Jurnal Elektronik Ilmu Komputer Udayana
Volume 12, No 2. November 2023

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Penerapan Steganografi dan Visible Watermarking Pada Gambar Digital Untuk Perlindungan Hak Cipta

Chelsy Elisabet Gultom[a1], I Ketut Gede Suhartana[a2]

[a]Progam Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Bali, Indonesia
[1]chelsyelisabet@email.com
[2]ikg.suhartana@unud.ac.id (Corresponding author)

Abstract

As technology develops, almost all information and data is stored in digital form. But as we know, digital storage is more vulnerable to theft where this thing is often happen to data that people shared on the internet, include digital image. From the problem above, we do the research where we build a windows-based program using steganography with least significant bit method and visible watermarking that implement encryption hidden message and visible watermarking to the digital image we want to. This program also can decode the hidden message from the digital image that contain the message. The research prove that using the combination of steganography and visible watermarking can help the owner of the digital image to claim the copyright of their digital image. This happened because they can encrypt the proof of the ownership in the image by visible dan invisible way.

Keywords: *Image Processing, Steganography, Least Significant Bit (LSB), Data Hiding, Watermark*

1. Pendahuluan

Seiring berkembangnya teknologi, hampir semua informasi maupun data disimpan dalam bentuk digital. Namun seperti diketahui, penyimpanan digital lebih rentan terhadap pencurian. Hal ini disebabkan karena keamanan pada media digital lebih lemah. Alasan lainnya adalah hampir semua perangkat yang digunakan dalam membuat atau menyimpan media digital terkoneksi dengan jaringan internet dan hal ini membuat perangkat rawat terinfeksi virus atau bug atau bahkan hacker yang dapat mencuri data kita. Selain itu, data yang disebarluasakan maupun dijual secara digital juga rawan pembajakkan yang dimana data yang kita sebar atau jual dapat dicuri dan diubah hak kepemilikannya, hal ini membuat kita sebagai pemilis asli data menjadi rugi.

Pembajakkan dan pencurian hak cipta ini sangat sering terjadi kepada gambar digital. Hal inilah yang mendorong orang – orang untuk mengembangkan berbagai metode yang nantinya dapat digunakan untuk meningkatkan keamanan data. Terdapat beberapa metode yang digunakan untuk menunjukkan hak cipta, seperti steganografi dan watermarking

Steganografi adalah ilmu yang mempelajari tentang cara untuk menyembunyikan pesan atau informasi [1]. Steganografi biasanya digunakan untuk menyembunyikan pesan pada sampul media, dimana orang tidak akan curiga, karena letak keberadaan pesan tersebut biasanya sulit diketahui [2]. Watermark adalah tanda yang diletakkan pada suatu karya untuk menandakan kepemilikan atau hak cipta dari karya tersebut. Watermark dapat berupa tulisan, bit, gambar, logo, dan lain lain.

Berdasarkan hal tersebut, kami ingin melakukan peneitian dimana kami membuat aplikasi steganowater yang dimana pada pada aplikasi tersebut kami menggabungkan steganografi menggunakan metode Least Significant Bit (LSB) dengan visible watermark. Penelitian ini bertujuan untuk meningkatkan perlindungan hak cipta digital baik secara langsung (terlihat oleh mata) dan tidak langsung (tidak kasat mata).

2. Metode Penelitian

Penelitian yang akan kami lakukan memiliki beberapa tahapan penelitian. Untuk proses enkripsi steganografi dan watermark, pertama kami menginput file gambar yang akan menjadi tempat/media

text dan watermark disisipkan. Kedua menginput watermark yang akan digunakan pada gambar. Selanjutnya menggabungkan watermark dengan gambar sehingga dihasilkan gambar yang telah memiliki watermark. Tahap terakhir, gambar yang telah digabung dengan watermark akan disisipi oleh teks steganografi menggunakan metode Least Significant Bit (LSB). Untuk proses dekripsi

yaitu teks yang akan disisipkan ke dalam sampul gambar digital RGB

2.1. Data

Pada penelitian ini, kami menggunakan data berbentuk gambar RGB berbagai jenis yang diambil secara acak dari internet maupun gambar ada pada perangkat. Gambar yang akan digunakan sebagai data, adalah gambar yang memiliki format file *PNG yang meliputi: gambar polos, gambar hitam putih, gambar warna – warni, dan gambar pemandangan yang akan digunakan sebagai media yang akan disisipkan steganografi dan watermark. Selai gambar, penelitian ini juga membutuhkan data berupa text yang akan digunakan menjadi watermark maupun menjadi teks steganografi.

2.2. Least Significant Bit (LSB)

Least Significant Bit (LSB) merupakan metode steganografi yang paling sederhana. Tidak seperti most significant bit yang merupakan bagian dari barisan data biner terbesar yaitu barisan bagian kiri, Least Signifiant Bit merupakan bagian dari barisan data biner terkecil yaitu barisan bagian kanan [3].

Penerapan steganografi menggunakan metode LSB bekerja dengan menginput pesan rahasia ke dalam bit paling kanan atau paling tidak signifikan [4]. Karena pesan diinput pada bit paling tidak signifikan, gambar yang disisipi tidak mengalami banyak perubahan dan tidak dapat dideteksi oleh penglihatan biasa [5]. Adapun kekurangan dari metode LSB adalah mudahnya pesan rahasia untuk rusak apabisa terjadi sesuatu pada gambar (gambar diedit).

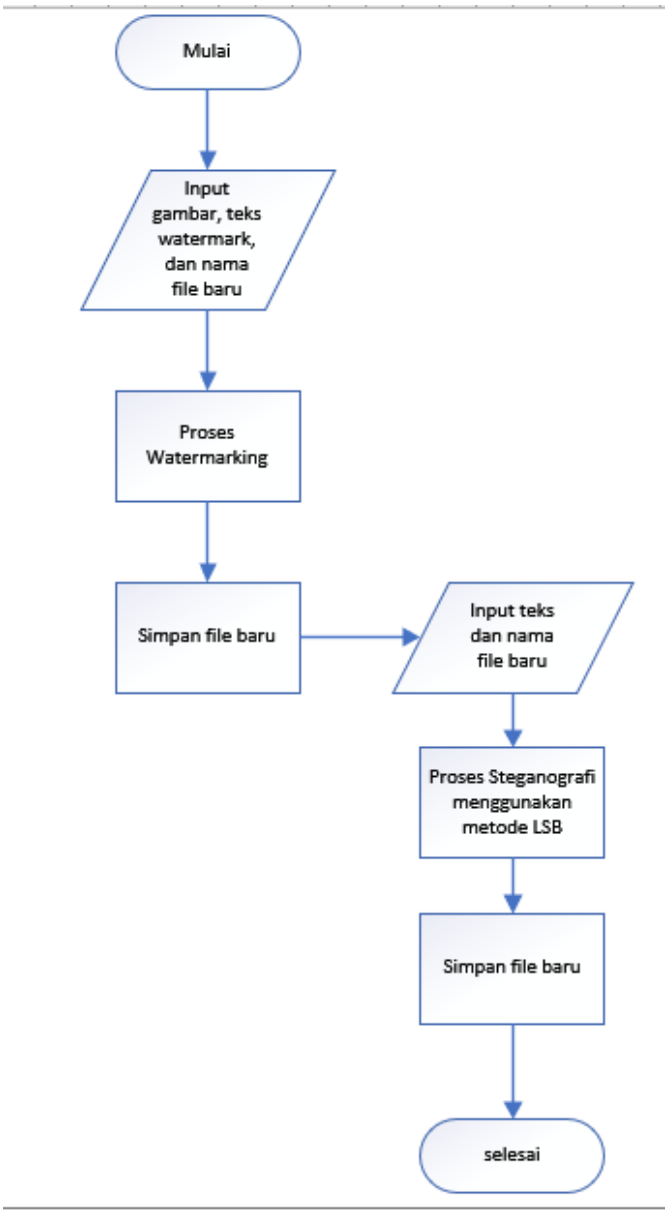
2.3. Watermark

Watermark adalah informasi atau pesan yang menyatakan hak cipta dari pada suatu data multimedia. Watermark berfungsi untuk melindungi sekaligus menyatakan kepemilikan hak cipta sehingga dapat menghindari akses tidak sah atau pencurian hak cipta [6]. Visible watermark biasanya digunakan pada media yang akan disebarluaskan sebagai proteksi hak cipta.

2.4. Desain Sistem

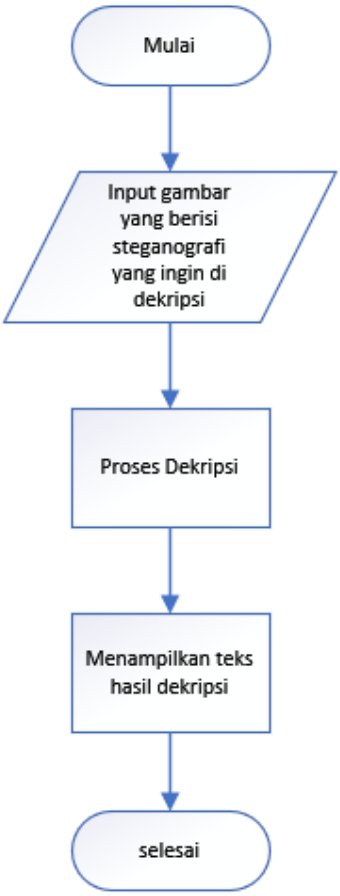
Program steganomark (steganografi dan watermark) memiliki dua proses utama, yaitu enkripsi dan dekripsi. Pada proses enkripsi, pengguna diminta untuk memasukkan gambar dalam bentuk *png. Selanjutnya pengguna diminta untuk menginput teks yang akan dijadikan visible watermark dan nama file baru (bentuk file harus sama bentuk file gambar) yang akan berisi gambar berwatermak yang telah dibuat. File gambar berwatermark tersebut kemudian akan secara otomasi dibaca oleh sistem dan kemudian user akan diminta menginpukan teks yang akan menjadi pesan tersembunyi dan nama file baru (bentuk file harus sama bentuk file gambar) yang akan berisi gambar yang telah memiliki visible watermark dan pesan tersembunyi. Adapun flowchart proses enkripsi dapat dilihat pada gambar 2.4.1.

p-ISSN: 2301-5373
e-ISSN: 2654-5101



Gambar 2.4.1 proses enkripsi

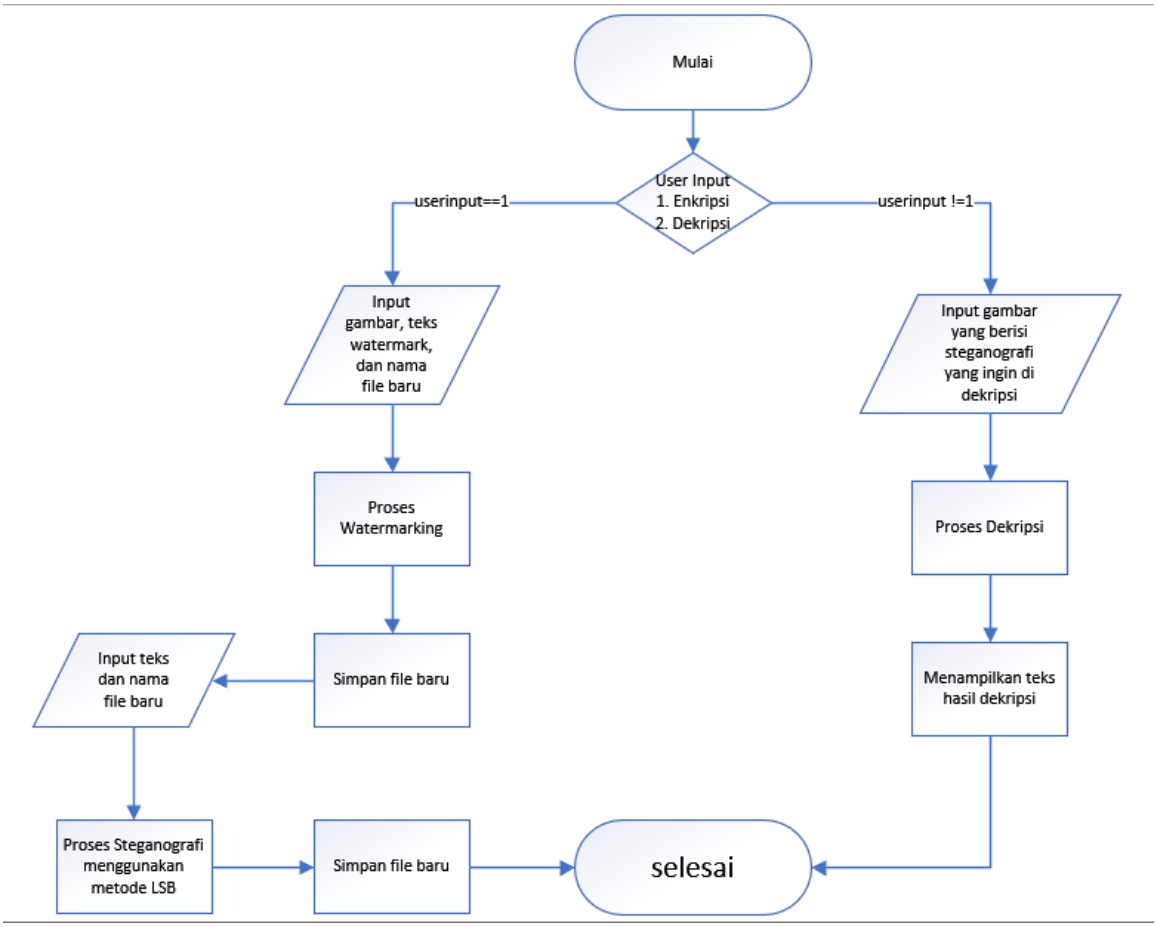
Pada proses dekripsi, pengguna diminta untuk memasukkan gambar yang berisi pesan tersembunyi dalam bentuk *png. Sistem kemudian cera otomatis akan mendekripsi gambar dan menampilkan teks tersembunyi. Flowchart proses dekripsi dapat dilihat pada gambar 2.4.2.



Gambar 2.4.2 proses dekripsi

Flowchart program yang berisi proses ekstraksi dan destraksi, dapat dilihat pada gambar 2.4.3.

p-ISSN: 2301-5373
e-ISSN: 2654-5101

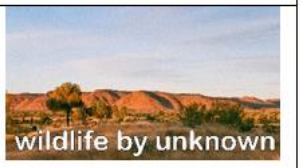


Gambar 2.4.3 flowchat program

3. Hasil dan Pembahasan

Pengujian ini dilakukan untuk melihat apakah ada perbedaan terlihat maupun tidak terlihat antara gambar asli dengan hasil gambar yang sudah disisipi watermark dan steganomark. Pengujian ini juga

dilakukan untuk melihat apakah program berhasil melakukan enkripsi dan deksripsi. Berikut merupakan tabel berisi gambar sebelum dan sesudah di lakukan watermarking dan steganografi

No	Jenis Gambar	Gambar Asli	Gambar Watermark	Gambar SteganoMark
1	Polos			
2	Hitam Putih			
3	Warna-warni			
4	Pemandangan			

Tabel 3.1 tampilan gambar sebelum dan sesudah dilakukan enkripsi

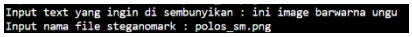
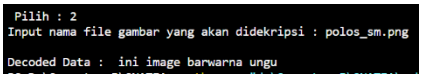
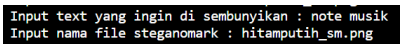
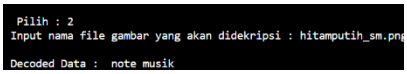
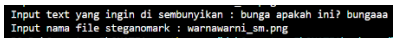
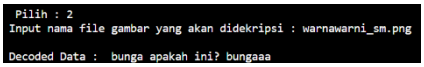
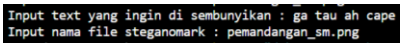
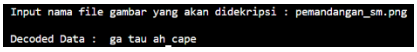
Berdasarkan tabel diatas, selain penambahan watermark yang terlihat, tidak ada perubahan warna yang terlihat.

No	Jenis Gambar	Perbedaan	Gambar Asli	Gambar Watermark	Gambar SteganoMark
1	**Polos**	Ukuran file	2,12 KB	7.33 KB	9,32 KB
2	**Hitam Putih**		34,3 KB	43,1 KB	50,2 KB
3	**Warnawarni**		3,12 MB	3.09 MB	2,85 MB
4	**Pemandangan**		3,75 MB	3,72 MB	3,87 MB

Tabel 3.2 perbedaan ukuran file gambar asli dan gambar setlah dilakukan enkripsi

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Berdasarkan tabel diatas, diketahui setiap penambahan yang dilakukan baik penambahan watermark maupun pesan tersembunyi menimbulkan perubahan pada ukuran file. Adapun pada proses deskripsi, dari seluruh pesan yang diinput pada gambar steganomark, dapat dilihat pada tabel 3.3 dibawah.

No	Jenis Gambar	Gambar SteganoMark	
		Enkripsi	Dekripsi
1	Polos		
2	Hitam Putih		
3	Warnawarni		
4	Pemandangan		

Tabel 3.3 penyisipan pesan

Pada tabel diatas, dapat dilihat isi pesan yang telah di masukkan untuk proses enkripsi, pada proses dekripsi semua pesan tersebut dapat ditampilkan seluruhnya tanpa ada pengurangan atau penambahan maupun kecacatan pada teks.

4. Kesimpulan

Berdasarkan proses dan hasil penelitian yang telah kami lakukan, yaitu pembuatan aplikasi menggunakan Steganografi dengan metode LSB (least significant bit) dan visible watermark untuk melindungi hak cipta berhasil. Aplikasi yang kami buat berhasil menyisipkan baik visible watermark dan pesan rahasia ke dalam sebuah gambar digital berformat *PNG yang dimana hampir tidak ada perubahan yang terlihat dari sampul gambar selain penambahan watermark. Pesan rahasia yang disisipkan juga berhasil ditampilkan seutuhnya. Dengan hal ini, pengguna yang menyisipkan steganomark pada gambar yang mereka miliki dapat memiliki bukti hak cipta dari gambar tersebut.

References

[1] A. Muh. Ramadhani and Tasrif Hasanuddin, “Modifikasi Least Significant Bits pada Gambar sebagai Data Hiding Steganography,” *Indones. J. Data Sci.*, vol. 2, no. 2, pp. 91–102, 2021, doi: 10.56705/ijodas.v2i3.48.

[2] Y. P. Dewi, “Pengembangan Teknik Steganografi Dengan Kriptografi Modifikasi dari Caesar Cipher dan SHA-256 Untuk Merahasiakan Pesan,” *J. Comput. Sci. Vis. …*, vol. 5, pp. 10–21, 2020, [Online]. Available: http://journal.unusida.ac.id/index.php/jik/article/view/129%0Ahttps://journal.unusida.ac.id/index.php/jik/article/download/129/215.

[3] N. A. Ramadhani and I. Susilawati, “Penerapan Steganografi untuk Penyisipan Pesan Teks pada Citra Digital dengan Menggunakan Metode Least Significant Bit,” *J. Multimed. Artif. Intell.*, vol. 4, no. 1, pp. 21–27, 2020.

[4] D. Tupen, W. E. Sridaryanto, and ..., “Penerapan Least Significant Bit untuk Penyisipian Penanda Pada Gambar,” *J. Infomedia Tek. …*, vol. 5, no. 1, 2020, [Online]. Available: http://e-jurnal.pnl.ac.id/index.php/infomedia/article/view/1577.

[5] S. Lutfi and R. Rosihan, “Perbandingan Metode Steganografi Lsb (Least Significant Bit) Dan Msb (Most Significant Bit) Untuk Menyembunyikan Informasi Rahasia Kedalam Citra Digital,” *JIKO (Jurnal Inform. dan Komputer)*, vol. 1, no. 1, pp. 34–42, 2018, doi: 10.33387/jiko.v1i1.1169.
[6] V. Kristianingrum, M. Faishal, and A. S. Yuda Irawan, “Systematic Literature Review: Rancang Bangun Image Digital Watermarking,” *JBMI (Jurnal Bisnis, Manajemen, dan Inform.*, vol. 19, no. 1, pp. 48–60, 2022, doi: 10.26487/jbmi.v19i1.20246.

(