karakteristik Steganografi

Tiga kriteria digunakan untuk mengklasifikasikan algoritma steganografi, diantaranya:

- Kapasitas
- Transparansi
- Ketahanan

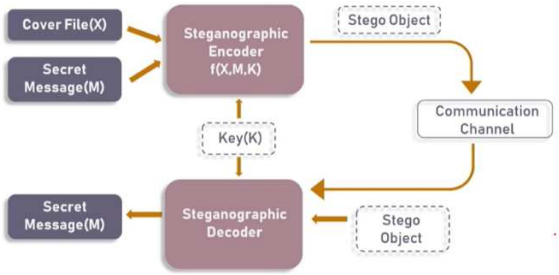


Gambar 2. Karakteristik steganografi

Ketiga karakteristik tersebut tidak dapat dimaksimalkan secara bersamaan. Masing-masing akan mempengaruhi satu sama lain, yaitu:

- Kapasitas sesuai dengan massa data yang dapat dimasukkan ke dalam wadah, dalam kaitannya dengan ukurannya.

- Transparansi yang mengukur kebisingan yang dihasilkan oleh proses penyembunyian dan tidak terlihatnya pesan kita.
- Terakhir, *robustness* menentukan kapasitas pesan kami untuk tetap utuh jika penampung diubah (Pemfilteran, kompresi)



Gambar 3. Karakteristik steganografi

Model Steganografi Dasar

Pada terhadap gambar di atas, file gambar asli (X) dan pesan rahasia (M) yang akan disembunyikan dimasukkan ke didalam encoder steganografi sebagai input. Fungsi *Steganographic Encoder*, f(X,M,K) menyematkan pesan rahasia ke didalam file gambar samaran dengan memanfaatkan tehnik pengkodean bit yang signifikansinya terkecil atau LSB (*Least Significant Byte*). Gambar stego yang dihasilkan muncul sangat mirip dengan dengan file awal gambar samaran Anda, tanpa perubahan yang terlihat. Untuk mendapatkan pesan rahasia, objek stego dimasukkan ke didalam *Steganographic Decoder*.

Steganografi Gambar

Menyembunyikan informasi di dalam gambar adalah teknik yang populer saat ini. Gambar dengan pesan rahasia di dalamnya dapat dengan mudah disebarkan ke melalui internet. Penggunaan steganografi di *newsgroup* telah diteliti oleh ahli steganografi Jerman Niels Provos, yang membuat kluster pemindaian yang mendeteksi keberadaan pesan tersembunyi di dalam gambar yang diposting di internet. Namun, setelah memeriksa satu juta gambar, tidak ada pesan tersembunyi yang ditemukan, sehingga penggunaan steganografi secara praktis masih terbatas.

Untuk menyembunyikan pesan di dalam gambar tanpa mengubah properti yang terlihat, sumber sampul dapat diubah di area "bising" dengan banyak variasi warna, jadi kurang perhatian pada modifikasi. Metode yang paling umum untuk membuat perubahan ini melibatkan penggunaan bit atau LSB yang paling tidak signifikan, masking, pemfilteran, dan transformasi pada gambar sampul. Teknik ini dapat digunakan dengan berbagai tingkat keberhasilan pada berbagai jenis file gambar.

Dalam steganografi digital, gambar banyak digunakan sebagai sumber samaran karena ada sejumlah besar bit yang ada dalam representasi digital suatu gambar. Dimana ada

kelompok bit yang bisa disisipkan pesan tanpa ada perubahan gambar secara kasat mata. Ada banyak cara untuk menyembunyikan informasi di dalam gambar. Pendekatan umum meliputi:

1. *Least Significant Bit Insertion*
2. *Masking and Filtering*
3. *Redundant Pattern Encoding*
4. *Encrypt and Scatter*
5. *Coding and Cosine Transformation*

Teknik Steganografi Least Significant Bit (LSB)

Gambar digital merupakan sebagai sekumpulan nilai digital terbatas, yang disebut piksel. Piksel adalah elemen individual terkecil dari sebuah gambar, yang memiliki nilai yang mewakili kecerahan warna tertentu pada titik tertentu. Sehingga kita dapat menganggap gambar sebagai matriks (atau larik dua dimensi) piksel yang berisi sejumlah baris dan kolom yang tetap.

Pendekatan sederhana untuk menanamkan informasi pada gambar samaran adalah menggunakan *Least Significant Bits* (LSB). LSB merupakan teknik steganografi paling sederhana dengan cara menanamkan bit pesan langsung ke bidang bit paling tidak signifikan dari gambar sampul dalam urutan deterministik. Memodulasi bit yang paling tidak signifikan tidak menghasilkan perbedaan yang dapat dilihat manusia karena amplitudo perubahannya kecil.

Untuk menyembunyikan pesan rahasia di dalam gambar, diperlukan gambar samaran yang tepat. Karena metode ini menggunakan bit dari setiap piksel pada gambar, maka perlu menggunakan format kompresi *lossless* seperti pada gambar BMP dan PNG, jika tidak, informasi tersembunyi akan hilang dalam transformasi algoritma kompresi *lossy*. Saat menggunakan gambar berwarna 24-bit, bit dari masing-masing komponen warna merah, hijau dan biru dapat digunakan, sehingga total 3bit dapat disimpan di setiap piksel. Misalnya, *grid* berikut dapat dianggap sebagai 3 piksel dari gambar berwarna 24-bit, menggunakan memori 9 byte:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Ketika dimasukkan huruf A, yang memiliki nilai biner 10000001, *grid* piksel akan berubah menjadi:

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

Perhatikan perubahan nilai biner pada setiap bagian akhir *byte* di atas.

Dalam contoh kasus ini, hanya tiga bit yang perlu diubah untuk memasukkan karakter huruf Adengan sukses. Rata-rata, hanya setengah dari bit dalam gambar yang perlu dimodifikasi untuk menyembunyikan pesan rahasia dengan menggunakan ukuran gambar samaran maksimal. Hasil perubahan yang dibuat untuk *Least Significant Bits* (LSB) terlalu kecil untuk dikenali oleh sistem visual manusia atau *Human Visual System* (HVS), sehingga pesan tersebut secara efektif disembunyikan.

Seperti yang kita lihat, *Least Significant Bits* (LSB) pada warna baris ketiga tidak mengalami perubahan apa pun. Ini dapat digunakan untuk memeriksa integritas 8 bit yang tertanam dalam 3 piksel ini. Dengan kata lain, ini bisa digunakan sebagai "bit paritas"

AES (*Advanced Encryption Standard*)

Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128-bit, 192-bit, dan 256-bit. Perbedaan dari ketiga urutan tersebut adalah panjang kunci yang mempengaruhi jumlah round (perputaran) yang dapat digambarkan dalam bentuk tabel:

Tabel 1 Tabel urutan data algoritma AES

	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-129	6	4	12
AES-256	8	4	14

Tabel 1 di atas menjelaskan tentang variasi algoritma AES dengan panjang kunci, panjang blok dan jumlah putaran yang berbeda-beda

Terdapat 4 transformasi putaran/*rounds* pada proses enkripsi dan dekripsi [14]:

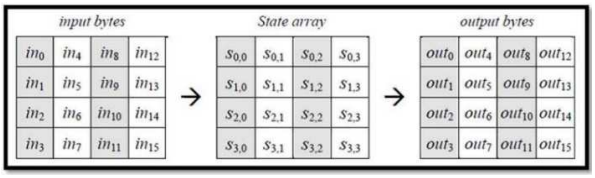
1. *SubBytes* Fungsinya menukar isi dari *byte* dengan memakai tabel substitusi.
2. *ShiftRows* Proses pergeseran blok per baris pada *state array*.
3. *MixColumn* Proses mengalikan blok data (pengacakan) di masing-masing *state array* dengan rumus sebagai berikut:
   $A(x) = \{03\}x^2 + \{01\}x^2 + \{01\}x + \{02\}$
4. *AddRoundKey* Mengombinasikan state array dan round key dengan hubungan XOR.

Pada proses dekripsi algoritma AES prosesnya sebagai berikut:

1. *InvShiftRows*, Melakukan pergeseran bit ke kanan pada setiap blok baris.
2. *InvSubBytes* Setiap elemen pada *state* dipetakan dengan tabel *Inverse S-Box*.
3. *InvMixColumn* Setiap kolom dalam state dikalikan dengan matriks AES.

4. *AddRoundKey* Mengombinasikan *state array* dan *round key* dengan hubungan XOR.

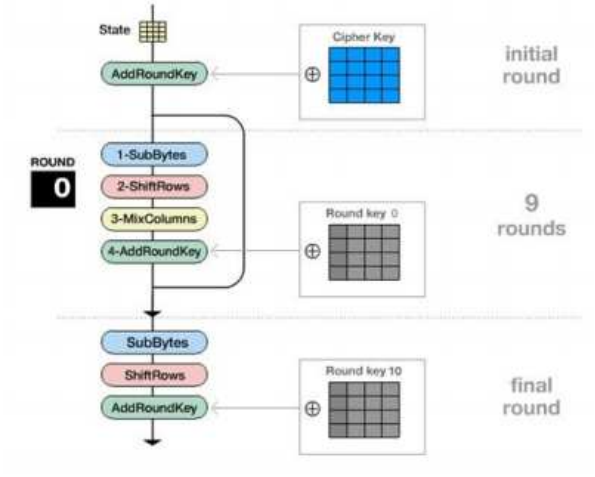
Penggambaran proses transformasi putaran dapat dilihat dari Gambar 4



Gambar 4. Proses *input bytes, state array, output bytes*.

Dari Gambar 1 di atas menunjukkan bahwa algoritma AES memiliki dasar, dimana algoritma AES ini merupakan *array of bytes*, memiliki dua dimensi yang disebut dengan state. Rumus ukuran state yaitu $NROWS\ x\ NCOLS$, melalui state ini akan dilakukan enkripsi dan dekripsi yang kemudian hasilnya dimasukkan ke dalam *array of state*. Proses enkripsi dimulai dengan memasukkan data ke dalam *input bytes* yang kemudian disalin ke dalam *array state*, melalui proses ini kemudian dilakukan enkripsi serta dekripsi, hasil keluaran yang didapat akan ditampung dalam output bytes.

Di awal proses enkripsi, input yang tersalin dalam state akan mengalami transformasi *AddRoundKey*. Kemudian *state* akan mengalami transformasi *SubBytes, ShiftRows, MixColumns*, dan *AddRoundKey* secara berulang sebanyak *round*/putaran (Nr). Proses dalam algoritma AES ini disebut sebagai *round function*. Pada *round* atau putaran yang terakhir, *state* tidak diberikan transformasi *MixColumns*. Ilustrasi pemrosesan awal pada enkripsi menggunakan algoritma AES -128 dapat dilihat pada Gambar 5:



Gambar 5. Contoh proses enkripsi dengan menggunakan algoritma AES-128.

III. METODE PENELITIAN

3.1 Metode Observasi

Melakukan pengumpulan data-data dengan cara mengamati serta mencatat secara sistematis tentang perangkat dan aplikasi yang digunakan dalam konfigurasi dalam praktek langsung.

3.2 Metode Studi Pustaka

Yaitu menggunakan literatur baik dalam bentuk media online, artikel atau buku bacaan yang berkaitan dengan penyusunan artikel ini.

3.3 Metode Pengembangan Jaringan

1. Analisa Kebutuhan

Analisa akan dilakukan melalui beberapa tahapan, yaitu

a. Observasi langsung
b. Memahami semua kondisi kebutuhan di lapangan terkait kebutuhan steganogtafi
c. Analisia hasil observasi.

2. Desain

Perancangan dilakukan melalui beberapa tahapan, yaitu:

a. Pemilihan aplikasi steganografi untuk pengujian.
b. Penentuan metode steganografi

3. Testing

Melakukan perbandingan gambar sebelum dan sesudah disisipkan data melalui steganografi, dan memastikan data yang disembunyikan dapat diekstraksi

4. Implementasi

Untuk menjalankan OpenVAS diperlukan langkah berikut.

a. Instalasi dan konfigurasi Windows 10

Instalasi Windows 10 dilakukan pada mesin virtual (VM) pada sistem lokal. Windows dipilih karena merupakan salah OS paling *user friendly*. *Server* diinstall dengan spesifikasi:

Processor : 4 core
RAM : 16 GB
Hard Disk : 100GB

b. Instalasi OpenStego

Setelah Windows diinstall, langkah selanjutnya adalah melakukan instalasi OpenStego yang didownload melalui internet.

IV. HASIL PENELITIAN

Pada bab ini akan dijelaskan mengenai hasil pengujian dan analisa perbandingan gambar sebelum dan sesudah disisipkan pesan rahasia

4.1. Pengujian Pada File resolusi 1000 x 1252 pixel

Pada pengujian pertama digunakan gambar berukuran 1000 x 1252 pixel (1.252.000 pixel), berukuran 3,669 MB sebagai gambar samaran untuk menyisipkan 7 file berukuran berbeda secara terpisah. Selain itu pesan akan disandikan menggunakan algoritma AES-256. Kemudian file awal dan file hasil akan dibandingkan kualitasnya menggunakan metode PSNR (*Peak Signal-to-Noise Ratio*).

Gambar 6. Gambar sumber berukuran 1000 x 1252 pixel

Tabel 2 Tabel PSNR file BMP1000x1252 pixel

Message Size	PSNR Value
50	88.72
500	88.34
1000	88.32
2000	87.92
10000	87.15
50000	85.56
100000	83.99

Dari hasil pengujian di atas ditemukan bahwa nilai awal PSNR pada file pesan berukuran 50 karakter 88.72 kemudian menurun seiring bertambahnya ukuran pesan.

4.2. Pengujian Pada File resolusi 100 x 125 pixel

Pada pengujian pertama digunakan gambar berukuran lebih kecil dari sebelumnya yaitu 100 x 125 pixel (12500 pixel), berukuran 37KB sebagai gambar samaran untuk menyisipkan 7 file berukuran berbeda secara terpisah. Selain itu pesan akan disandikan menggunakan algoritma AES-256. Kemudian file awal dan file hasil akan dibandingkan kualitasnya menggunakan metode PSNR (*Peak Signal-to-Noise Ratio*).

Gambar 7. Gambar sumber berukuran 100 x 125 pixel

Tabel 3 Tabel PSNR file BMP 100x125 pixel

Message Size (char)	PSNR Value
50	68.46
500	68.29
1000	68.09
2000	67.84
10000	n/a
50000	n/a
100000	n/a

Dari hasil pengujian di atas ditemukan bahwa nilai awal PSNR pada file pesan berukuran 50 karakter 68.46 kemudian menurun seiring bertambahnya ukuran pesan. Namun karena keterbatasan ukuran file, pesan berukuran 10.000 karakter ke atas tidak dapat disisipkan dalam file gambar samaran.

V. KESIMPULAN

Dari pengujian kualitas gambar berdasarkan ukuran pesan yang disisipkan diperoleh kesimpulan sebagai berikut:

1. Semakin besar ukuran gambar semakin baik nilai PSNR untuk ukuran pesan yang sama.
2. File gambar samara berukuran kecil memiliki keterbatasan dalam menampung file pesan yang disisipkan
3. File awal dan akhir secara kasat mata tidak dapat dibedakan. Atau secara Human Visual System terlihat mirip

DAFTAR PUSTAKA

Bhowmik S. 2016, “A New Approach in Color Image Steganography with High Level of Perceptibility and Security”, 283–286.

Nilizadeh A., Nilchi ARN, 2016 “A novel steganography method based on matrix pattern and LSB algorithms in RGB images. 1st Conference on Swarm Intelligence and Evolutionary Computation”, CSIEC 2016 - Proceedings, 154–159. https://doi.org/10.1109/CSIEC.2016.7482107

Kadam K., Koshti A., Dunghav P. 2012 “Steganography Using Least Significant Bit Algorithm. International Journal of Engineering Research and Applications, 2(3), 338–341.

Gupta S., Goyal A., Bhushan B. 2012, “Information Hiding Using Least Significant Bit Steganography and Cryptography”. International Journal of Modern Education and Computer Science, 4(6), 27–34. https://doi.org/10.5815/ijmecs.2012.06.04

May, Rupali. May 2020 " Image Steganography using Python" TowardsDataScience.com. https://towardsdatascience.com/hiding-data-in-an-image-image-steganography-using-python-e491b68b1372 (diakses pada 21 Mei 2020 15:24 WIB)

Dittmann Jana, David Megías, Andreas Lang, Jordi Herrera-Joancomartí. 2006 “Theoretical Framework for a Practical Evaluation and Comparison of Audio Watermarking Schemes in the Triangle of Robustness, Transparency and Capacity”, Lecture Notes in Computer Science, Volume 4300, pp.1-40.

Khaldi, Amine. May 2018 “Diffie-Hellman Key Exchange through Steganographied Images” The Law, State and Telecommunications Review, Brasilia, v.10, n. 1, p. 147-160

Choudary, Archana. Nov 2020 "Steganography Tutorial – A Complete Guide For Beginners" Edureka! https://www.edureka.co/blog/steganography-tutorial (diakses pada 27 November 2020 18:33 WIB)

Nosrati M., Karimi R., Hariri M. August 2011 "An introduction to steganography methods" World Applied Programming, Vol (1), No (3), August 2011. 191-195

Mohamed Amin, Muhalim and Ibrahim, Subariah and Salleh, Mazleena and Katmin, Mohd Rozi. 2003" Information hiding using steganography." Project Report. http://eprints.utm.my/id/eprint/4339/1/71847.pdf (diakses pada 2 Des 2020 20:59 WIB)

Krenn, Robert. March. 2004 "Steganography and steganalysis" Internet Publication March 2004. http://www.krenn.nl/univ/cry/steg/article.pdf (diakses pada 3 Des 2020 11:59 WIB)

Putra, Soni Harza, dkk. 2013 "Implementasi Algoritma Kriptografi ADVANCED ENCRYPTION STANDARD (AES) Pada Kompresi Data Teks". Jurnal Teknologi Informasi, Universitas Brawijaya Malang. 2013.

Munir, Rinaldi. Kriptografi. 2006 Bandung: Penerbit Informatika.

R.Kristoforus JB, dkk. 2012 "Implementasi Algoritma Rijndael Untuk Enkripsi dan Dekripsi Pada Citra Digital".Seminar Nasional Aplikasi Teknologi Informasi 2012 (SNATI 2012). ISSN: 1907-5022. 2012

Voni Yuniati, dkk. April 2009 "Enkripsi dan Dekripsi Dengan Algoritma AES-256 Untuk Semua Jenis File". Jurnal Informatika Volume 5 No. 1 April 2009

Osama F. AbdelWahab, et al. June 2019 "Hiding data in images using steganography techniques with compression algorithms" TELKOMNIKA, Vol.17, No.3, June 2019, pp.1168~1175

Kunjir, Satyavan M., et al. Oct 2016 "Review On Stenography Tools" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 - 0056 Volume: 03 Issue: 10 | Oct -2016.