

PERPADUAN INTERPOLASI *BILINEAR* DAN *LEAST SIGNIFICANT BIT* PADA CITRA DIGITAL DALAM TEKNIK STEGANOGRAFI

Garno¹, Riza Ibnu Adam², Dadang Yusup³

^{1,2,3}Program Studi Teknik Informatika
Fakultas Ilmu Komputer
Universitas Singaperbangsa Karawang
Email : garno@staff.unsika.ac.id¹, riza.adam@staff.unsika.ac.id²,
dadang.dyf@staff.unsika.ac.id³

(Naskah masuk: 17 Desember 2018, diterima untuk diterbitkan: 28 Februari 2019)

ABSTRAK

Penelitian ini bergerak bidang steganografi dengan kombinasi proses awal pada citra *cover*. Pengaruh ketika suatu *cover image* diselipi pesan berupa *file* diantaranya berubahnya kapasitas dan ciri secara fisik lainnya dari *cover image* tersebut sehingga secara *interceptibility* terlihat, hal ini mengakibatkan tujuan dari steganografi tidak tercapai. Penelitian ini mengajukan metode preparation proses yang digunakan untuk mengolah *cover image* yaitu dengan interpolasi bilinear sebagai cara pembesaran. Setelah *cover image* diproses pembesaran baru proses steganografi dimulai dengan *least significant bit*. Kontribusi yang diberikan pada penelitian ini dengan hasil tingkat kemiripan *stegoimage* dibanding dengan *original image* sangat besar. Hasil penelitian memiliki tingkat akurasi PSNR senilai 59,09 db dan MSE senilai 0.17 db. Artinya proses steganografi dengan metode LSB dan interpolasi bilinear sebagai basis dari citranya dan mendapatkan tingkat PSNR yang baik.

Kata Kunci: Steganografi, Penyisipan pesan, interpolasi, *bilinear* interpolasi, *least significant bit* (LSB)

ABSTRACT

This research is engaged in the field of steganography using the initial process on the cover image. Influence when a cover image is inserted in the form of a file, including changes in the physical capacity and characteristics of the cover image. Another characteristic as the effect of steganography is that stegoimage in the interceptibility test is seen, this results in the goal of steganography not being reached. This study proposes a process preparation method used to process cover images, namely by bilinear interpolation as a way of enlarging images. The image cover that has been processed zooming is then processed with least significant bit steganography. Contributions in this

study provide the results of the similarity of stegoimage with a very large original image. The results of the study have an accuracy of PSNR worth 59.09 db and MSE worth 0.17 db. This means that the steganography process with the LSB method and bilinear interpolation as the basis of its image and get a good level of PSNR.

Keywords: Steganography, Message insertion, interpolation, bilinear interpolation, least significant bit (LSB)

PENDAHULUAN

Skema penyembunyian data merupakan salah satu subjek penelitian yang penting dibidang kriptografi dan keamanan informasi (Irawan, Purnomo, & Kelana, 2018) (C. Yang, 2016). Pengolahan media penyembunyian banyak dilakukan untuk mendapatkan hasil sebagai syarat keamanan informasi yang baik (Syafrizal, 2007). Media penyembunyian atau sering disebut *coverimage* (Nurfauzan, Hidayat, & Saidah, 2018) digunakan untuk menyelipkan pesan. Hasil penyelipan jika semakin besar nilai kemiripan *stegoimage* dengan *original image* maka semakin baik (Prasetyo, 2018), berarti secara kasat mata tidak terlihat perbedaan antara *originalimage* dengan *stegoimage*. Teknik penyembunyian pesan atau sering disebut steganografi (Sembiring, 2013) (Edisuryana, Isnanto, & Somantri, 2013) banyak ragam cara dan metode, semuanya bertujuan untuk meningkatkan nilai samar dan memperkecil nilai *error* (Neyman, Guritman, & Lindayati, 2012).

Steganografi untuk pengamanan pesan rata-rata dari penelitian sebelumnya memiliki permasalahan hasil yang masih terlihat kasar sehingga nilai MSE dari *stegoimage* besar dan tingkat perbedaan antara *image* asli dan *stegoimage* atau nilai PSNR masih tergolong ketara. Permasalahan lain dari steganografi yaitu pada steganografi yang dipergunakan untuk penyisipan pesan berupa *file-file* besar yang secara umum mempengaruhi intensitas, resolusi dan *size* dari *stegoimage* yang dihasilkan. Proses pembesaran gambar atau *zooming* pada *cover* semula dimaksudkan untuk mendapatkan kapasitas yang besar dari data yang disembunyikan namun sering memiliki efek hasil *stegoimage* yang berbentuk kasar dan mudah terlihat perbedaan antara *coverimage* dengan *stegoimage*

sehingga secara akurasi nilai PNSR kecil dan MSE besar. Banyak ragam metode proses *zooming* pada *image* dan rata-rata menggunakan teknik interpolasi. Teknik ini ada berbagai macam seperti interpolasi *nearest neighbor*, interpolasi *bicubic*, interpolasi *lagrange*, interpolasi *bilinear*, interpolasi *spline*, interpolasi *newton* dan lain-lain (Pratama, Sianipar, & Wiryajati, 2014).

Penelitian sebelumnya yang pertama yaitu permasalahan dalam pengolahan citra diatasi dengan interpolasi *bicubic* modifikasi yang dimodelkan dengan uji berbagai skala *image* namun tidak digunakan dalam steganografi, dan mendapatkan hasil pengujian citra berformat jpg yang memiliki dominan PSNR yang baik sekitar 37,59 dB pada citra RGB dan 40,08 dB pada citra *greyscale*, penelitian ini berjudul Implementasi Metode Interpolasi *Bicubic* Modifikasi pada Proses *Downsampling* Citra, dan pada penelitian tersebut memiliki problem pada pengiriman citra digital yang memiliki *size* besar membutuhkan bandwidth internet yang besar dan waktu yang lama (Wijaya, Saputra, & Alamsyah, 2016). Penelitian yang kedua yaitu pengolahan citra yang digunakan untuk menyelipkan data berupa gambar dengan metode pemrosesan gambarnya dengan *neighbor mean interpolation* dan metode penyelipannya menggunakan LSB dan optimal *pixel adjustment process* (OPAP) penelitian ini mengusulkan mengatasi masalah dari nilai *interceptibility* yang tidak tinggi. Paper ini berjudul *improving stego image quality in image interpolation based data hiding*, dan mendapatkan hasil akurasi PSNR mencapai 45,26 dB (C. Yang, 2016). Penelitian ketiga yang berjudul *An interpolation based texture and pattern preserving algorithm for inpainting color image*, dalam paper ini mengatasi masalah pada suatu penelitian sering tidak efisien ketika dimensi data meningkat walaupun semula memiliki akurasi yang tinggi dan lebih mendasar lagi problem yang ada jika dalam *image* ditemukan tekstur dan pola disuatu area tersebut hilang. Penelitian ini menggunakan metode *langrange* interpolasi dan mendapatkan hasil lebih baik dari sebelumnya (Karaca & Tunga, 2018).

Penelitian steganografi ini dilakukan mengukur kualitas hasil *stego* secara *fidelity* untuk mengetahui PSNR dan MSE. Secara teknis pengujian dilakukan

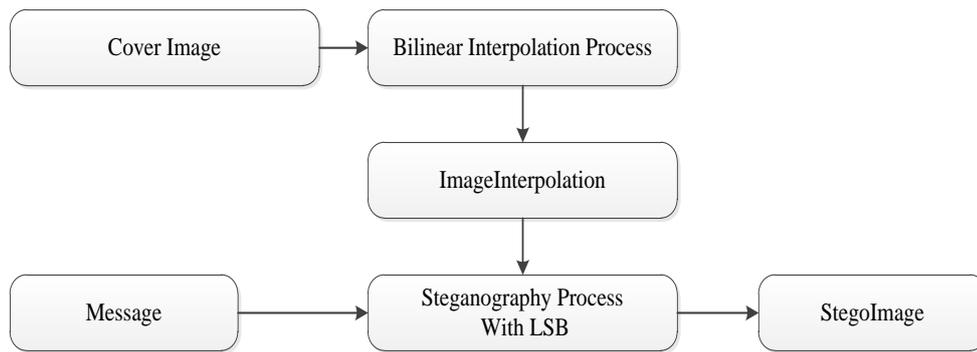
dengan menyelipkan *file* pesan berformat doc/docx, pdf, zip atau txt pada *imageinterpolasi*, pada hasil dan pembahasan hanya menampilkan hasil uji penyelipan pesan ke dalam *imageinterpolasi* sehingga menghasilkan *stegoimage*, dan hasil pengujian kualitas *stegoimage* mengetahui nilai PSNR dan MSE. Penelitian memiliki tahapan dengan melakukan teknik *preparation* proses terhadap *coverimage* dengan Interpolasi *Bilinear* sebagai bentuk pengolahan citra diawal, sehingga kualitas citra yang digunakan sebagai media penyelipan memiliki intensitas dan resolusi tinggi. Steganografi dikerjakan setelah proses interpolasi *bilinear* pada *coverimage* selesai, kemudian dilakukan teknik penyisipan pesan dengan metode *least significant bit* (LSB) sehingga memiliki efek nilai akurasi PNSR yang besar dan MSE yang kecil, yang artinya kualitas hasil *stegoimage* memiliki nilai baik.

METODE PENELITIAN

Metode penelitian yang dipergunakan dalam penelitian adalah eksperimen, dengan langkah sebagai berikut:

1. Mengkaji berbagai sumber dari journal-journal terbaru dengan menganalisis *research question* setiap paper tersebut.
2. Pengumpulan bahan dan tools yang dipergunakan dalam penelitian.
3. Eksperimen dan pengujian dengan melakukan langsung uji penyelipan pesan ke dalam *cover image* yang telah di interpolasi.
4. Menguji kualitas hasil steganografi dengan uji objektif yaitu uji *fidelity*.

Metode yang bekerja dalam proses uji steganografi dapat dilihat pada Gambar 1.

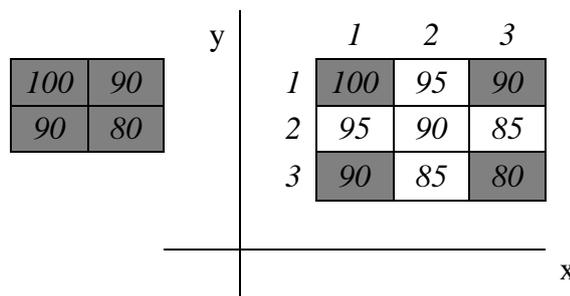


Gambar 1. Proses Steganografi

Steganografi seperti Gambar 1, pertama melakukan proses pada *coverimage*. *Coverimage* dengan ukuran yang sudah ditentukan di proses interpolasi *bilinear*, kemudian dari proses menghasilkan *imageinterpolasi*. Hasil ini yang akan menjadi wadah media untuk menyisipkan pesan. Proses steganografi dengan metode *least significant bit* dengan menyisipkan pesan dilakukan setelahnya dan menghasilkan *file* baru dengan istilah *stegoimage*.

Proses Interpolasi *bilinear* yang terjadi pada *cover image* yaitu bekerja dengan melakukan proses pada salah satu sisi terlebih dahulu (vertikal atau horizontal) kemudian baru mengerjakan proses pada sisi yang lain (W. Yang et al., 2018).

Adapun dalam proses pembesaran *image* secara interpolasi *bilinear* dimodelkan seperti Gambar 2 berikut;



Gambar 2. Proses Interpolasi *Bilinear*

Gambar 2 sebagai bentuk model interpolasi *bilinear*, secara matematis di rumuskan dengan bentuk sebagai berikut;

$$f(x) = f(x_0) + \frac{f(x_1)-f(x_0)}{x_1-x_0} (x - x_0) \quad (1)$$

Adapun keterangan pada rumus persamaan (1) diatas, untuk mendapatkan nilai setiap pixel seperti pada Gambar 2, dapat dilihat perhitungannya sebagai berikut;

1. $f(95) = f(x_1) + \frac{f(x_3) - f(x_1)}{x_3 - x_1} (x - x_1)$
 $= 100 + \frac{90-100}{3-1} (2 - 1)$
 $= 95$
2. $f(85) = f(x_1) + \frac{f(x_3) - f(x_1)}{x_3 - x_1} (x - x_1)$
 $= 90 + \frac{80-90}{3-1} (2 - 1)$
 $= 85$
3. $f(95) = f(y_1) + \frac{f(y_3) - f(y_1)}{y_3 - y_1} (y - y_1)$
 $= 100 + \frac{90-100}{3-1} (2 - 1)$
 $= 95$
4. $f(90) = f(y_1) + \frac{f(y_3) - f(y_1)}{y_3 - y_1} (y - y_1)$
 $= 95 + \frac{85-95}{3-1} (2 - 1)$
 $= 90$
5. $f(85) = f(y_1) + \frac{f(y_3) - f(y_1)}{y_3 - y_1} (y - y_1)$
 $= 90 + \frac{80-90}{3-1} (2 - 1)$
 $= 85$

Proses steganografi dengan LSB pada *imageinterpolasi* berubah menjadi *biner* dan *file* pesan berubah menjadi *biner* kemudian proses penyelipan dilakukan, adapun bentuk metode penyelipan dengan LSB dapat dilihat sebagai berikut;

Misalnya pesan yang ingin disisipkan adalah A dalam 3 *pixel* dan asumsikan tidak ada kompresi. *Raster* data asli untuk 3 *pixel* (9 *byte*) menjadi:

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

Nilai *biner* untuk A adalah 10000011. Sisipkan untuk nilai biner untuk A dalam tiga *pixel*, maka akan dihasilkan:

(00100111 11101000 11001000)
 (00100110 11001000 11101000)
 (11001001 00100111 11101001)

Bit-bit yang digaris bawahi hanya tiga perubahan secara aktual dalam 8 *byte* yang digunakan. Secara rata-rata LSB membutuhkan hanya setengah *bit* dalam suatu perubahan suatu gambar (Hermansyah & Siahaan, 2018).

HASIL DAN PEMBAHASAN

Hasil pengujian dari steganografi penyisipan pesan dengan metode LSB pada citra berbasis interpolasi *bilinear* dapat dilihat pada Tabel 1.

Tabel 1. Hasil Penyisipan *File* Pesan pada Citra *Stego*

No.	Pesan	Citra Cover	Citra Stego
1	Soal.docx (20.6 KB)	 Baboon.bmp (4.68 MB)	 Baboon_Stegodocx.bmp(4.68 MB)
2	Pesan.zip (18.1 KB)	 Baboon.bmp (4.68 MB)	 Baboon_Stegozip.bmp (4.68 MB)
3	Teks.txt (3.34 KB)	 Baboon.bmp (4.68 MB)	 Baboon_Stegotxt.bmp (4.68 MB)
4	Soal.docx (20.6 KB)	 Tiger.jpg (227 KB)	 Tiger_Stegodocx.jpg (227 KB)
5	Pesan.zip (18.1 KB)	 Tiger.jpg (227 KB)	 Tiger_Stegozip.jpg (227 KB)
6	Teks.txt (3.34 KB)	 Tiger.jpg (227 KB)	 Tiger_Stegotxt.jpg (227 KB)

No.	Pesan	Citra Cover	Citra Stego
7	Soal.docx (20.6 KB)	 Koala.png (1.81 MB)	 Koala_Stegodocx.png (1.81 MB)
8	Pesan.zip (18.1 KB)	 Koala.png (1.81 MB)	 Koala_Stegozip.png (1.81 MB)
9	Teks.txt (3.34 KB)	 Koala.png (1.81 MB)	 Koala_Stegotxt.png (1.81 MB)

Penyisipan pesan terhadap citra *cover* rata-rata tidak mengalami perubahan yang cukup nampak jelas secara kasat mata. Hal ini menunjukkan bahwa penyisipan pesan ke dalam citra *cover* adalah tidak terlalu mempengaruhi kualitas citra *stego* dalam penglihatan manusia.

Hasil proses steganografi menghasilkan citra *stego* atau sering disebut *stegoimage*. Adapun untuk mengetahui nilai akurasi dari *stegoimage* sesuai uji objektif yaitu aspek *fidelity* untuk mengetahui PSNR dan MSE dapat dilihat pada Tabel 2.

Tabel 2. Nilai MSE dan PSNR Citra *Stego* /*stegoimage*

No.	Citra Stego	MSE	PSNR (dB)
1	 Baboon_Stegodocx.bmp (4.68 MB)	0,59	50,51
2	 Baboon_Stegozip.bmp (4.68 MB)	0,39	52,22

No.	Citra Stego	MSE	PSNR (dB)
3	 Baboon_Stegotxt.bmp (4.68 MB)	0,09	58,61
4	 Tiger_Stegodocx.jpg (227 KB)	0,02	64,06
5	 Tiger_Stegozip.jpg (227 KB)	0,01	66,41
6	 Tiger_Stegotxt.jpg (227 KB)	0,01	66,82
7	 Koala_Stegodocx.png (1.81 MB)	0,25	54,06
8	 Koala_Stegozip.png (1.81 MB)	0,16	55,97
9	 Koala_Stegotxt.png (1.81 MB)	0,03	63,16

Hasil pengujian secara rata-rata dapat disajikan nilai MSE rata-rata adalah 0,17 dB dan nilai rata-rata dari PSNR adalah 59,09 dB.

KESIMPULAN DAN SARAN

Hasil dari pemanfaatan interpolasi *bilinear* yang digunakan untuk memproses *cover image* dan kemudian digunakan untuk menyelipkan pesan rata-

rata memiliki nilai PSNR 59,09 dB yang artinya memiliki tingkat kemiripan dengan *coverimage* sebelum diselipi pesan nilainya tinggi atau baik karena masih melebihi dari 40 dB sebagai setandar minimum kemiripan.

Hasil pengujian MSE didapatkan nilai rata-rata 0,17 dB yang artinya memiliki tingkat *error* kecil. Maka dari hasil penelitian ini dengan tema teknik steganografi dengan metode LSB pada citra berbasis interpolasi *bilinear* dapat dikategorikan sangat baik.

Saran buat penelitian berikutnya agar melakukan penelitian dengan penyelipan pesan berbentuk *video* atau *audio* pada *image* interpolasi dan menggunakan metode-metode dengan tingkat kompresi yang lebih tinggi sehingga minim mempengaruhi kondisi *cover image* sebagai media penampung.

DAFTAR PUSTAKA

- Edisuryana, M., Isnanto, R. R., & Somantri, M. (2013). Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode End of File. *Transien*, 2(3), 1–9.
- Hermansyah, & Siahaan, A. P. U. (2018). Technique of Hiding Information in Image using Least Significant Bit. *International Journal for Innovative Research in Multidisciplinary Field*, 4(10), 67–70.
- Irawan, P. lucky T., Purnomo, B., & Kelana, O. H. (2018). Rancang Bangun Aplikasi Manajemen Hak Cipta Citra Digital Menggunakan Des Dan Lsb. *Jurnal SimanteC*, 6(3), 105–112.
- Karaca, E., & Tunga, M. A. (2018). An interpolation-based texture and pattern preserving algorithm for inpainting color images. *Expert Systems with Applications*, 91, 223–234. <http://doi.org/10.1016/j.eswa.2017.09.001>
- Neyman, S. N., Guritman, S., & Lindayati. (2012). Teknik Penyembunyian Data Rahasia pada Berkas Gambar Digital Menggunakan Steganografi Least Significant Bit Variable-Sized. *Jurnal Ilmu Komputer Agri-Informatika*, 1, 30–36.

- Nurfauzan, R. A., Hidayat, B., & Saidah, S. (2018). Analisis Steganografi Ganda pada Citra Digital Menggunakan Metode Discrete Wavelet Transform dan Singular Value Decomposition dengan Penyisipan Spread Spectrum Image Steganography. *Proceeding of Engineering*, 5(1), 299–304.
- Prasetyo, D. (2018). Peningkatan Ekstraksi Fitur Berbasis Scale Invariant Feature Transform Menggunakan Metode Multiscale Retinex Untuk Meningkatkan Jumlah Keypoint. *Jurnal Teknikom*, 2(2).
- Pratama, R., Sianipar, R. ., & Wiryajati, I. K. (2014). Pengaplikasian Metode Interpolasi Dan Ekstrapolasi Lagrange , Chebyshev Dan Spline Kubik Untuk Memprediksi. *Dielektrika*, 1(2), 116–121.
- Sembiring, S. (2013). Perancangan Aplikasi Steganografi Untuk Menyisipkan Pesan Teks Pada Gambar Dengan Metode End Of File. *Pelita Informatika Budi Darma*, 4(2), 1–7. <http://doi.org/ISSN: 2301-9425>
- Syafrizal, M. (2007). ISO 17799 : Standar Sistem Manajemen Keamanan Informasi. *Seminar Nasional Teknologi 2007*, 2007(November), 1–10.
- Wijaya, F., Saputra, R., & Alamsyah, D. (2016). Implementasi Metode Interpolasi Bicubic Modifikasi pada Proses Downsampling Citra. *Jutisi*, 2(2).
- Yang, C. (2016). Improving Stego Image Quality in Image Interpolation Based Data Hiding. *Computer Standards & Interfaces*. <http://doi.org/10.1016/j.csi.2016.10.005>
- Yang, W., Liu, J., Li, M., & Guo, Z. (2018). Isophote-Constrained Autoregressive Model with Adaptive Window Extension for Image Interpolation. *IEEE Transactions on Circuits and Systems for Video Technology*, 28(5), 1071–1086. <http://doi.org/10.1109/TCSVT.2016.2638864>