Research Article
Forbis: Journal Forensic Business Information Systems
Published online on: https://journal.universitasmulia.ac.id/index.php/forbis **1 (1) Januari 2024**

IMPLEMENTASI STEGANOGRAFI DAN STEGANALISIS MENGGUNAKAN METODE LSB (LEAST SIGNIFICANT BIT) PADA FILE GAMBAR

Jihan Rizky Maulidina[1*], Nasruddin Bin Idris[2], Djumhadi[3]

[1,2,3] Teknologi Informasi, Fakultas Ilmu Komputer, Universitas Mulia

email: [1]*jihanrizky@students.universitasmulia.ac.id*, [2]nasruddin@universitasmulia.ac.id, [3]djumhadi@universitasmulia.ac.id
[*]*Correspondence*

ARTICLE INFO

Article History
Received : 27 November 2023
Revised : 21 Januari 2024
Accepted : 22 Januari 2024
Available online : 22 Januari 2024

Keywords:
Bit, Chi-Square), Steganografi, LSB, Steganalisis

Please cite this article in IEEE style as:

ABSTRACK

With the progress of technology and the growing concerns about information security, individuals have increasingly turned to steganography as a means of covert communication and safeguarding data. This study delves into the attributes of steganographic files through an experimental approach. SilentEye application is utilized to embed concealed messages within JPEG images, and subsequent analysis employs steganalysis techniques. The investigation primarily centers on bit analysis (specifically, bit 0 and bit 1) of the steganographic file using the Least Significant Bit (LSB) method. The research aims to assess the efficacy of this method in uncovering hidden content. Furthermore, Chi-Square (X2) testing is applied to gain deeper insights and formulate statistical hypotheses (both null and alternative) regarding the nature of the file (whether it is steganographic or not.

ABSTRAK

Dengan kemajuan teknologi dan meningkatnya kekhawatiran terhadap keamanan informasi, individu semakin beralih ke steganografi sebagai cara untuk berkomunikasi secara rahasia dan melindungi data. Penelitian ini menginvestigasi karakteristik dari file steganografi melalui pendekatan eksperimental. Aplikasi SilentEye digunakan untuk menyisipkan pesan tersembunyi dalam gambar JPEG, dan analisis selanjutnya menggunakan teknik steganalisis. Penelitian ini berfokus pada analisis bit (khususnya, bit 0 dan bit 1) dari file steganografi dengan menggunakan metode Least Significant Bit (LSB). Tujuan penelitian adalah mengevaluasi efektivitas pendekatan ini dalam mendeteksi konten tersembunyi. Selain itu, pengujian Chi-Square (X2) digunakan untuk memberikan wawasan lebih dalam dan menghasilkan hipotesis statistik (null dan alternatif) tentang sifat file (apakah steganografi atau tidak).

1. Pendahuluan

Dari kemajuan dan perkembangan zaman terutama di bidang teknologi informasi, pertukaran informasi secara elektronik sudah sangat umum dilakukan oleh masyarakat di dunia. Dalam kehidupan sehari-hari masyarakat menggunakan teknologi informasi untuk mengirim dan menyimpan data-data privasi atau rahasia. Dengan zaman yang terus berkembang dan teknologi yang terus maju, sebagian masyarakat dapat memanfaatkan perkembangan teknologi tersebut untuk mengirim dan menyimpan data-data rahasia dengan cara menyembunyikannya di media digital lain sebelum dikirim kepada orang lain atau menyimpannya untuk diri sendiri[1].

Media digital yang dapat digunakan adalah file gambar. Sesuai hidup di zaman berteknologi maju, file gambar dapat disisipkan pesan-pesan rahasia yang dalam tindakan penyisipan pesan-pesan ini mengarah dan merujuk kepada steganografi. Dengan melakukan pengiriman atau penyimpanan pesan-pesan rahasia yang telah menggunakan steganografi tidak menimbulkan kecurigaan selain pihak pembuat dan penerima pesan[2], [3].

Oleh karena itu, penelitian ini melakukan implementasi menyembunyikan pesan-pesan tersebut ke dalam file gambar dilanjutkan dengan melakukan steganalisis terhadap file gambar yang telah diubah menggunakan metode LSB melibatkan pengujian Chi-Square (X2) dengan tujuan mengidentifikasi file gambar tersebut mengandung pesan tersembunyi. Penelitian ini juga diharapkan dapat memberikan pemahaman yang lebih baik tentang keandalan dan kerahasiaan data/pesan yang disisipkan ke dalam file gambar [4]–[7]. Hasil penelitian dapat berguna dalam pengembangan teknik steganografi yang lebih canggih dan dapat berguna dalam upaya pengembangan metode steganalisis yang lebih efektif untuk mendeteksi data/pesan tersembunyi di dalam file gambar. Dan hasil penelitian ini juga dapat berkontribusi dalam pengembangan dan peningkatan keamanan dan privasi dalam komunikasi digital.

Di penelitian ini mengusung perpaduan antara dua aspek penting dalam keamanan informasi, yaitu steganografi untuk penyisipan pesan rahasia ke dalam file gambar dan steganalisis untuk mengidentifikasi adanya pesan tersembunyi hasil dari steganografi tersebut. Dalam konteks penelitian, identifikasi masalah dapat dilihat dari dua perspektif.

Pertama dari perspektif steganografi, identifikasi masalah meliputi pemahaman tentang bagaimana proses penyisipan pesan tersembunyi dilakukan pada file gambar menggunakan aplikasi SilentEye. Fokus dari identifikasi ini adalah melakukan uji coba terhadap kualitas visual gambar melalui lima buah opsi kualitas gambar pada aplikasi, yakni very low, low, normal, best, dan high. Dengan melakukan steganografi pada kelima opsi kualitas gambar, dapat mempertimbangkan aspek kerahasiaan dan ketahanan terhadap upaya pendeteksian.

Kedua dari perspektif steganalisis, identifikasi masalah akan menitikberatkan pada penerapan pengujian Chi-Square (X2) untuk menguji distribusi bit hasil penyispan pesan rahasia menggunakan metode LSB pada file gambar. Masalah yang diidentifikasi melibatkan kemampuan teknik steganalisis ini untuk mendeteksi adanya penyisipan pesan dengan mengamati perbedaan statistik antara distribusi bit yang diharapkan (distribusi bit pada file yang belum disisipkan pesan) dan distribusi bit yang diamati (distribusi bit yang telah disisipkan pesan)[8], [9].

Dengan demikian, identifikasi masalah mencakup teknik atau implementasi steganografi pada file gambar menggunakan aplikasi SilentEye dan penggunaan steganalisis dengan melibatkan pengujian Chi-Square (X2) untuk mendeteksi dan mengidentifikasi bahwa file hasil implementasi steganografi terdeteksi sebagai file steganografi atau tidak.

2. Metode Penelitian

Dalam penelitian ini, dilakukan penelitian eksperimental dengan pendekatan penggabungan penelitian antara analisis

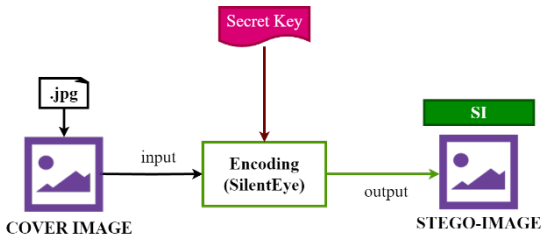
statistik dan pemodelan prediktif untuk mendeteksi adanya penyisipan pesan rahasia dalam file gambar. Peneliti menggunakan algoritma dan teknik steganografi untuk melakukan implementasi steganografi dan steganalisis terhadap file gambar.

2.1. Metode Pengumpulan Data

Metode pengumpulan data di penelitian ini terdiri dari tiga metode. Pertama, metode pengumpulan literature review yang melibatkan analisis dan sintetis terhadap sumber-sumber lieratur yang sudah ada, seperti jurnal, buku, artikel, makalah, dan sumber lainnya. Kedua, metode pengumpulan data wawancara yang melibatkan tanya jawab terhadap orang-orang di rumah. Pertanyaan yang diajukan hanya berkaitan dengan lokasi foto yang bagus untuk dijadikan bahan penelitian. Ketiga, metode pengumpulan data observasi yang dalam penelitian ini melakukan observasi di lingkungan rumah untuk mengumpulkan data/file gambar menggunakan smartphone VIVO.

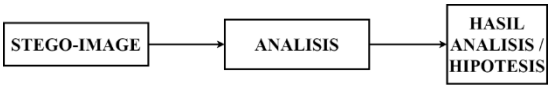
2.2. Alur Penelitian

Rancangan penelitian meliputi implementasi steganografi menggunakan aplikasi SilentEye dan steganalisis pada sebuah bit gambar menerapkan pengujian Chi-Square (X2). Masing-masing dapat dilihat pada Gambar 1 dan Gambar 2.



Gambar 1. Alur Steganografi

Sesuai pada gambar diatas, file pesan .jpg dan file cover image diinput ke dalam aplikasi dan menambahkan secret key serta melakukan encoding untuk menyisipkan pesan ke dalam file cover image, sehingga menghasilkan file stego-image.



Dalam steganalisis dilakukan analisis menggunakan metode LSB (bit yang paling tidak signifikan antara file gambar asli dengan file gambar hasil sisipan pesan) dengan cara melibatkan pengujian Chi-Square (X2). Jika terdapat perbedaan pola, distribusi, atau statistik ditemukan, hal ini bisa menjadi indikasi bahwa file tersebut terdeteksi sebagai file steganografi. Rumus pengujian Chi-Square (X2) sebagai berikut:

$$\chi 2 = \Sigma((O - E)^2 / E)$$

Keterangan:

- X^2 merupkan simbol nilai chi-square.
- $\sum$ merupakan simbol sigma yang menunjukkan penjumlahan keseluruhan elemen.
- O merupakan simbol observasi (jumlah bit pada gambar hasil sisipan pesan).
- E merupakan simbol ekspektasi / harapan (jumlah bit pada gambar yang belum disisipkan pesan).

3. Hasil dan Pembahasan

Dalam konteks steganografi, secret key digunakan untuk meningkatkan level keamanan pesan tersembunyi dan di beberapa kasus, secret key dapat menyulitkan upaya deteksi steganografi oleh pihak yang tidak berwenang.

3.1 Encoding

Proses *encode* yakni penyisipan pesan rahasia ke dalam file gambar akan berlangsung dan tunggu proses penyisipan selesai. Berikut ini adalah beberapa hasil implementasi steganografi yang telah dilakukan melalui aplikasi.

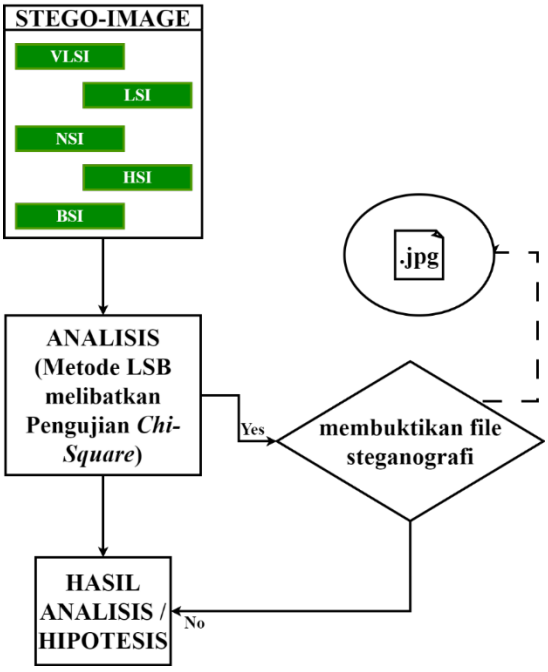
"VLSI.bmp"

"LSI.bmp"

Gambar 2. File dengan Steganofrafi

3.2 Steganalisis

Untuk melakukan steganalisis pada file gambar, hasil sisipan pesan kemudian dianalisis dengan tahapan pada gambar 3.



Gambar 3. Alur Steganalisis

Adapun proses sesuai tahapan di gambar 3 sebagai berikut:

- **Menyiapkan File Gambar**

  Menyiapkan file gambar yang belum disisipkan pesan (*cover image*) dan file hasil sisipan pesan (*stego-image*).
- **Mengubah Gambar Berwarna ke Gambar Binary**

  Karena fokus penelitian adalah menghitung jumlah nilai bit 0 dan bit 1, maka gambar berwarna dirubah terlebih dahulu ke gambar *binary* yang hanya terdiri dari dua warna saja yaitu hitam dan putih. Hal ini dapat dilakukan di aplikasi *ImageJ*.
- **Menyiapkan Histogram**

  Dari hasil perubahan warna di setiap gambar telah memiliki sebuah histogram. Histogram ini digunakan untuk mengetahui distribusi nilai bit yang ada pada sebuah gambar.
- **Membuat Tabel dan Menghitung Nilai Frekuensi Bit**

  Dari histogram, untuk menghitung nilai frekuensi bit dapat memperhatikan kolom "*Value*" dan kolom "*Count*" pada baris "0" dan "255". Hal ini masing-masing mewakili bit 0 dan bit 1. Apabila telah mendapatkan nilai frekuensi bit, maka dibuat tabel frekuensi bit yang terdiri dari dua baris dan tiga kolom.
- **Menghitung Nilai Chi-Square**

  Untuk menghitung nilai *Chi-Square* (X^2) perlu mengetahui terlebih dahulu nilai frekuensi observasi (*f_obs*) dan nilai frekuensi harapan (*f_exp*). Setelah itu, hitung nilai *Chi-Square* (X^2) untuk masing-masing bit 0 dan bit 1. Hasil masing-masing bit ditotalkan.
- **Menentukan Derajat Kebebasan (df)**

  Untuk menentukan derajat kebebasan, perhatikan saja jumlah baris dan kolom pada tabel frekuensi bit. Jadi, untuk derajat kebebasannya adalah "df = (jumlah_baris - 1) x (jumlah_kolom - 1) = 1 x 2 = 2".

- **Menentukan Tabel Konsultasi atau Tabel Distribusi Chi-Square**
  Di bagian ini hanya mengurai semua hasil steganalisis yang berisi nilai *Chi-Square (X^2)* lebih kecil atau lebih besar dari nilai derajat kebebasan

3.3 Penentuan File Steganografi

Hasil steganalis dihitung berdasarkan rumus yang telah disampaikan sebelumnya yang kemudian didapatkan sebuah hasil di tabel 1.

Tabel 1. Hasil Steganalisis

No	Nama	X^2	Penentuan	df
1	VLSI.bmp	2,48	>	2
2	LSI.bmp	10,21	>	2
3	NSI.bmp	2,52	>	2
4	HSI.bmp	0,016	<	2
5	BSI.bmp	0,0028	<	2

Proses berikutnya menentukan hipotesis dari nilai yang didapat, hasil hipotesis ditunjukkan pada tabel 2.

Tabel 2. Hasil Hipotesis

No	Nama File	Hipotesis		Keterangan
		Hasil	Lambang	
1	VLSI.bmp	Hipotesis Alternatif	H_1	File steganografi
2	LSI.bmp	Hipotesis Alternatif	H_1	File steganografi
3	NSI.bmp	Hipotesis Alternatif	H_1	File steganografi
4	HSI.bmp	Hipotesis Nol	H_0	Tidak terdeteksi sebagai file steganografi, jadi dibutuhkan bantuan metode steganalisis lain untuk membuktikan file steganografi
5	BSI.bmp	Hipotesis Nol	H_0	Tidak terdeteksi sebagai file steganografi, jadi dibutuhkan bantuan metode steganalisis lain untuk membuktikan file steganografi

Dari hasil hipotesis terdapat tiga file yang berhasil dideteksi sebagai file steganografi (X2 > df) yaitu file dengan kualitas very low, low, dan normal dan terdapat dua file yang tidak dapat dideteksi sebagai file steganografi dari pengujian Chi-Square (X2) (X2 < df) yaitu file dengan kualitas high dan best.

Hasil steganalisis seperti Hipotesis Alternatif (H1) dapat memberikan gambaran awal bahwa file yang dilakukan eksperimental dapat secara langsung diidentifikasi sebagai file steganografi, karena adanya perubahan yang lebih besar dari distribusi nilai bit dan adanya nilai Chi-Square (X2) yang lebih besar dari nilai harapan gambar tidak berubah. Sedangkan Hipotesis Nol (H0) dapat memberikan informasi bahwa file tersebut sulit dideteksi sebagai file steganografi dan memerlukan metode steganalisis lain yang lebih canggih.

Hasil pengujian Chi-Square (X2) juga dapat menunjukkan bahwa ketidaksesuaian statistik yang signifikan antara distribusi bit yang teramati (stego-image) dan yang diharapkan (cover image) dapat menjadi tanda adanya modifikasi pada file gambar yang disebabkan oleh penyisipan pesan. Oleh karena itu, teknik steganalisis ini mampu mendeteksi adanya pesan tersembunyi dengan tingkat keberhasilan yang diandalkan namun terbatas.

Dikarenakan perhitungan Chi-Square (X2) harus melibatkan kedua file antara cover image

dan stego-image, maka file cover image tidak dilakukan pengujian Chi-Square (X2).

Namun, untuk membantu membedakan antara file cover image dan file stego-image dapat dilakukan perbedaan terhadap histogram yang dihasilkan pada file gambar berwarna atau pada file yang belum dirubah ke dalam gambar binary.

Pada histogram yang dihasilkan akan memberikan perubahan yang jelas dari hasil penyisipan.

4. Kesimpulan

Penelitian mengenai cara menyembunyikan atau menyisipkan pesan-pesan rahasia ke dalam file gambar dapat menggunakan bantuan aplikasi yaitu SilentEye. Dalam penelitian, SilentEye mampu mengamankan pesan-pesan rahasia dengan baik dalam file gambar tanpa mengganggu tampilan visual gambar yang tampak alami yang bergantung pada kelima opsi yang tersedia dan target steganografi yang akan dihasilkan. Selain itu, penggunaan algoritma enkripsi atau secret key yang disediakan oleh aplikasi telah memberikan tingkat perlindungan yang cukup baik dan cukup tinggi terhadap dekripsi yang tidak sah.

Untuk melakukan steganalisis terhadap file stego-image, hal yang pertama kali dilakukan adalah dengan mengubah gambar berwarna menjadi sebuah gambar biner (binary) yang dimana gambar biner terdiri dari dua bit saja yaitu bit 0 dan bit 1. Kedua bit ini akan dihitung berdasarkan rumus pengujian Chi-Square (X2). Apabila nilai yang dihasilkan lebih besar dari nilai derajat kebebasan, maka file yang sedang dianalisis dapat terdeteksi secara langsung sebagai file steganografi. Sebaliknya apabila nilai yang dihasikan lebih kecil daripada nilai derajat kebebasan, maka file yang sedang dianalisis masih belum bisa dideteksi oleh pengujian Chi-Square (X2) dan untuk mendeteksi file dengan hasil seperti itu dibutuhkan metode steganalisis yang lebih canggih atau yang lebih sensitif terhadap deteksi file gambar.

5. Referensi

[1] P. Studi Ilmu Komunikasi, "Tren Penggunaan Media Sosial Selama Pandemi Di Indonesia," 2020.

[2] "346079-Implementasi-Steganografi-Pada-Berkas-Au-77e35ad0".

[3] S. Rohayah, G. W. Sasmito, And O. Somantri, "Aplikasi Steganografi Untuk Penyisipan Pesan," *Jurnal Informatika*, Vol. 9, No. 1, Jan. 2015, Doi: 10.26555/Jifo.V9i1.A2038.

[4] D. Darwis, "Implementasi Teknik Steganografi Least Significant Bit (Lsb) Dan Kompresi Untuk Pengamanan Data Pengiriman Surat Elektronik," *Jurnal Teknoinfo*, Vol. 10, No. 2, Pp. 1–7, 2016.

[5] G. Wisnu Bhaudhayana And I. Made Widiartha, "Implementasi Algoritma Kriptografi Aes 256 Dan Metode Steganografi Lsb Pada Gambar Bitmap," Vol. 8, No. 2, 2015.

[6] N. B. Pamungkas, D. Darwis, D. Nurjayanti, And A. T. Prastowo, "Perbandingan Algoritma Pixel Value Differencing Dan Modulus Function Pada Steganografi Untuk Mengukur Kualitas Citra Dan Kapasitas Penyimpanan."

[7] A. Rohmanu, "Implementasi Kriptografi Dan Steganografi Dengan Metode Algoritma Des Dan Metode End Of File," *Jurnal Informatika Simantik*, Vol. 2, No. 1, 2017, [Online]. Available: Www.Jurnal.Stmikcikarang.Ac.Id

[8] "Secret Communication On Facebook Using Image Steganography: Experimental Study." [Online]. Available: Https://Sites.Google.Com/Site/Ijcsis/

[9] A. Neyaz And C. Varol, "Audio Steganography Via Cloud Services: Integrity Analysis Of Hidden File."