

Implementasi Steganografi pada Citra dengan Metode Bit-Plane Complexity Segmentation Untuk Transformasi Data

Johannes Petrus
STMIK GI MDP Palembang
E-mail: johannes@stmik-mdp.net

Abstrak

Pengamanan terhadap informasi atau data yang didistribusikan sangat penting untuk menjaga kerahasiaan, keutuhan, dan keasliannya. Dalam praktek pemilihan kepala daerah dan wakil kepala daerah (Pilkada) di beberapa daerah di Indonesia, sering menyimpan banyak masalah yang berkaitan dengan kerahasiaan data pada saat proses pengiriman jumlah suara. Agar pesan rahasia hanya dapat dibaca dan dimengerti oleh orang tertentu saja, diperlukan cara untuk menyembunyikan pesan tersebut, salah satu cara yang dapat dilakukan adalah dengan mengembangkan aplikasi Transformasi Data Pilkada dimana algoritma steganografi digunakan dalam enkripsi datanya. Steganografi adalah penyembunyian pesan rahasia pada media lain, seperti image, audio atau video sehingga secara kasat mata media yang telah disisipi pesan tampak seperti biasa. Pada tulisan ini, steganografi diterapkan pada gambar digital dengan menggunakan metode Bit-plane complexity segmentation (BPCS). Bit-plane complexity segmentation (BPCS) merupakan teknik steganografi yang memiliki kapasitas besar, karena dapat menampung data rahasia dengan kapasitas yang relatif besar jika dibandingkan dengan metode steganografi lain. Aplikasi Transformasi Data Pilkada yang dikembangkan dapat meminimalisasi kebocoran-kebocoran informasi penting yang sangat rahasia dan bahaya jika sampai diketahui oleh orang lain.

Kata Kunci — Pilkada, Steganografi, Bit Plane Complexity Segmentation (BPCS)

Abstract

The security of distributed information or data is critical to maintain their confidentiality, integrity, and authenticity. In practice of the election of the regional head and deputy head (Pilkada) in several regions in Indonesia, it often occurs problems regarding the confidentiality of data during the delivery process of the vote. In order to make the encrypted message can only be read and understood by a particular person, it is required a technique to hide the message. One of them is to develop an application program of data election transformation using the steganographic algorithm for data encryption. Steganography is a technique for hiding the encrypted messages in other media, such as images, audio or video so that the media that have been inserted the message looks like having no differences than before. In this research, the steganography is applied to digital image using bit-plane complexity segmentation (BPCS) method. Bit-plane complexity segmentation (BPCS) is a steganography technique that has a large capacity, because it can accommodate confidential data with a relatively large capacity compared to other steganographic methods. The application program of data election transformation is developed to minimize leakage of the important informations that are highly confidential and risky to be known by others.

Keywords — Local Elections, Bit Plane Complexity Segmentation (BPCS)

1. PENDAHULUAN

Kerahasiaan dan keamanan suatu informasi pada jaman globalisasi sekarang ini semakin menjadi sebuah kebutuhan vital dalam berbagai aspek kehidupan. Suatu informasi akan memiliki nilai lebih tinggi apabila menyangkut aspek-aspek keputusan bisnis, keamanan, ataupun kepentingan umum. Dimana informasi-informasi tersebut tentunya akan banyak diminati oleh berbagai pihak yang juga memiliki kepentingan di dalamnya.

Sebagai contoh, dalam praktek pemilihan kepala daerah dan wakil kepala daerah di beberapa daerah di Indonesia, sering menyimpan banyak masalah, dan realitasnya tidak sesederhana seperti dalam konsep otonomi maupun konsep pilkada langsung sebagaimana diharapkan oleh Undang-Undang nomor 32 Tahun 2004 sebagai wujud pelaksanaan sistem *desentralisasi* yang nyata kepada daerah. Pengejawantahan dari isi Undang-Undang ini telah dilaksanakan diseluruh daerah di Indonesia, tidak terkecuali Sumatera Selatan (Sumsel) khususnya kota Palembang. Tahun 2008 untuk pertama kalinya digelar pemilihan kepala daerah Kota Palembang secara langsung. Lancarnya pelaksanaan pilkada di kota Palembang menunjukkan bahwa sebenarnya pilkada di kota Palembang dapat ditingkatkan kualitas pelaksanaannya dengan mengedepankan peran Teknologi Informasi di dalamnya[1].

Selain dukungan Teknologi Informasi dalam kelancaran pelaksanaan pilkada, dibutuhkan juga suatu sistem yang dapat memberikan keamanan dalam merahasiakan data ataupun informasi dalam hal ini berupa jumlah suara pada saat proses rekapitulasi guna meminimalisir terjadinya manipulasi terhadap data ataupun informasi tersebut. Agar pesan rahasia tersebut hanya dapat dibaca dan dimengerti oleh orang tertentu saja, maka diperlukan cara untuk menyembunyikannya, yaitu dengan menggunakan teknik steganografi. Kata steganografi (*steganography*) berasal dari bahasa Yunani, yaitu dari kata *Steganos* yang artinya tersembunyi dan *Graphen* yang artinya tulisan. Steganografi adalah teknik menyembunyikan data rahasia di dalam wadah (media) digital sehingga keberadaan data rahasia tersebut tidak diketahui orang. Steganografi membutuhkan dua *property*: wadah penampung dan data rahasia yang akan disembunyikan. Media penampung yang umum digunakan pada teknik steganografi adalah citra, suara (audio), video dan teks. Data rahasia yang disembunyikan juga dapat berupa citra, suara, video atau teks[2]. Selain itu juga Steganografi adalah penyembunyian pesan rahasia pada media lain, seperti *image*, *audio* atau *video* sehingga secara kasat mata media yang telah disisipi pesan tampak seperti biasa[3]. Salah satu teknik Steganografi adalah *Bit-plane complexity segmentation (BPCS)*. *Bit-plane complexity segmentation (BPCS)* merupakan teknik steganografi yang diperkenalkan oleh Eiji Kawaguchi dan Richard O. Eason pada tahun 1998. Teknik ini merupakan teknik steganografi yang memiliki kapasitas besar, karena dapat menampung data rahasia dengan kapasitas yang relatif besar jika dibandingkan dengan metode steganografi lain seperti *LSB (Least Significant Bit)*. Teknik *BPCS* ini adalah teknik steganografi yang tidak berdasarkan teknik pemrograman, tetapi teknik yang menggunakan sifat penglihatan manusia. Sifat penglihatan manusia yang dimanfaatkan yaitu ketidakmampuan manusia menginterpretasi pola biner yang sangat rumit. Eiji Kawaguchi dan R. O. Eason memperkenalkan teknik *BPCS* ini untuk digunakan pada dokumen citra berwarna yang tidak terkompresi dengan format *BMP*. Dokumen citra tersebut dibagi menjadi beberapa segmen dengan ukuran 8x8 piksel setiap segmennya. Pada dokumen citra 8-bit, setiap satu segmen akan memiliki 8 buah *bit plane* yang merepresentasikan piksel-piksel dari setiap bit tersebut. Proses pembagian segmen 8x8 piksel menjadi 8 buah *bit plane* disebut proses *bit slicing*. Representasi kedelapan *bit plane* ini merupakan *PBC system (Pure Binary Code)*. Pada *BPCS*, proses penyisipan dilakukan pada *bit plane* dengan sistem *CGC (Canonical Gray Code)* karena proses *bit slicing* pada *CGC* cenderung lebih baik dibandingkan pada *PBC*. Sehingga pada proses penyisipan, *bit plane* dengan representasi *PBC* diubah menjadi *bit plane* dengan representasi *CGC*. Pada teknik *BPCS*, kapasitas data yang disisipkan dapat mencapai 30-50% dari ukuran *cover image*nya [4].

Tujuan yang hendak dicapai dalam tulisan ini adalah Membangun sebuah aplikasi steganografi pada citra dengan metode *Bit-Plane Complexity Segmentation (BPCS)* dan Melindungi data hasil rekapitulasi Pilkada SUMSEL yang bersifat rahasia agar tidak diketahui oleh orang-orang yang tidak berhak.

2. METODE PENELITIAN

Tahapan yang digunakan dalam penyusunan penelitian ini dapat dilihat pada gambar 1.



Gambar 1. Tahapan Penelitian

Keterangan:

1. Memilih dan menentukan terlebih dahulu permasalahan atau tema apa yang akan diambil.
2. Studi Literatur, metode yang dilakukan adalah membaca, mencari, dan memahami berbagai sumber referensi yang ada, seperti buku, internet.
3. Perbandingan Antar Metode, membandingkan metode – metode steganografi pada citra guna mendapatkan metode yang tepat untuk diimplementasikan pada proses pembuatan aplikasi.
4. Penggunaan suatu metode pengembangan sistem yang tepat dan disesuaikan dengan permasalahan dan aplikasi yang akan dibangun, Metodologi yang digunakan dalam pengembangan aplikasi ini adalah metode sekuensial linier atau metode *waterfall*.
5. Pengujian program adalah tahapan yang dilakukan untuk Validitas dan reliabilitas pada program yang dibuat.
6. Menulis laporan dalam bentuk dokumen.

3. HASIL DAN PEMBAHASAN

3.1. Analisis dan Rancangan

3.1.1. Analisis Kebutuhan Non Fungsional

Berikut ini kebutuhan non fungsional dari aplikasi steganografi pada citra dengan metode *Bit Plane Complexity Segmentation (BPCS)* adalah sebagai berikut:

1. Kinerja, kecepatan proses data tergantung dari maksimal jumlah kapasitas data yang dapat disisipkan ke dalam citra atau tidak melebihi ukuran dari data penampung.

2. *Security*, dimana teks atau pesan rahasia yang disimpan memiliki tingkat keamanan karena disisipkan ke dalam gambar.
3. *Interface*, dengan menggunakan GUI (*Graphical User Interface*) yaitu tampilan grafis yang memudahkan *user* berinteraksi dengan perintah teks berupa komponen-komponen yang terdapat pada bahasa pemrograman yang dipakai penulis dalam pembuatan aplikasi seperti komponen *button*, *open file dialog*, *memo* dan sebagainya, sehingga program yang dibuat menjadi lebih *user friendly*.
4. Kebutuhan *Hardware* dan *Software*.
 - a. Kebutuhan *Hardware*

Dalam membangun aplikasi ini penulis menggunakan laptop dengan spesifikasi sebagai berikut:

 - 1) *Processor Intel Core i3 2.13 GHz*
 - 2) *Memory 2 GB*
 - 3) *Harddisk Drive 320 GB*
 - b. Kebutuhan *Software*

Dalam pengerjaan aplikasi ini dibutuhkan beberapa aplikasi perangkat lunak pendukung antara lain:

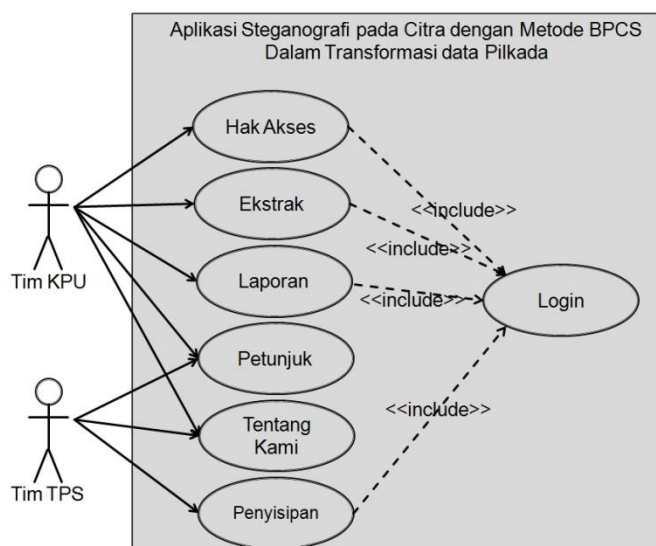
 - 1) *Sistem Operasi*

Dalam hal ini penulis menggunakan sistem operasi *Microsoft Windows 7 Home Basic*.
 - 2) *Bahasa Pemrograman*

Dalam pembuatan aplikasi penulis menggunakan bahasa pemrograman *Borland C++ Builder 6.0*. Pengguna dapat mengoperasikan aplikasi pada semua sistem operasi *windows*.

3.1.2. Analisis Kebutuhan Fungsional

Secara umum fungsionalitas yang dimiliki oleh perangkat lunak sistem aplikasi steganografi pada citra dengan metode *Bit Plane Complexity Segmentation (BPCS)* dalam Transformasi Data Pilkada dapat digambarkan dengan diagram *use case* seperti yang ditunjukkan pada Gambar 2 dan rincian penjelasannya pada Tabel 1.



Gambar 2. Use Case Diagram Sistem Secara Keseluruhan

Tabel 1. Deskripsi Use Case Program

Nama Use Case	Deskripsi	Aktor
Login	Use Case ini menggambarkan kejadian dimana Tim TPS dan Tim KPUD dapat melakukan <i>login</i> sebagai pengguna aplikasi.	Tim TPS dan Tim KPUD
Hak Akses	Use Case ini menggambarkan kejadian dimana Tim KPUD yang menentukan hak akses kepada Tim TPS yang dapat melakukan proses penyisipan.	Tim KPUD
Penyisipan	Use Case ini menggambarkan kejadian dimana Tim TPS dapat melakukan proses penyisipan pesan.	Tim TPS
Ekstrak	Use Case ini menggambarkan kejadian dimana Tim KPUD dapat melakukan proses ekstraksi pesan.	Tim KPUD
Laporan	Use Case ini menggambarkan kejadian dimana Tim KPUD dapat menampilkan data hasil ekstraksi kedalam bentuk laporan.	Tim KPUD
Bantuan	Use Case ini menggambarkan kejadian dimana Tim TPS dan Tim KPUD dapat melihat dan membaca petunjuk proses penyisipan dan ekstraksi pesan.	Tim TPS dan Tim KPUD
Tentang Kami	Use Case ini menggambarkan kejadian dimana Tim TPS dan Tim KPUD dapat melihat informasi tentang aplikasi dan pembuatnya.	Tim TPS dan Tim KPUD

3.1.3. Tahapan metode BPCS

Adapun tahapan dalam metode tersebut adalah sebagai berikut:

1. Proses Penyisipan Pesan

Adapun urutan langkah proses penyisipan antara lain:

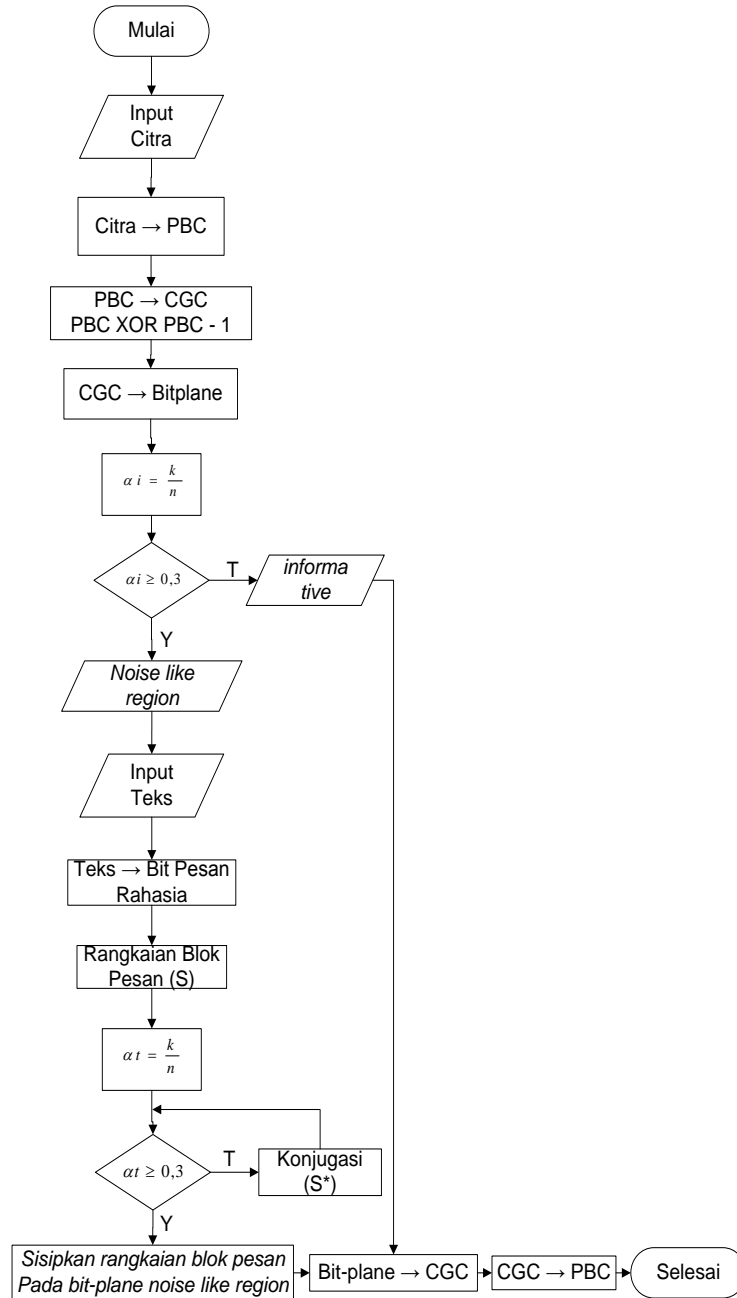
- a. *Cover image* dengan system *PBC* diubah menjadi system *CGC*, kemudian gambar tersebut di-*slice* menjadi *bit-plane* dalam bentuk gambar biner. Setiap *bit-plane* mewakili bit dari setiap piksel pada gambar.
- b. Segmentasi setiap *bit-plane* pada *cover image* menjadi *informative* dan *noise like region* dengan menggunakan nilai batas / *threshold* (α_0). Nilai umum dari $\alpha_0 = 0,3$.
- c. Kelompokkan *byte-byte* pesan rahasia menjadi rangkaian blok pesan rahasia.
- d. Jika blok (S) kurang kompleks dibandingkan dengan nilai batas, maka lakukan konjugasi terhadap S untuk mendapatkan S* yang lebih kompleks. Blok konjugasi (S*) pasti lebih kompleks dibandingkan dengan nilai batas.
- e. Sisipkan setiap blok pesan rahasia ke *bit-plane* yang merupakan *noise like region* (atau gantikan semua bit pada *noise like region*). Jika blok dikonjugasi, maka simpan data pada "*conjugation map*".
- f. Sisipkan juga *conjugation map* seperti yang dilakukan pada blok pesan rahasia.
- g. Ubah *stego-image* dari system *CGC* menjadi system *PBC*.

2. Proses Ekstraksi Pesan

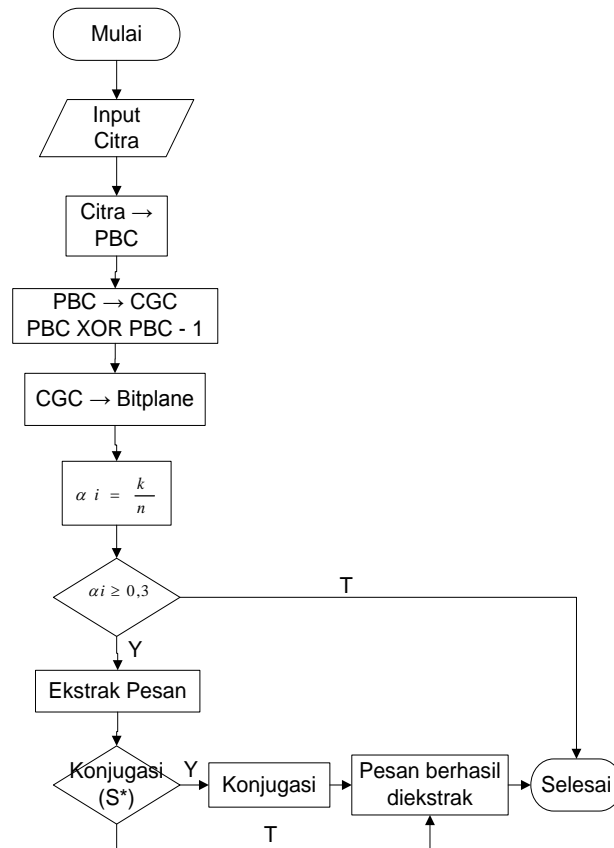
Proses Ekstraksi merupakan kebalikan dari langkah-langkah proses Penyisipan.

3.1.4. Flowchart Algoritma

Flowchart algoritma menjelaskan tentang alur urutan logika program dari tahapan metode *Bit-Plane Complexity Segmentation* yang dipakai penulis dalam pengembangan aplikasi. Adapun flowchart tersebut terdiri dari flowchart penyisipan dan ekstraksi pesan yang ditunjukkan pada Gambar 3 dan Gambar 4.



Gambar 3. Flowchart Proses Penyisipan Metode BPCS

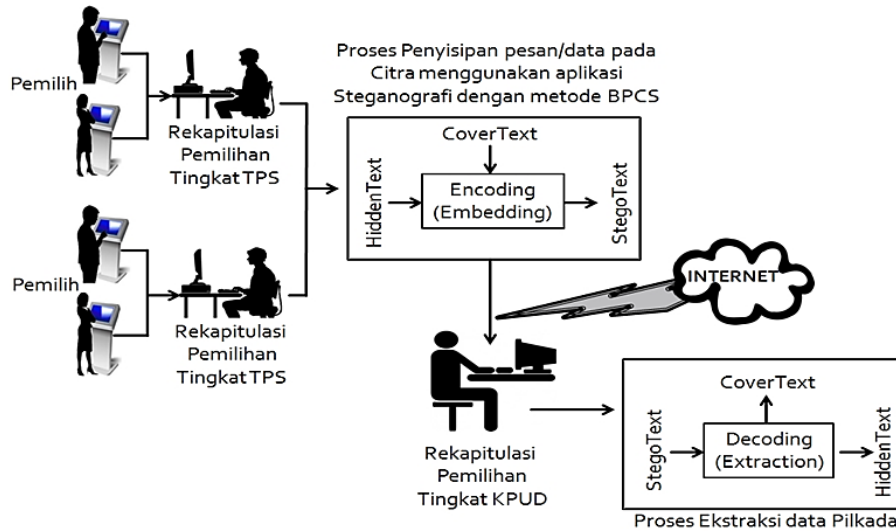


Gambar 4. Flowchart Proses Ekstraksi Metode BPCS

3.2. Arsitektur Aplikasi pada Simulasi Pilkada

Berdasarkan Gambar 5, tahapan proses Transformasi Data Pilkada dalam proses pengiriman Rekapitulasi hasil pemilihan adalah sebagai berikut:

1. Pemilih melakukan proses mencontreng / mencoblos dengan menggunakan komputer di tiap-tiap TPS.
2. Tim tingkat TPS yang telah diberi hak akses oleh Tim KPUD dapat melakukan tahap rekapitulasi hasil pemilihan dari tiap-tiap TPS kemudian mengirimkan data rekapitulasi hasil pemilihan tersebut langsung kepada Tim Rekapitulasi hasil pemilihan tingkat KPUD yang sebelumnya data tersebut disisipkan kedalam citra menggunakan aplikasi steganografi dengan metode BPCS sehingga data tersebut disebut *stegotext*.
3. Tim KPUD akan memvalidasi data *stegotext* tersebut dengan mengekstraknya menggunakan aplikasi steganografi, kemudian melakukan rekapitulasi data hasil pemilihan tersebut dan memasukkan data tersebut kedalam *database* yang kemudian akan ditampilkan kedalam bentuk laporan.



Gambar 5. Simulasi Transformasi Pilkada

3.3. Implementasi

3.3.1. Form Login

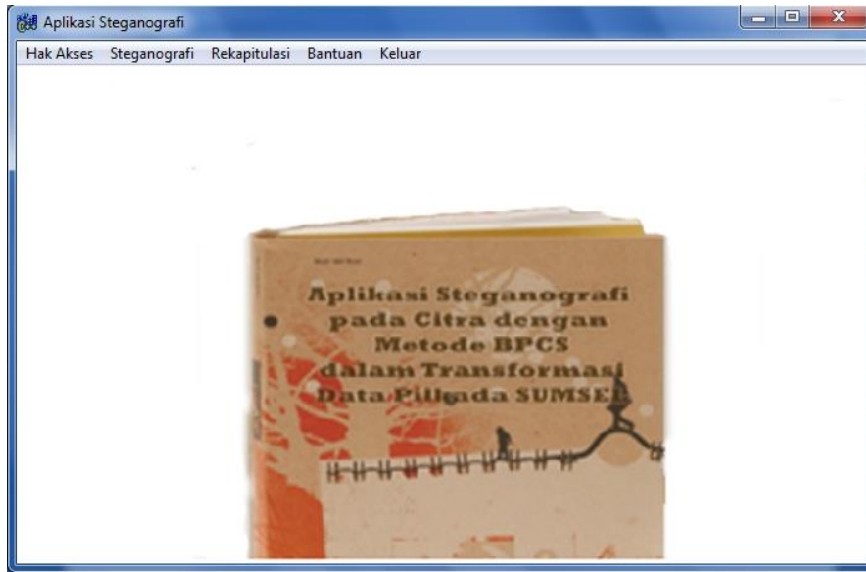
Ketika *user* pertama kali membuka aplikasi akan ditampilkan *form login*, dimana *user* terdiri dari dua tim yaitu Tim TPS dan Tim KPUD. Adapun *form login* tersebut ditunjukkan pada Gambar 6.



Gambar 6. Form Login

3.3.2. Form Menu Utama

Setelah *user* melakukan proses *login*, maka akan tampil *form* menu utama yang terdiri dari menu Hak Akses, menu Steganografi yaitu proses penyisipan dan ekstraksi, menu rekapitulasi yaitu Laporan, serta menu bantuan yaitu Petunjuk dan Tentang Kami yang dapat ditunjukkan pada Gambar 7.

Gambar 7. *Form Menu Utama*


3.3.3. *Form Proses Penyisipan*

Jika pengguna adalah Tim TPS, pengguna tersebut dapat melakukan proses penyisipan pesan dari menu steganografi pada menu utama. Proses Penyisipan dapat dilihat pada Gambar 8.

Gambar 8. *Form Proses Penyisipan*

3.3.4. *Form Hak Akses*

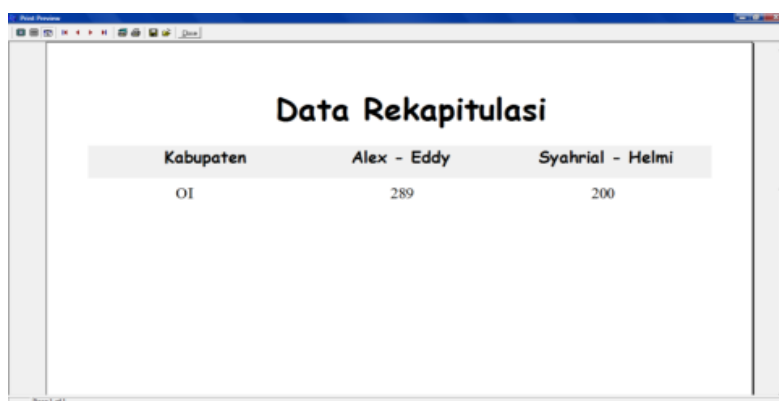
Jika pengguna adalah Tim KPUD, pengguna tersebut dapat memilih menu Hak Akses, melakukan proses ekstraksi pesan dari menu steganografi, dan dapat melihat laporan pada menu rekapitulasi. Tampilan *form* Hak Akses, Proses Ekstraksi dan laporan dapat dilihat pada Gambar 9, Gambar 10 dan Gambar 11.



Gambar 9. Form Hak Akses



Gambar 10. Form Proses Ekstraksi

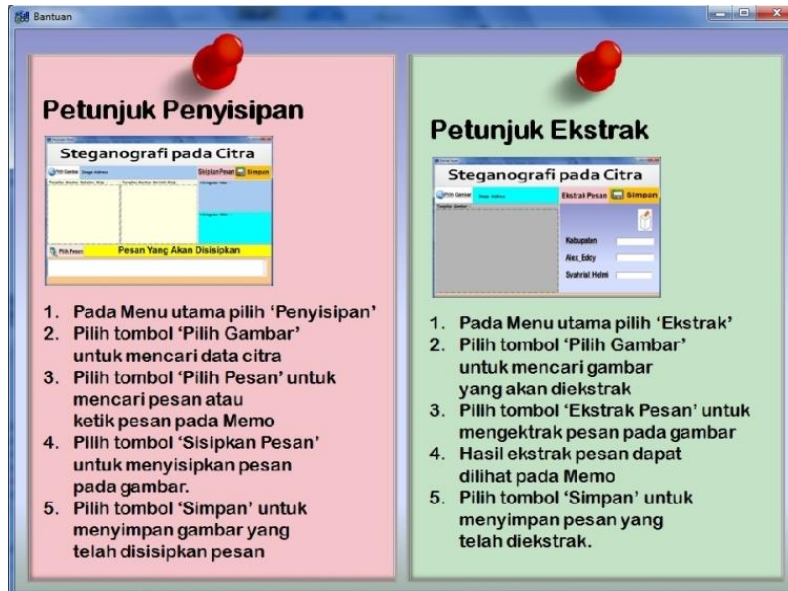


Kabupaten	Alex - Eddy	Syahrial - Helmi
OI	289	200

Gambar 11. Form Laporan

3.3.5. Form Petunjuk

Untuk seluruh pengguna dapat memilih menu Bantuan dari menu utama yang terdiri dari *form* Petunjuk mengenai proses penyisipan dan ekstraksi pesan. Tampilan *form* Petunjuk dapat dilihat pada Gambar 12.



Gambar 12. *Form* Petunjuk

4. KESIMPULAN

Dari keseluruhan sistem yang telah dibuat dan pengujian yang telah dilakukan dapat disimpulkan bahwa proses penggunaan aplikasi penyisipan teks kedalam gambar sangat baik untuk keamanan data, karena:

1. Aplikasi transformasi Data pilkada yang dikembangkan dapat meminimalisasikan permasalahan dalam pengiriman data jumlah suara pilkada. Hal tersebut terbukti ketika tampilan gambar sebelum dan sesudah penyisipan teks tidak berubah tergantung dari kualitas *cover object* jika dilihat dengan indera mata karena steganografi menggunakan gambar berdasarkan persepsi manusia.
2. Penggunaan metode steganografi, khususnya dengan teknik BPCS dapat menjaga kerahasiaan data saat dilakukan transformasi data. Hal ini ditunjukkan dengan pemanfaatan gambar sebagai media yang digunakan dalam penyisipan data sangat kecil kemungkinannya untuk disadap.

5. SARAN

Saran yang dapat direkomendasikan oleh penulis yang dapat berguna untuk pengembangan aplikasi ini adalah:

1. Perlunya pengembangan sistem, tidak hanya *file text* (.txt) yang dapat disembunyikan pada citra melainkan semua file (*.All files).
2. Menggunakan metode steganografi lain yang lebih baik dari BPCS dalam hal penyembunyian data pada gambar.
3. Mengkombinasikan metode BPCS dengan metode lain sehingga dapat meningkatkan keamanan data yang lebih baik.

DAFTAR PUSTAKA

- [1] Petrus, J., Yuwono, B., 2010, Perancangan Infrastruktur SI/TI untuk Pelaksanaan PILKADA Kota Palembang, *Information Systems: Bridging Gap Between Theories and Practices, Prosiding KNSI*, Palembang, 22-23 Januari 2010.
 - [2] Munir, R., 2004, *Pengolahan Citra Digital dengan Pendekatan Algoritmik*, Informatika, Bandung.
 - [3] Anggraini, Utami, E., 2007, Analisis Penyisipan Data pada Citra Bitmap menggunakan Metode Bit Plane Complexity Segmentation, <http://p3m.amikom.ac.id/detail.php?id=62&Analisis-Penyisipan-Data-Pada-Citra-Bitmap-Menggunakan-Metode-Bit-Plane-Complexity-Segmentation>, Diakses tanggal 17 Februari 2011.
 - [4] Widyanarko, A., 2008, Implementasi Steganografi dengan Metode Bit-Plane Complexity Segmentation (BPCS) untuk Dokumen Citra Terkompresi, http://www.informatika.org/~rinaldi/TA/Makalah_TA%20Arya_Widyanarko.pdf, Diakses tanggal 17 Februari 2011.
-