Nusantara Journal of Computersand its Applications
Volume 1– No.1, Juni 2016

Penerapan Metode Steganografi One Domain (OD) Untuk Keamanan Penyisipan Data Pada File Gambar

Rahmad Zainul Abidin
[1,)]Program Studi Teknik Informatika Universitas Yudharta
Jl. Pesantren Ngalah No.7 Sengonagung Purwosari Pasuruan
e-mail: abidin@yudharta.ac.id

ABSTRAK

Berbagai teknik untuk menangkal kejahatan yang menggunakan teknologi informasi telah dilakukan, seperti teknik penyampaian pesan dengan steganografi LSB (Least Significan Bit). Namun LSB memiliki kelemahan, yaitu menyisipkan data pada semua warna merah hijau biru (RGB). Hal ini akan mengakibatkan pixel gambar akan lebih banyak berubah. Sedangkan steganografi OD (One Domain) perubahan warna pixel lebih sedikit dikarenakan hanya warna merah saja yang disisipi teks . Berdasarkan kelemahan LSB tersebut maka penelitian ini mengusulkan teknik steganografi OD sebagai teknik penyisipan data rahasia pada gambar digital.

Proses pengujian penelitian ini dengan diuji dengan analisis PNSR, untuk mengetahui tingkat perubahan gambar asli (cover image) dengan gambar sisipan (stego image).

Hasil dan kesimpulan yang didapat bahwa metode steganografi OD lebih baik dari pada steganografi LSB.

***Kata Kunci**: Steganografi, One Domain, stego image.*

ABSTRACT

Various techniques to ward off evil that use information technology have been made, such as the delivery of messages with steganographic techniques LSB (Least significan Bit). However LSB has a weakness, which inserts the data on all of the colors red green blue (RGB). This will result in more pixels the image will change. While steganography OD (One Domain) pixel color change less because only the red color just inserted text. Based on LSB weakness, this research proposes a steganography technique OD as the insertion technique of confidential data on digital images.

The testing process was tested by this research with PNSR analysis, to determine the rate of change in the original image (cover image) with the inset image (stego image).

The results and conclusions obtained that OD steganographic method is better than the LSB steganography.

***Keywords:**Steganography, One Domain, stego image*

I. PENDAHULUAN

Tindak kejahatan dan kriminal pada sekarang ini sudah banyak melibatkan teknologi informasi dan komunikasi. Pemanfaatan komputer, telepon genggam, email, Internet, dan perangkat digital lainnya bisa mengundang berbagai pihak untuk melakukan kejahatan berbasis teknologi komunikasi. Oleh karena itu, dibutuhkan teknik untuk mengamankan penyampaian teks agar orang tidak mampu menyadap atau mengambil pesan teks tersebut untuk kejahatan.

Diantara teknik untuk mengamankan penyampaian pesan teks adalah dengan metode Steganografi (Yadav, 2011). Steganografi adalah suatu metode untuk menyembunyikan suatu pesan di dalam pesan yang lain yang mana orang lain tidak mencurigai bahwa pesan rahasia tersebut ada di balik pesan yang tampak. Tujuan pengembangan Steganografi adalah mempertahankan data pesan yang disisipkan pada media citra digital agar tidak bisa terdeteksi oleh aplikasi lain bahwa di dalam citra digital tersebut tersembunyi pesan rahasia.

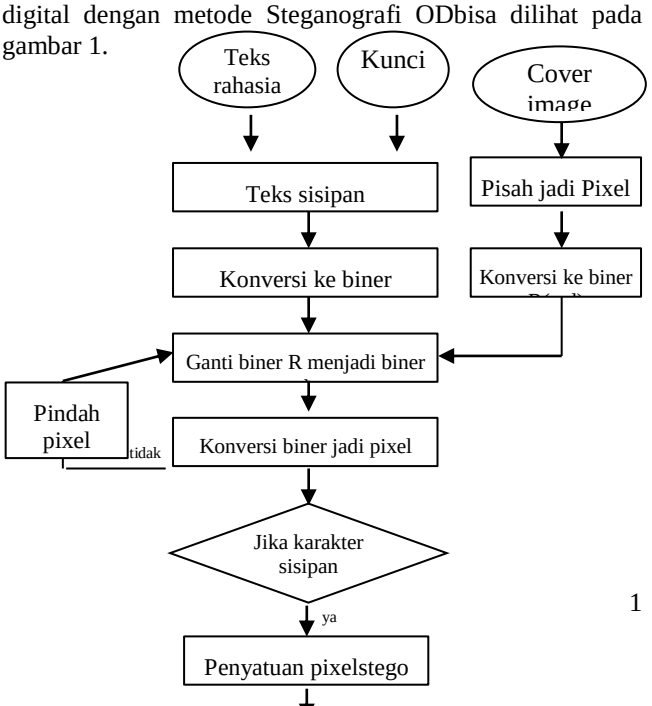
Teknik penyampaian pesan teks dengan steganografi sudah dilakukan, seperti penelitian yang telah dilakukan oleh Wijaya (2014) tentang LSB. Namun steganografi LSB memiliki kelemahan, yaitu menyisipkan pesan teks kepada bit terakhir semua warna RGB (merah, hijau, biru). Hal ini akan mengakibatkan setiap pixel akan lebih banyak mengalami perubahan warna. Berbeda dengan steganografi OD dalam penyisipan data menggunakan warna merah saja. Sehingga warna setiap pixel akan lebih sedikit mengalami perubahan warna.

Berdasarkan penjelasan kelemahan tersebut maka penelitian ini mengambil teknik OD (One Domain) sebagai metode keamanan pada steganografinya. Jadi fokus penelitian ini terletak pada penerapan sistem metode steganografi OD. Yang dimaksud dengan membangun sistem di sini adalah membuat algortima steganografi OD.

II. METODE STEGANOGRAFI ONE DOMAIN

A. Konsep Steganografi OD (One Domain)

Algoritma penyisipan tesk rahasia pada sebuah gambar digital dengan metode Steganografi ODbisa dilihat pada gambar 1.



Gambar 1. Algoritma Steganografi OD.

Berikut ini penjelasan algoritma steganografi OD:

1. Menggabungkan teks rahasia dengan teks kunci menjadi satu teks sisipan.
2. Mengkonversi teks sisipan menjadi bilangan biner.
   Misalkan teks sisipan adalah "A" maka binernya 00001111
3. Memisah gambar utuh menjadi pixel-pixel yang berurutan.
4. Mengkonversi pixel(baris, kolom) menjadi bilangan biner. Hanya pixel warna merah saja (R)
   Misalkan
   pixel(1, 1) = RGB (255, 255, 255) maka R = 255, dikonversi biner R jadi 11111111
   pixel(1, 2) = RGB (254, 255, 255) maka R = 255, dikonversi biner R jadi 11111110
   pixel(1, 3) = RGB (253, 255, 255) maka R = 255, dikonversi biner R jadi 11111101
   pixel(1, 4) = RGB (252, 255, 255) maka R = 255, dikonversi biner R jadi 11111100
   pixel(1, 5) = RGB (251, 255, 255) maka R = 255, dikonversi biner R jadi 11111011
   pixel(1, 6) = RGB (250, 255, 255) maka R = 255, dikonversi biner R jadi 11111010
   pixel(1, 7) = RGB (249, 255, 255) maka R = 255, dikonversi biner R jadi 11111001
   pixel(1, 8) = RGB (248, 255, 255) maka R = 255, dikonversi biner R jadi 11111000

5. Mengganti biner R menjadi biner teks sisipan.
   Misalkan biner sisipan = 00001111, sedangkan biner R = 11111111

Biner R pixel1-8	1 1 1 1 1 1 1	1 1 1 1 1 1 0	1 1 1 1 1 0 1	1 1 1 1 1 0 0	1 1 1 1 1 1 1	1 1 1 1 0 1 0	1 1 1 1 0 0 1	1 1 1 1 0 0 0
Biner sisipan	0	0	0	0	1	1	1	1
Biner baru	1 1 1 1 1 1 1 0	1 1 1 1 1 1 1 0	1 1 1 1 1 1 0 0	1 1 1 1 1 1 0 0	1 1 1 1 1 0 1 1	1 1 1 1 1 0 1 1	1 1 1 1 1 0 0 1	1 1 1 1 1 0 0 1

   Maka biner baru / biner stego adalah 11111110, 11111110, 11111100, 11111100, 11111011, 11111011, 11111001, 11111001.

6. Mengkonversi biner teks sisipan menjadi pixel stego.
   Jika biner stego adalah 11111110, 11111110, 11111100, 11111100, 11111011, 11111011, 11111001, 11111001, maka pixel stego adalah
   biner stego1 = 11111110 maka pixel stego (1, 1) = RGB (254, 255, 255)
   biner stego2 = 11111110 maka pixel stego (1, 2) = RGB (254, 255, 255)
   biner stego3 = 11111100 maka pixel stego (1, 3) = RGB (252, 255, 255)
   biner stego4 = 11111100 maka pixel stego (1, 4) = RGB (252, 255, 255)
   biner stego5 = 11111011 maka pixel stego (1, 5) = RGB (251, 255, 255)
   biner stego6 = 11111011 maka pixel stego (1, 6) = RGB (251, 255, 255)
   biner stego7 = 11111001 maka pixel stego (1, 7) = RGB (249, 255, 255)
   biner stego8 = 11111001 maka pixel stego (1, 8) = RGB (249, 255, 255)

7. Mengulangi langkah 3-6 sampai karakter teks sisipan yang terakhir.
8. Menyatukan/menggabungkan semua pixel menjadi satu gambar utuh.

III. IMPLEMENTASI DAN PEMBAHASAN

A. Sampel Gambar

Adapun sampel image diambil dari database laboratorium SIPI-USC (Signal and Image Processing Institute – University of Southern California). Database gambar SIPI-USC adalah kumpulan gambar standar yang dapat digunakan untuk penelitian gambar dan analisis citra. Sampel gambar yang diambil adalah gambar yang berkarakteristik foto udara dari luar angkasa dengan ukuran gambar 512x512 pixel, kedalaman warna 24 bit per pixel, serta ukuran file sebesar 786.572 bytes dengan format file TIFF, dan nama filenya "2.1.02.tiff" yang bisa didownload di (http://sipi.usc.edu/database/database.php).

Sedangkan untuk melakukan pengujian gambar format file diubah menjadi tipe Bitmap (BMP), dikarenakan format BMP adalah format standar yang biasa digunakan untuk menampilkan gambar dan belum mengalami perubahan kompresi warna. Oleh karena itu file sampel gambar akan dikonversi dahulu dari format TIFF menjadi BMP dengan program Microsoft Paint. Gambar 2 menampilkan file yang sebagai sampel gambar pada penelitian ini.

Gambar 2 Sampel gambar yang digunakan

B. Tampilan GUI

Aplikasi yang dirancang pada penelitian ini menggunakan bahasa pemrograman Visual Basic 6.0yang dapat dilihat pada gambar 3.

Gambar 3 Tampilan GUI BlenBlow

C. Hasil dan Analisis PSNR

Peak Signal to Noise Ratio (PSNR) adalah perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya noise yang berpengaruh pada sinyal tersebut (Ansari, 2015). PSNR merupakan parameter standar untuk menilai kualitas suatu citra secara obyektif dengan membandingkan noise cover image dan stego image terhadap sinyal puncak dalam satuan desibel (dB) (Ansari, 2015). PSNR sering digunakan untuk mengukur kualitas file gambar asli (cover image) dengan file gambar sisipan (stego image). Untuk menghitung nilai PSNR, terlebih dahulu harus menghitung nilai MSE (Mean Squared Error) dengan menggunakan persamaan:

$$\text{MSE} = \frac{1}{M.N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}\left(f(x,y)-g(x,y)\right)^2$$

Keterangan :
f(x,y) = nilai piksel cover image
g(x,y) = nilai piksel stego image
M, N = merupakan dimensi citra

Kemudian menghitung nilai PSNR menggunakan persamaan berikut :

$$\text{PSNR} = 20.\log 10\left(\frac{255}{\sqrt{MSE}}\right)$$

Pada penelitian ini PSNR digunakan untuk menentukan tingkat noise cover image dan stego image. Semakin tinggi nilai PNSR maka semakin sedikit perubahan yang terjadi pada cover image dan stego image, artinya steganografi akan semakin tidak terdeteksi. Nilai MSE yang tinggi menandakan kualitas penyisipan data kurang baik dan sebaliknya nilai yang tinggi PSNR menandakan kualitas penyisipan data sangat baik. Stego image yang baik harus memiliki nilai PSNR diatas 35dB (Cheddad, 2010).

Paramater keamanan yang digunakan pada analisis PNSR adalah mengukur nilai PNSR pada stego image steganografi LSB dan OD. Semakin tinggi nilai PNSR maka semakin tidak terdeteksi stego image, artinya semakin baik dalam meningkatkan penyampaian pesan teks dan semakin rendah nilai MSE maka semakin baik dalam meningkatkan penyampaian pesan teks.

Proses analisis PNSR pada penelitian ini menggunakan 4 sampel gambar (cover image). Pada setiap sampel gambar disisipi pesan teks dengan teknik LSB dan OD. Kemudian pada masing-masing stego image ditentukan nilai PNSR. Kemudian dibandingkan nilai PNSR stego image LSB dengan OD. Tabel 2 menampilkan perbandingan hasil analisis PNSR stego image LSB dan OD.

Sampel gambar	Stego image LSB		Stego image OD	
	MSE	PNSR	MSE	PNSR
Sky	0,1523	40,4943	0,0694	58,2938
Temple	0,1938	40,2948	0,0657	58,4256
Lena	0,1203	41,3384	0,0746	59,4059
Baboon	0,1637	41,3984	0,0785	59,3419

Tabel 2 Perbandingan analisis PNSR stego image LSB dan OD

Pada tabel 2 bisa dilihat bahwa nilai PNSR gambar Sky dengan penyisipan data steganografi LSB bernilai 40,4943 dan nilai MSE 0,1523, sedangkan pada steganografi OD nilai PNSR 58,2938 dan nilai MSE 0,0694. Nilai PNSR OD lebih tinggi dari pada PNSR LSB dan nilai MSE OD lebih rendah dari MSE LSB, maka hasil stego image pada gambar Sky OD lebih baik dari LSB. Pada gambar Temple nilai PNSR steganografi LSB bernilai 40,2948 dan nilai MSE 0,1938, sedangkan pada steganografi OD nilai PNSR 58,4256 dan nilai MSE 0,0657. Nilai PNSR OD lebih tinggi dari pada PNSR LSB dan nilai MSE OD lebih rendah dari MSE LSB, maka hasil stego image pada gambar Temple OD lebih baik dari LSB. Pada gambar Lena nilai PNSR steganografi LSB bernilai 41,3384 dan nilai MSE 0,1203, sedangkan pada steganografi OD nilai PNSR 59,4059 dan nilai MSE

0,0746. Nilai PNSR OD lebih tinggi dari pada PNSR LSB dan nilai MSE OD lebih rendah dari MSE LSB, maka hasil stego image pada gambar Lena OD lebih baik dari LSB. Pada gambar Baboon nilai PNSR steganografi LSB bernilai 41,3984 dan nilai MSE 0,1637, sedangkan pada steganografi OD nilai PNSR 59,3419 dan nilai MSE 0,0785. Nilai PNSR OD lebih tinggi dari pada PNSR LSB dan nilai MSE OD lebih rendah dari MSE LSB, maka hasil stego image pada gambar Baboon OD lebih baik dari LSB.

Pada 4 gambar sampel tersebut semua nilai PNSR OD lebih tinggi dari pada nilai PNSR LSB dan nilai MSE OD lebih rendah dari MSE LSB, maka dengan parameter analisis PNSR dapat disimpulkan bahwa steganografi OD lebih baik dari pada steganografi LSB. Tabel 3 menampilkan ringkasan selisih nilai perbedaan PNSR LSB dengan OD.

Sampel gambar	Selisih MSE LSB terhadap OD	Selisih PNSR LSB terhadap OD
Sky	-0,0829	17,7995
Temple	-0,1281	18,1308
Lena	-0,0457	18,0675
Baboon	-0,0852	17,9435

Tabel 3 selisih nilai MSE PNSR LSB dengan OD

Pada tabel 3 nilai PNSR OD lebih tinggi dari pada nilai PNSR LSB dan nilai MSE OD lebih rendah dari MSE LSB, maka dapat disimpulkan bahwa steganografi OD lebih baik dari pada steganografi LSB.

IV. KESIMPULAN

Berdasarkan hasil yang didapat dari proses implementasi dan pembahasan maka dapat ditarik kesimpulanbahwa implementasi dari steganografi OD perubahan pixelnya lebih sedikit dibandingkan dengan perubahan pixel steganografi LSB sehingga steganografi OD lebih baik.

V.DAFTAR PUSTAKA

[1]. Autoimager. http://www.autoimager.com/download.asp. Diakses pada 1 September 2015

[2]. Ansari, Munawir. (2015).Komparasi Metode Hybrid Image Watermarking DWT-SVD Dengan RDWT-SVD Untuk Proteksi Pada Citra Digital. Yogyakarta, fakultas Teknologi Industri, Universitas Islam Indonesia.

[3]. Boora & Gambhir. (2013). Arnold Transform Based Steganography. International Journal of Soft Computing and Engineering (IJSCE). ISSN: 2231-2307, Volume-3, Issue-4.

[4]. Cheddad, A., Condell, J., Curran, K., Kevitt, P.Mc., 2010. Digital Image Steganography : Survey and Analysis of Current Methods. Signal Processing, Elsevier. Northern Ireland, UK.

[5]. Gutte, Chincholkar and Lahane. (2013). Steganography For Two And Three Lsbs Using Extended Using Extended Substitution Algorithm. Ictact Journal On Communication Technology, March 2013, volume: 04, issue: 01.

[6]. Haldankar & Kuwelkar. (2014). Implementation Of Aes And Blowfish Algorithm. International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN: 2321-7308.

[7]. Padmaa. & Venkataramani. (2014). Encypted Secret OD With Image Steganography For Enhanced Imperceptibility Dan Capacity. Tamilnadu India.

[8]. Poornima & Iswarya. (2013). AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY. International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.1,February 2013.

[9]. SIPI, The USC-SIPI Image Database, website pada http://sipi.usc.edu, diakses pada 24 Agustus 2015.

[10]. Wijaya, Wijaya Satriya. (2014). Integrasi Metode Steganografi LSB Pada Image Dengan Kriptografi Blowfish. Yogyakarta, fakultas Teknologi Industri, Universitas Islam Indonesia.

[11]. Wijaya, Satriya. & Prayudi, Yudi. (2014). Konsep hidden message menggunakan teknik steganografi dynamic cell spreading. Jurnal media informatika, ISSN: 0854-4743, Volume 2. NO. 1, PP 23-38.

[12]. Yadav. (2011). Information Security Using OD of Steganography and Cryptography. Int. J. Comp. Tech. Appl., Vol 2 (6), 2023-2036. ISSN:2229-6093

[13]. Kumar and Karthikeyan. 2012. Investigating the Efficiency of Blowfish and Rejindael (AES) Algorithms. I. J. Computer Network and Information Security, 2012, 2, 22-28. DOI: 10.5815/ijcnis.2012.02.04