

USULAN TUGAS AKHIR

1. IDENTITAS PENGUSUL

Nama : **Brian Madityawan**
NRP : **5108100156**
Dosen Wali : **Ir. FX. Arunanto, M.Sc.**
Dosen Pembimbing : **1. Henning Titi Ciptaningtyas, S.Kom., M.Kom.**
2. Hudan Studiawan, S.Kom., M.Kom.

2. JUDUL TUGAS AKHIR

***“Implementasi Steganografi pada Media Image Berbasis Metode Pixel
Modification Value Menggunakan Fungsi Modulus”***

3. LATAR BELAKANG

Steganografi adalah pengetahuan menyembunyikan data rahasia dengan cara menyisipkan data rahasia di dalam multimedia. Walaupun istilah steganografi dikenal ribuan tahun, praktik steganografi pada media digital datang terlambat dan riset baru dikembangkan di akhir tahun 2001.

Steganalisis adalah ilmu untuk mendeteksi pesan rahasia yang ada dalam objek steganografi. Untuk mengetahui algoritma steganografi didasarkan pada 2 jenis yaitu domain spasial dan domain transform. Tujuan utama steganografi adalah dibuat untuk tidak terdeteksi, ketahanan, dan kapasitas data rahasia. Fitur-fitur ini yang memisahkan dari teknik terkait yang lainnya seperti *watermarking* dan kriptografi.

Metode steganografi *Least Significant Bit* (LSB) adalah pendekatan umum steganografi. Penyisipan, *masking* dan *filtering*, serta transformasi [1] adalah beberapa metode lainnya dalam teknik steganografi. Penyisipan menggunakan metode LSB dengan cara dua atau lebih bit LSB piksel diganti dengan bit rahasia. Chan dan Cheng [2] mengusulkan penggantian LSB dengan pengaturan piksel optimal untuk menanamkan data dengan cara sederhana. Wu dan Tsai [3] mengusulkan sebuah metode *Pixel Value*

Differencing (PVD) dengan kualitas yang bagus dan menyembunyikan lebih banyak data rahasia. Setelah itu, berbagai macam pendekatan berbasis PVD banyak diusulkan [4].

Metode PVD adalah menyembunyikan data berdasarkan perbedaan piksel di dalam gambar aslinya [5]. Di mana area gambar asli akan diklasifikasikan menjadi 2 tipe yaitu daerah halus dan daerah kasar. Di dalam daerah halus perbedaan piksel dengan piksel yang lainnya kecil, sehingga tidak cocok untuk menyisipkan data rahasia. Daerah kasar mempunyai banyak perbedaan dengan piksel tetangganya. Oleh karena itu, daerah kasar cocok untuk menyisipkan data, akan tetapi metode PVD lebih mudah dideteksi.

Dalam usulan tugas akhir ini, pendekatan steganografi menggunakan *Pixel Value Modification* (PVM). Komponen piksel warna akan dipisah menjadi 3 yaitu bidang *Red* (R), *Green* (G), dan *Blue* (B). Metode yang dipakai gambar berwarna digunakan sebagai gambar untuk menyembunyikan data rahasia. Fungsi modulus digunakan pada tiap nilai R, G, dan B gambar. Harapan menggunakan metode PVM adalah agar data rahasia tidak mudah dideteksi oleh pihak ketiga dan kapasitas penyimpanan data rahasia semakin besar.

4. TUJUAN TUGAS AKHIR

Mendapatkan gambar berisi data rahasia yang lebih banyak dan lebih aman menggunakan metode PVM sehingga sulit dideteksi.

5. MANFAAT TUGAS AKHIR

Membantu pengiriman data rahasia melalui internet agar lebih aman. Pihak ketiga yang ingin mengambil data tersebut tidak bisa mencuri data rahasia pengguna lain.

6. RUMUSAN MASALAH

Rumusan masalah yang diangkat dalam tugas akhir ini adalah:

1. Bagaimana menyembunyikan data rahasia dengan cara menyisipkan ke dalam setiap bidang R, G, dan B?
2. Bagaimana mendapatkan data rahasia dari gambar steganografi?

7. BATASAN MASALAH

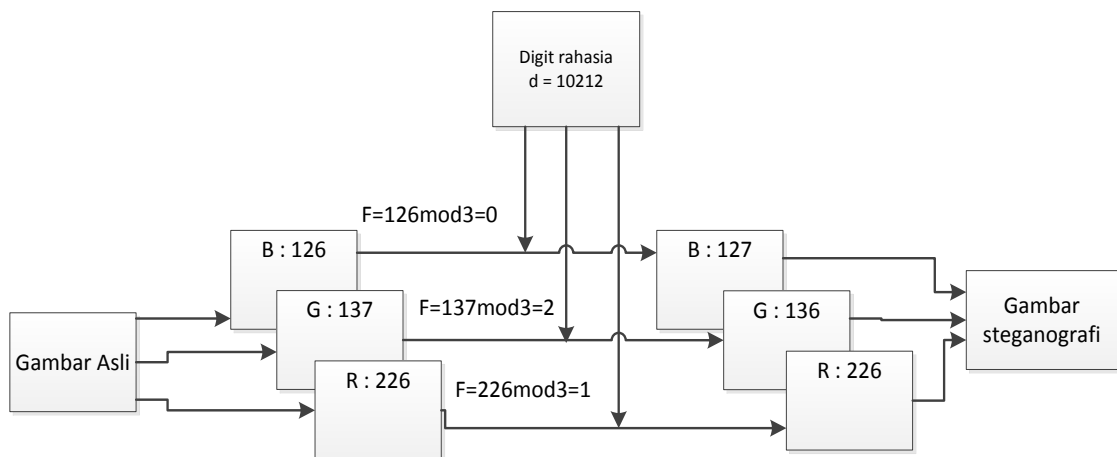
Permasalahan yang dibahas dalam tugas akhir ini memiliki beberapa batasan, yaitu sebagai berikut:

1. Penerapan sistem dalam tugas akhir ini menggunakan aplikasi *desktop*.
2. Menggunakan bahasa pemrograman C#.
3. Prosedur penyisipan dan pengambilan data rahasia menggunakan metode PVM.

8. RINGKASAN TUGAS AKHIR

Metode PVM yang digunakan dalam tugas akhir ini menggunakan cara membagi gambar asli menjadi 3 bidang yaitu bidang R, G, dan B. Setiap piksel mengandung 24 bit karena setiap bidang R, G, dan B mengandung 8 bit komponen di dalam piksel. Metode PVM menggunakan semua 3 komponen matriks untuk menyisipkan data rahasia. Pertama, setiap komponen yang berasal dari setiap piksel dipisahkan dan 3 bagian terpisah matriks berukuran $M \times N$ piksel didapatkan.

Metode PVM untuk penyembunyian data di dalam setiap bidang dilakukan secara berurutan. Penyisipan bit dalam piksel pertama dari bidang matriks R lalu piksel pertama dari bidang matriks G, kemudian piksel pertama dari bidang matriks B. Selanjutnya, menyisipkan nomor yang berbeda dari bit untuk setiap komponen piksel yang berbeda agar meningkatkan keamanan, kapasitas, dan memperbaiki kualitas gambar steganografi yang dihasilkan. Ilustrasi metode PVM dapat dilihat pada Gambar 1.



Gambar 1. Ilustrasi penyisipan data rahasia menggunakan metode PVM

a. Prosedur Penyisipan

Langkah pertama adalah pisahkan gambar asli ke dalam 3 komponen warna matriks dan terapkan setiap langkah penyisipan secara berurutan. Menerapkan langkah penyisipan ke dalam nilai piksel pertama pada matriks R lalu nilai piksel pertama pada

matriks G , kemudian nilai piksel pertama pada matriks B . Langkah penyisipan dilakukan secara terus-menerus pada nilai piksel kedua dan seterusnya.

Langkah kedua adalah buat variabel d sebagai digit rahasia. Data rahasia diubah menjadi 3 nilai (0, 1, 2). Nilai rahasia ini disisipkan ke dalam 3 bidang pada langkah pertama.

Langkah ketiga adalah nilai piksel dari matriks gambar dikelompokkan ke dalam g_1, g_2, \dots, g_n . Nilai desimal dari piksel bidang R direpresentasikan sebagai g_{ri} , sedangkan nilai desimal pada bidang G dan B direpresentasikan sebagai g_{gi} dan g_{bi} . Fungsi f dihitung dengan Persamaan 1 untuk setiap bidang.

$$f = f(g_1, g_2, g_3, \dots, g_n) = \sum^n i = 1 g_{ri} \bmod 3 \quad (1)$$

Langkah keempat adalah memilih piksel yang tepat untuk metode PVM. Piksel yang tepat untuk metode PVM berada dalam jangkauan $0 \leq g_i \leq 250$ dari gambar asli. Fungsi f punya 3 kondisi :

- Kondisi 1 jika $f = d$, lalu modifikasi tidak diperlukan, secara langsung g_{ri} diambil sebagai nilai piksel baru g_{ri}' .
- Kondisi 2 jika $f \neq d$ dan $f < d$, maka tambahkan 1 pada nilai g_{ri} , $g_{ri}' = (g_{ri} + 1)$ kemudian nilai modifikasi piksel yang baru didapatkan.
- Kondisi 3 jika $f \neq d$ dan $f > d$, maka kurangi 1 pada nilai g_{ri} , $g_{ri}' = (g_{ri} - 1)$ kemudian nilai modifikasi piksel yang baru didapatkan.

Langkah kelima adalah lakukan langkah ketiga dan keempat untuk modifikasi nilai piksel dalam bidang matriks G dan B .

Langkah keenam adalah setelah nilai piksel modifikasi didapat dengan data rahasia yang disisipkan di dalam bidang R , G , dan B . Kombinasi pada bidang R , G , dan B ini memberikan hasil gambar steganografi.

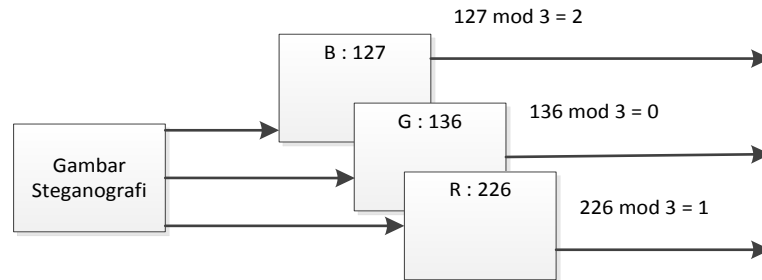
b. Prosedur Ekstraksi

Langkah pertama adalah klasifikasikan gambar steganografi ke dalam 3 komponen bidang R , G , dan B . Untuk menerima gambar steganografi, nilai piksel yang dipilih berkisar antara $0 \leq g_i \leq 253$ pada bidang R , G , dan B .

$$d = g_{ri}' \bmod 3 \quad (2)$$

Langkah kedua adalah nilai piksel dari bidang R diekstrak kemudian gunakan Persamaan 2 untuk mendapatkan digit rahasia d .

Langkah ketiga adalah lakukan langkah ketiga pada bidang G dan B. Akhirnya, digit rahasia berbasis 3 didapatkan bila dikonversi menjadi data rahasia yang asli. Ilustrasi prosedur ekstraksi dapat dilihat pada Gambar 2.



Gambar 2. Ilustrasi ekstraksi menggunakan metode PVM

9. METODOLOGI

Metodologi yang akan dilakukan dalam tugas akhir ini memiliki beberapa tahapan, diantaranya sebagai berikut:

1. Penyusunan Proposal Tugas Akhir

Tahap awal untuk memulai pengerjaan tugas akhir adalah penyusunan proposal tugas akhir. Pada proposal ini, penulis mengajukan gagasan implementasi steganografi menggunakan metode PVM.

2. Studi Literatur

Tahap pencarian literatur dilakukan melalui referensi *paper* utama. Sampai saat ini sudah ada beberapa literatur yang sesuai dengan tugas akhir penulis dan tidak menutup kemungkinan ada tambahan referensi dari sumber lain. Berikut tahap penerapan sistem beserta referensi:

- a) Mempelajari bagaimana mendapatkan nilai setiap piksel menjadi 3 komponen dalam bidang R, G, dan B.
- b) Mempelajari literatur pembuatan aplikasi *desktop* dengan menggunakan bahasa pemrograman C#.
- c) Mempelajari bagaimana menyisipkan gambar dengan metode PVM.
- d) Mempelajari bagaimana mengekstrak data rahasia dari gambar steganografi menggunakan metode PVM.

3. Implementasi

Implementasi merupakan tahap untuk implementasi metode PVM pada steganografi yang digunakan untuk mengamankan data.

4. Pengujian dan Evaluasi

Pada tahap ini dilakukan uji coba terhadap implementasi metode PVM yang telah dibuat, mengamati kinerja metode PVM yang baru dibuat, serta mengidentifikasi kendala yang mungkin timbul.

5. Penyusunan Buku Tugas Akhir

Tahap terakhir merupakan penyusunan laporan yang memuat dokumentasi mengenai pembuatan serta hasil dari implementasi steganografi menggunakan metode PVM yang telah dibuat.

10. JADWAL PEMBUATAN TUGAS AKHIR

| No | Tahapan | Bulan | | | | | | | | | | | |
|----|------------------------|----------|--|--|-------|--|--|-------|--|--|-----|--|--|
| | | Februari | | | Maret | | | April | | | Mei | | |
| 1 | Penyusunan Proposal | | | | | | | | | | | | |
| 2 | Studi Literatur | | | | | | | | | | | | |
| 3 | Perancangan sistem | | | | | | | | | | | | |
| 4 | Implementasi | | | | | | | | | | | | |
| 5 | Pengujian dan Evaluasi | | | | | | | | | | | | |
| 6 | Penyusunan Buku Tugas | | | | | | | | | | | | |

11. DAFTAR ISI

- [1] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE Journal on Selected Areas*, p. pages 474–481, 1998.
- [2] C. Chan and L. Cheng, "Hiding data in images by simple LSB substitution," *pattern recognition*, vol. 37, no. 3, pp. 469-474, 2004.
- [3] D. Wu and W. Tsai, "A Steganographic method for images by pixel-value differencing," *Pattern Recognition Letters*, vol. 24, pp. 1613-1626, 2003.
- [4] H. Wu, N. Wu, C. Tsai and M. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *IEE Proceedings on Vision, Image and Signal Processing*, vol. 152, pp. 611-615, 2005.
- [5] C. Wang, N. Wu, C. Tsai and M. Hwang, "A high quality steganography method with pixel-value differencing and modulus function," *Journal of System Software*, vol. 81, pp. 150-158, 2008.

- [6] K. Chang, C. Chang, P. Huang and T. Tu, "A Novel Image Steganographic Method Using Triway Pixel-Value Differencing," *Journal of Multimedia*, vol. 3, no. 2, pp. 37-44, 2008.
- [7] J. Mandal and D. Das, "Steganography Using Adaptive Pixel Value Differencing (APVD) for Gray Images through Exclusion of Underflow/Overflow," *Computer Science & Information Series*, pp. 93-102, 2012.
- [8] M. Padmaa and D. Y. Venkataramani, "ZIG-ZAG PVD – A Nontraditional Approach," *International Journal of Computer Applications*, vol. 5, pp. 5-10, 2010.
- [9] K.-H. Jung and K.-Y. Yoo, "Improved Exploiting Modification Direction Method by Modulus Operation," *International Journal of Signal Processing, Image Processing and Pattern*, vol. 2, no. 1, 2009.
- [10] J. Mandal and D. Das, "Color Image Steganography Based on Pixel Value Differencing in Spatial Domain," *International Journal of Information Sciences and Techniques (IJIST)*, vol. 2, no. 4, 2012.
- [11] V. Nagaraj, D. V. Vijayalakshmi and D. G. Zayaraz, "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function," *International Conference on Electronic Engineering and Computer Science*, vol. 4, pp. 17-24, 2013.

LEMBAR PENGESAHAN

Surabaya, 2014

Menyetujui,

Dosen Pembimbing I,

Dosen Pembimbing II,

**(Henning Titi Ciptaningtyas, S.Kom.,
M.Kom.)
(NIP. 19840708 201012 2 004)**

**(Hudan Studiawan, S.Kom., M.Kom.)
(NIP. 19870511 201212 1 003)**