Implementasi Steganografi Citra Digital Pemberkasan Arsip Menggunakan Metode Least Significant Bit

Studi Kasus: PT. Angkasa Pura I (Persero) Bandar Udara Internasioanal Juanda Surabaya

Yanuar Nurdiansyah., Ayu Lusia Fitrasari Riftana
Sistem Informasi, Program Studi Sistem Informasi, Universitas Jember (UNEJ)
Jl. Kalimantan 37, Jember 68121
Yanuar_pssi@unej.ac.id

***Abstrak*—Implementasi steganografi citra digital pada pemberkasan arsip menggunakan metode Least Significant Bit (LSB) (Studi kasus: PT. Angkasa Pura I (Persero) Cabang Bandar Udara Internasioanal Juanda Surabaya) merupakan sistem yang bertujuan untuk memberikan keamanan data pemberkasan arsip. Metode Least Significant Bit (LSB) digunakan untuk menyembunyikan informasi rahasia dari data arsip dengan cara menyisipkan informasi pada media citra. Penyisipan informasi dengan mensubtitusi bit akhir dari informasi dengan bit media citra. Informasi yang sisipkan sebelumnya dienkripsi terlebih dahulu menggunakan Algoritma Twofish untuk antisipasi saat informasi yang disisipkan terekstrak oleh pihak tidak berwanang. Metode LSB dipilih karena ukuran informasi yang disisipkan pada metode LSB tidak merubah media aslinya sehingga metode ini dapat menampung informasi yang tersembunyi tanpa menimbulkan kecurigaan. Sistem pemberkasan arsip yang dibangun berbasis website agar dapat digunakan dengan mudah oleh pengguna. Pembuatan sistem ini dibangun mengadopsi dari model protoyipe. Sistem pemberkasan arsip dirancang dan dibangun dengan 2 (dua) hak akses, yaitu admin, dan sekretaris dengan berbagai fitur yang dapat memudahkan penggunanya. Hasil dari penelitian ini, sistem mampu mengimplementasikan metode LSB untuk memberi keamanan pada data arsip rahasia.**

Kata kunci— Arsip, Steganografi, Least Significant Bit

I. PENDAHULUAN

PT. Angkasa Pura I merupakan salah satu perusahaan Badan Usaha Milik Negara (BUMN) yang bergerak pada bidang jasa pengelolaan dan pelayanan penerbangan. Perusahaan berdasar jasa transportasi udara ini telah subur tumbuh dan berkembang di Indonesia. Perusahaan ini membawahi 13 bandara berbasis Internasional, hal ini semakin memantapkan posisinya dalam memberikan pelayanan. PT. Angkasa Pura I sebagai perusahaan komersil kebandaraan memiliki tujuan untuk memberikan pelayanan terbaik, keselamatan dan pelayanan bertaraf internasional.

Bandar Udara Internasional Juanda merupakan salah satu bandar udara yang berada dibawah pengelolaan PT. Angkasa Pura I. Bandar Udara Internasioanal Juanda sendiri memiliki dua terminal yaitu Terminal 1 (T1) yang melayani penerbangan *domestic*, umroh, dan haji sedangkan Terminal 2 (T2) yang melayani penerbangan *domestic* dan internasional. PT. Angkasa Pura I Bandar Udara Internasional Juanda juga memiliki sebuah kantor yang menangani kegiatan yang ada di bandar udara dan kegiatan administratif perusahaan.

PT. Angkasa Pura I mempunyai tujuan untuk pengoptimalan sumber daya untuk memberikan pelayanan yang bermutu dan meningkatkan nilai perusahaan, serta tingkat kepercayaan masyarakat. Selain meningkatkan nilai tambah yang optimal bagi masyarakat dan lingkungan, perusahaan juga mimilki tujuan untuk meningkat kualitas agar dapat berdaya saing baik dengan perusahaan domestik ataupun Internasional.

Hal yang dibutuhkan untuk mewujudkan tujuan perusahaan PT. Angkasa Pura I adalah adanya data pendukung terkait kegiatan dari setiap bagian (*departement*) pada PT. Angkasa Pura I. Tujuan kegiatan pada setiap bagian (*departement*) dapat berlanjut dengan adanya aktivitas pokok dan aktivitas penunjang. Aktivitas pokok yaitu aktivitas yang secara langsung, sedangkan aktivitas penunjang yaitu menunjang aktivitas pokok meliputi kegiatan tata usaha dan administratif.

Kegiatan Tata Usaha merupakan kegiatan yang berhubungan dengan warkat, surat-surat, dan dokumen atau sering disebut arsip. Arsip ini sangat berperan penting bagi sebuah organisasi atau perusahaan karena merupakan pusat atau sumber informasi. Dokumen dalam arsip berperan terhadap perencanaan, penganalisisan, perumusan kebijaksanaan, pengambilan keputusan, pembuatan laporan, penilaian, pengendalian dan pelaksanaan pertanggungjawaban secara tepat. Sehingga informasi arsip memiliki hak akses terbatas kerena menyimpan rahasia informasi perusahaan.

Informasi tersebut dihimpun secara sistematis dan logis sesuai konteks sehingga menjadi satu koteks yang memiliki hubungan informasi atau biasa disebut pemberkasan arsip. Pemberkasan arsip harus secara benar dan aman agar informasi penting atau rahasia milik perusahaan tidak disalah gunakan oleh pihak yang tak bertanggung jawab. Semakin majunya teknologi dan perkembangan sistem informasi, juga memepengaruhi keamanan sebuah data. Banyaknya peretas yang akan mencoba utuk mendapatkan informasi secara illegal. Selain itu ancaman juga datang dari pihak dalam atau pekerja dalam organisasi tersebut. Pengamanan data pada pemberkasan arsip untuk menjaga informasi penting atau rahasia, dari ancaman luar atau dalam organisasi itu sendiri. Sehingga

pemberkasan arsip pada PT. Angkasa Pura I dapat menerapkan steganografi.

Steganografi merupakan salah satu pengamanan data guna menyamarkan atau menyembunyikan sebuah informasi rahasia. Penerapan steganografi pada pemberkasan arsip dengan memanfaatkan media citra sebagai tempat penyisipannya. Dengan menggunakan media citra akan menghilangkan kecurigaan bahwa tersimpan pesan rahasia di dalamnya. Informasi yang disisipkan di dalam media citra tersebut tidak akan terlihat dengan kasat mata [1].

Banyak metode steganografi yang dapat digunakan untuk pengamanan informasi rahasia diantaranya yaitu metode *Least Significant Bit* (LSB). Metode LSB merupakan metode yang menyisipkan informasi rahasia bukan dengan menambah atau mengurangi melainkan mengganti bit terakhir pada media penyimpanan [2]. Ukuran informasi yang dimasukan pada metode LSB tidak merubah media aslinya sehingga metode ini dapat menampung informasi yang tersembunyi tanpa menimbulkan kecurigaan.

Pencegahan sebagai antisipasi ancaman yang mungkin terjadi terhadap informasi dalam gambar stego, maka informasi rahasia tersebut akan diubah sebelum disisipkan pada media. Pengubahan informasi yang akan disisipkan dilakukan dengan menggunakan kriptografi algoritma *twofish*. Algoritma *twofish* ini digunakan karena diantara algoritma enkripsi yang merupakan finalis dari *Advance Encryption Standard* (AES) pada tahun 1998 di Amerika yaitu *Rijndael*, *Serpent*, *Twofish*, *MARS*, dan *RC6*, algoritma *Twofish* dianggap sebagai algoritma yang memiliki tingkat keamanan yang tinggi.

Berdasarkan paparan di atas, dalam penelitian ini menggunakan steganografi dengan metode LSB pada pemberkasan arsip pada PT. Angkasa Pura I (Persero) Cabang Bandar Udara Internasioanal Juanda Surabaya, informasi yang akan disisipkan akan diubah terlebih dahulu menggunakan algoritma *twofish* [3].

Dari latar belakang masalah, tujuan yang ingin dicapai dan manfaat yang ingin diperoleh dalam penelitian ini.: (1) untuk merancang dan membangun sistem steganografi citra digital pada pemberkasan arsip menggunakan metode *Least Significant Bit* (LSB). dan (2) untuk mengetahui tingkat *security* dan *robustness* pada sistem.

II. METODE

A. Jenis Penelitian

Penelitian ini menggunakan pendekatan penegembangan (*development research*), dikarenakan penelitian ini bukan untuk membuat atau menguji kebenaran suatu teori maupun hipotesis, melainkan menghasilkan dan mengembangkan produk.

B. Pengumpulan Data

Tahap pengumpulan data dilakukan dengan cara mencari data yang dibutuhkan dalam mengimplementasikan metode LSB pada pemberkasan arsip. Pada tahap ini studi pustaka dan wawancara.

C. Tahapan Penelitian

Tahapan penelitian ini meliputi tahap pengumpulan data dan tahap analisis data. Penelitian dimulai dengan mencari studi literatur wawancara yang kemudian dilanjutkan ke analisis data untuk merumuskan analisis kebutuhan dari sistem. Setelah analisis kebutuhan terpenuhi, proses selanjutnya yaitu perancangan dan implementasi meliputi desain, *coding* kemudian *testing* aplikasi yang dibangun. Jika terjadi *error* maka akan dilakukan perbaikan sistem. Tahap terakhir yaitu penyusunan laporan.

D. Perancangan sistem

Tahapan penelitian pengembangan sistem mengadopsi dari model *prototype*. Model *prototype* merupakan model yang harus dievaluasi dan dimodifikasi kembali sesuai dengan kebutuhan pengguna, sehingga memungkinkan pengembangan untuk memahami kebutuhan pengguna [4]. Tahapan penelitian *prototype* meliputi tahap dengan perancangan secara cepat, perancangan prototype, evaluasi prototype, pengkodean, dan pengujian.

1) Perancangan Secara Cepat

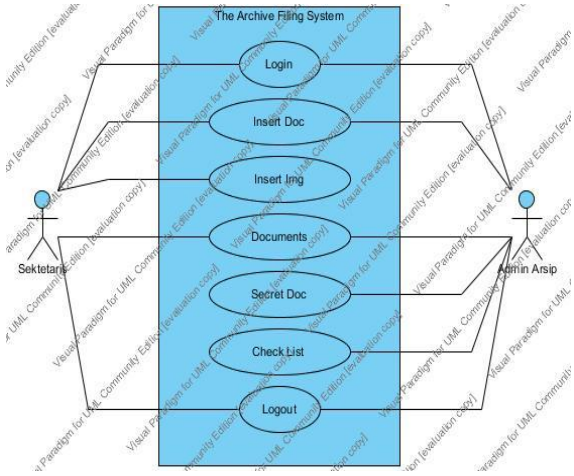
Pada tahap ini dilakukan analisis untuk mendapatkan kebutuhan sistem sesuai dengan keinginan pengguna. Analisis kebutuhan merupakan kegiatan menganalisa hasil informasi yang telah didapat untuk kemudian dikelompokan menjadi kebutuhan fungsional dan kebutuhan non-fungsional.

2) Perancangan Prototype

Tahap ini merupakan tahap perancangan prototipe dengan membuat perancangan sementara yang digunakan untuk penyajian pada pengguna. Perancangan sementara dibuat dengan membuat tampilan dari sistem. Tampilan yang dibuat berdasarkan hasil dari analisis kebutuhan yang telah didapatkan.

3) Evaluasi Prototype

Evaluasi digunakan untuk mengatahui prototipe yang sudah dibangun telah sesuai dengan keinginan pengguna. Tahap ini peneliti menggunakan menggunakan *Unified Modeling Language* (UML) yang dirancang menggunakan konsep *Object-Oriented Programming* (OOP). Berikut pemodelan UML yang akan digunakan antara lain: *Business Process*, *Usecase* Diagram dapat dilihat pada Gambar 1.



Gambar 1. Usecase Diagram

ISBN : XXXXXXXXXXX

4) Pengkodean

Tahap implementasi dari desain yang telah dibuat menjadi kode program. Hal yang dilakukan dalam implementasi antara lain: penulisan kode program (*coding*) menggunakan bahasa pemrograman *Page Hyper Text Pre-Processor* (PHP).dan manajemen basis data menggunakan MySQL.

5) Pengujian

Pengujian dilakukan terhadap perangkat lunak yang telah dibuat. Tujuan dari tahap ini adalah untuk mengetahui apakah sistem yang dibuat sudah sesuai dengan kebutuhan serta mencari kesalahan atau *bug*. Terdapat dua pengujian yang dilakukan, yaitu pengujian perangkat lunak meliputi ; *White Box Testing* dan *Black Box Testing* serta pengujian metode yang meliputi ; pengugujian visual, Pengujian *Peak Signal to Noise Ratio* (PSNR) dan pengujian *Robustness* [5] [6] [7].

III. HASIL DAN DISKUSI

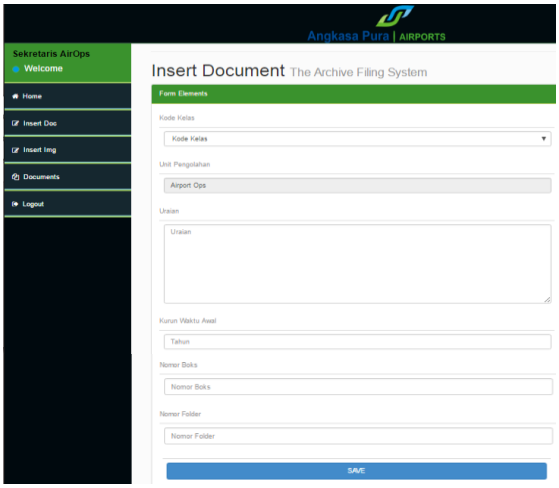
Hasil dan diskusi sistem selama dilakukannya penelitian yang mencakup setiap tahap implementasi dan pengujian sistem penilaian konsumen terhadap sistem pemberkasan arsip menggunakan metose LSB.

A. Hasil Pembuatan Sistem Steganografi Citra Digital Pada Pemberkasan Arsip Menggunakan Metode LSB

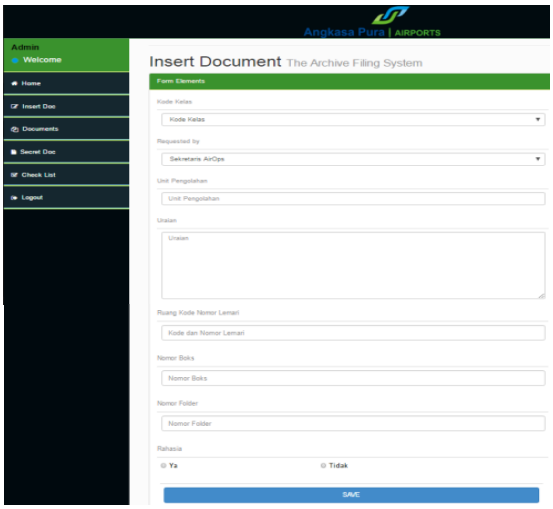
Tahap ini merupakan tahap pengkodean dari perancangan yang telah dibuat ke dalam bahasa pemrograman. Penelitian ini menggunakan bahasa PHP sebagai bahasa pemrograman. Tahap pengkodean akan menghasilkan beberapa *interface* atau tampilan dari sistem steganografi citra digital pada pemberkasan arsip yang dapat diakses oleh dua pengguna, yaitu admin dan sekretaris. Sistem ini memiliki beberapa fitur. Berikut fitur *Insert Doc*, *Insert Img*, dan *Secret Doc*.

1) Insert Doc

Fitur *insert doc* merupakan fitur untuk menambah data arsip baru. Fitur ini dapat diakses oleh dua pengguna admin dan sekretaris. Pada tampilan fitur terdapat perbedaan antara pengguna, tampilan admin lebih komplek karena dapat menambahkan data arsip rahasia, sedangkan sekretaris hanya dapat menambahkan data arsip yang tidak rahasia. Tampilan lebih lengkapnya dapat dilihat pada Gambar 2 dan Gambar 3.



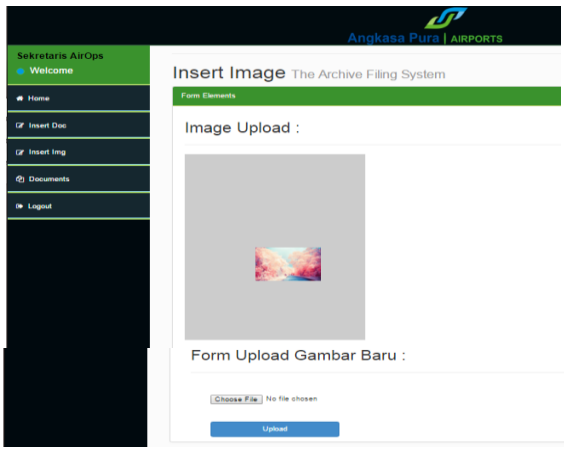
Gambar 2. Insert Doc Sekretaris



Gambar 3. *Insert Doc* Admin

2) Insert Img

Fitur *insert img* merupakan fitur untuk memasukan gambar baru, yang digunakan sebagai pengajuan arsip rahasia pada admin. Fitur ini diakses oleh sekretaris. Terdapat dua tombol, yaitu *Choose File* yang digunakan untuk memilih *file* yang akan dimasukan dan *Upload* yang digunakan untuk memasukan gambar dapat dilihat pada Gambar 4.

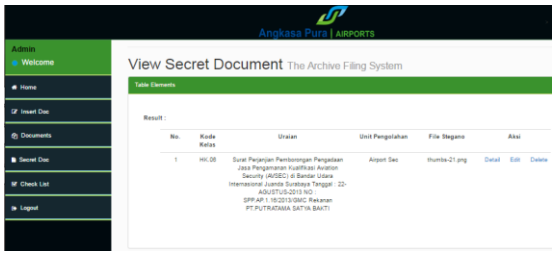


Gambar 4. Insert Img

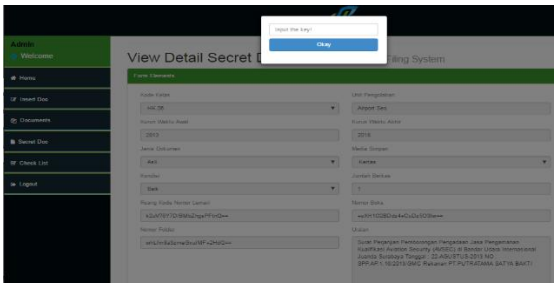
3) Secret Doc

Fitur *secret doc* merupakan fitur untuk mengelola data arsip rahasia yang telah dimasukan oleh admin berdasarkan pengajuan sekretaris. Fitur ini diakses oleh admin. Pada tampilan fitur ini terdapat tiga tombol, *Detail* digunakan untuk melihat rincian dari data arsip, *Edit* digunakan untuk mengubah data arsip, dan *Delete* digunakan untuk menghapus data, dimana akan muncul *popup* untuk melihat dan merubah data arsip rahasia Gambar 5, Gambar 6, dan Gambar 7.

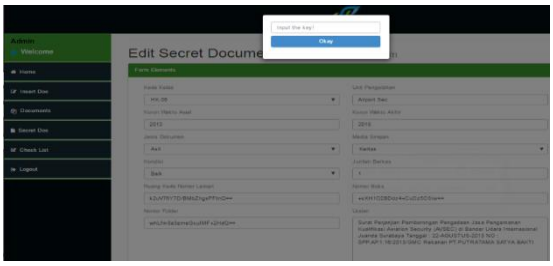
ISBN : XXXXXXXXXXX



Gambar 5. Secret Doc



Gambar 6. Detail Secret Doc



Gambar 7. Edit Secret Doc

B. *Implementasi Metode Least Significant Bit (LSB)*

Pada penelitian ini mengimplementasikan steganografi metode LSB. Steganografi metode LSB ini terdiri dari dua proses, yaitu *embedding* dan *extracting*. Berikut penjelasan mengenai implementasi metode yang digunakan.

1) Embedding

Proses *embedding* atau proses menyisipkan pesan pada gambar terdapat pada fungsi *submit()*. Pada bahasan ini akan dipaparkan bagaimana proses meyisipkan pesan rahasia pada gambar *cover*. Langkah awal dari proses ini yaitu membaca pesan rahasia dalam bentuk biner dengan s*yntax* "str_pad(decbin(ord($value), 7, '0', STR_PAD_LEFT)". Langkah ini dapat dilihat pada Gambar 8.

```
$message = str_split($message2);
foreach ($message as $key => $value) {
    $message[$key] = str_pad(decbin(ord($value)), 7, '0', STR_PAD_LEFT);
}
$message = implode($message);
```

Gambar 8. Kode Program Membaca Pesan Rahasia dalam Bentuk Biner

Langkah kedua yaitu mengubah gambar *cover* dalam bentuk biner. Gambar *cover* akan diambil pixelnya terlebih dahulu dengan urutan dari atas berjalan ke kanan, s*yntax* yang digunakan "getimagesize" dan "imagecreatetruecolor ($dimension[0], $dimension[1])" dan perulangan untuk mendapatkan urutan yang dibutuhkan. Hasil dari *pixel* gambar *cover* tersebut diubah pada bentuk biner, dengan s*yntax* "$pixel = imagecolorat($cover, $x, $y)" dan "$red = ($pixel >> 16) & 0xFF;". Langkah ini dapat dilihat pada Gambar 9.

```
$dimension = getimagesize($cover);
$cover = imagecreatefrompng($cover);
$stego = imagecreatetruecolor($dimension[0], $dimension[1]);
for ($y = 0; $y < $dimension[1]; $y++) {
    for ($x = 0; $x < $dimension[0]; $x++) {
        if (strlen($message) == 0) {
            $message = "0000000";
        }
        $pixel = imagecolorat($cover, $x, $y);
        $red = ($pixel >> 16) & 0xFF;
        $green = ($pixel >> 8) & 0xFF;
        $blue = $pixel & 0xFF;
```

Gambar 9. Kode Program Mengubah Pixel Menjadi Biner

Langkah selanjutnya yaitu memasukan pesan rahasia gambar *cover*. Pada langkah ini biner dari gambar akan disubtitusi dengan biner pesan rahasia dengan s*yntax* "$red = 2 * floor($red / 2) + substr($message, 0, 1);". Hasil dari subtitusi biner, diubah kembali dalam bentuk *pixel* untuk mengembalikan gambar, menjadi gambar stego dengan s*yntax* "imagecolorallocate" dan "imagesetpixel". Langkah ini dapat dilihat pada Gambar 10

```
switch ($this->color) {
    case "red":
        $red = 2 * floor($red / 2) + substr($message, 0, 1);
        break;
    case "green":
        $green = 2 * floor($green / 2) + substr($message, 0, 1);
        break;
    case "blue":
        $blue = 2 * floor($blue / 2) + substr($message, 0, 1);
        break;
}
$message = substr($message, 1);
$pixel = imagecolorallocate($stego, $red, $green, $blue);
imagesetpixel($stego, $x, $y, $pixel);
```

Gambar 10. Kode program subtitusi mengubah biner menjadi pixel

2) Extracting

Proses *extracting* atau proses mengembalikan pesan yang telah disisipkan dari gambar terdapat pada fungsi *dec()*. Pada bahasan ini akan dipaparkan bagaimana proses pengembalian pesan rahasia dari gambar stego. Langka pertama yaitu mengubah gambar stego dalam bentuk biner. Gambar stego akan diambil pixelnya terlebih dahulu dengan urutan dari atas berjalan ke kanan, s*yntax* yang digunakan "getimagesize" dan "imagecreatetruecolor($dimension[0], $dimension[1])" dan perulangan untuk mendapatkan urutan yang dibutuhkan. Hasil dari *pixel* gambar stego tersebut diubah pada bentuk biner, untuk mendapatkan biner dari pesan rahasia dengan s*yntax* "$pixel = imagecolorat($cover, $x, $y)", "$red = ($pixel >> 16) & 0xFF;", dan "$binary .= $pixel % 2;". Langkah ini dapat dilihat pada Gambar 11.

```
$dimension = getimagesize($stego);
$stego     = imagecreatefrompng($stego);
$binary    = "";
for($y = 0; $y < $dimension[1]; $y++)
{
    for($x = 0; $x < $dimension[0]; $x++)
    {
        $pixel = imagecolorat($stego, $x, $y);
        switch($this->color)
        {
            case "red":
                $pixel   = ($pixel >> 16) & 0xFF;
                $binary .= $pixel % 2;
                break;
            case "green":
                $pixel   = ($pixel >> 8) & 0xFF;
                $binary .= $pixel % 2;
                break;
            case "blue":
                $pixel   = $pixel & 0xFF;
                $binary .= $pixel % 2;
                break;
        }
    }
}
```

Gambar 11. Kode program mengambil biner pesan dari pixel gambar

Langkah selanjutnya yaitu mengubah kembali dalam bentuk *string* untuk mengembalikan pesan rahasia yang tersimpan pada gambar stego dengan perulangan dan s*yntax* "chr(bindec(substr($binary, $index, 7)))". Langkah ini dapat dilihat pada Gambar 12.

```
$message = "";
for($index = 0; $index < strlen($binary); $index += 7)
{
    $message .= chr(bindec(substr($binary, $index, 7)));
}
```

Gambar 12. Kode program Mengubah Biner Menjadi String

C. *Pengujian Metode*

Tahap ini merupakan tahap pengujian dari metode yang telah diimplementasikan pada sistem. Pengujian ini menggunakan gambar stego atau gambar hasil dari proses steganografi metode LSB.

1) Pengujian Visual

Pengujian visual merupakan pengujian dengan membandingkan antara citra *cover* dengan citra stego. Pengujian ini digunakan untuk melihat adanya perbedaan jika dilihat secara kasat mata. Pada Tabel 1 dapat dilihat bahwa secara kasat mata tidak ada perbedaan antara gambar cover dengan gambar stego.

TABEL 1. PENGUJIAN VISUAL

Gambar Cover	
Pesan Rahasia	k2uV76D/BMb2hgsPFtnQ==,whLfm8a2zme6xuIMF+2HdQ==,+vXH1O2BDdz4+CuDz5O3Iw==
Gambar Stego	

2) Pengujian PSNR

Pengujian PSNR digunakan untuk mengetahui kualitas dari gambar stego. Semakin tinggi nilai PSNR menunjukan semakin tinggi kualitas dari gambar stego dan semakin kecil kemungkinan dapat dipresepsi oleh panca indra Pada tahap ini dilakukan pengecekan nilai PSNR gambar stego dengan menggunakan *ImageMagick. ImageMagick* dapat diaplikasikan dengan cmd, dengan *query* "*magick compare –channel* (red/green/blue, sesuai channel yang digunakan) –metric PSNR filestego.png filecover.png diff.png". Pengujian PSNR dengan *ImageMagick* dapat dilihat pada gambar 13 dan hasil dari pengujian PSNR dapat dilihat pada tabel 2. Hasil dari PSNR dari gambar stego memiliki nilai diatas 40db yang berati gambar stego memiliki kualitas baik [3].

```
C:\xampp\htdocs\steg>magick compare -channel red -metric PSNR stego.png Sakura.p
ng diff.png
51.1693
C:\xampp\htdocs\steg>magick compare -channel red -metric PSNR stego.png stego.pn
g diff.png
1.#INF
```

Gambar 12. Pengujian PSNR dengan ImageMagick

TABEL 2. PENGUJIAN PSNR

Ukuran Gambar Cover	Hasil PSNR (db)
640 x 379	51.169

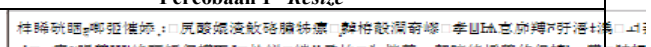
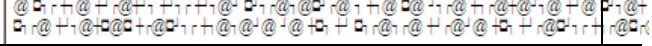
3) Pengujian Robustness

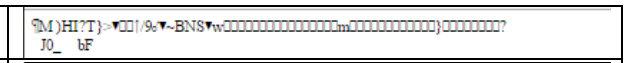
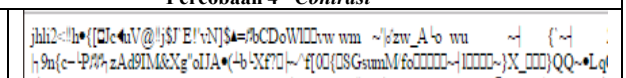
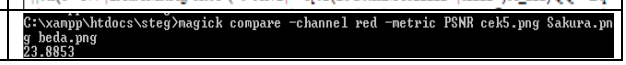
Pengujian *robustness* merupakan pengujian dengan melakukan *image processing* pada gambar stego. Pengujian ini untuk mengetahui ketahanan dari gambar stego. Pengujian *robustness* dapat dilihat pada tabel 3 dan.4. Hasil dari uji *robustness* menunjukan bahwa gambar stego yang telah dilakukan perubahan mengakibatkan pesan tidak dapat diektrak kembali.

TABEL 3. HASIL PENGUJIAN ROBUSTNESS

Gambar Stego	
Hasil Uji	k2uV76D/BMb2hgsPFtnQ==,whLfm8a2zme6xuIMF+2HdQ==,+vXH1O2BDdz4+CuDz5O3Iw==
Nilai PSNR	51.169
Percobaan 1 "*Resize*"	
Hasil Uji	-
Nilai PSNR	-
Percobaan 2 "*Rotation*"	
Hasil Uji	-
Nilai PSNR	-
Percobaan 3 "*Brightness*"	
Hasil Uji	-
Nilai PSNR	13.794
Percobaan 4 "*Contrast*"	
Hasil Uji	-
Nilai PSNR	23.885

TABEL 4. HASIL PENGUJIAN ROBUSTNESS

	Gambar Stego
Hasil Uji	k2uV76D/BMb2hgsPFtnQ==,whLfm8a2zme6xuIMF+2HdQ==,+vXH1O2BDdz4+CuDz5O3Iw==
Nilai PSNR	C:\xampp\htdocs\steg>magick compare -channel red -metric PSNR stego.png Sakura.png diff.png 51.1693
Percobaan 1 "*Resize*"	
Hasil Uji	
Nilai PSNR	C:\xampp\htdocs\steg>magick compare -channel red -metric PSNR cek1.png Sakura.png beda.png compare: image widths or heights differ 'cek1.png' @ error/compare.c/CompareImagesCommand/1150.
Percobaan 2 "*Rotation*"	
Hasil Uji	
Nilai PSNR	C:\xampp\htdocs\steg>magick compare -channel red -metric PSNR cek2.png Sakura.png beda.png compare: image widths or heights differ 'cek2.png' @ error/compare.c/CompareImagesCommand/1150.
Hasil Uji	
Nilai PSNR	C:\xampp\htdocs\steg>magick compare -channel red -metric PSNR cek4.png Sakura.png beda.png 13.7936
Percobaan 3 "*Brightness*"	

Hasil Uji	
Nilai PSNR	
Percobaan 4 "*Contrast*"	
Hasil Uji	
Nilai PSNR	

D. Hasil Pembahasan Sistem Pemberkasan Arsip Menggunakan Metode LSB

Pembahasan ini menjelaskan hasil pengamatan yang dilakukan mengenai sistem pemberkasan arsip telah dibangun. Berdasarkan pengamatan yang dilakukan, diperoleh hasil bahwa sistem pemberkasan arsip menggunakan metode LSB dapat membantu petugas arsip dalam melakukan pemberkasan arsip dan mejaga kerahasian serta keamanan informasi arsip.

Hasil analisa dari pengimplementasian steganografi metode LSB didapatkan kelebihan dan kekurangan sistem. Adapun kelebihan dan kekurangan dari sistem, yaitu:

1) Kelebihan Sistem

Dari hasil pembuatan sistem, peneliti dapat menganalisa kelebihan dari sistem yang dibuat, yaitu:

a. Pengguna harus melakukan *login* untuk menggunakan sistem. Hal ini dimaksudkan untuk keamanan data yang dimiliki oleh pengguna.
b. Sistem mampu menampilkan pesan ketika terjadi *error*. Hal ini memudahkan pengguna untuk mengetahui bahwa terjadi kesalahan pada saat menjalankan sistem.
c. Sistem mampu menampilkan pemberitahuan pada *user* admin, ketika ada pengajuan gambar baru. Hal ini dapat memudahkan *user* admin dalam memasukan dalam manajemen data.
d. Sistem menggunakan steganografi metode LSB dalam proses penyimpanan data. Hal ini dapat menjamin keamanan dan menghilangkan kecurigaan pesan rahasia yang disimpan.
e. Hasil gambar dari proses steganografi memiliki kualitas yang baik dan tidak terlihat perbedaan dengan gambar *cover* secara kasat mata.

2) Kelemahan Sistem

Dari hasil pembuatan sistem, penulis dapat menganalisa kekurangan dari sistem yang dibuat, yaitu hasil gambar dari proses steganografi tidak memiliki ketahan tehadap *imageprocessing*, karena pesan yang disisipkan tidak dapat diekstrak.

Berdasarkan dari kelemahan di atas, diperlukan pengembangan metode yang digunakan untuk mempertahankan gambar hasil stego yang telah dilakukan *imageprocessing*. Pengembangan dapat berupa penambahan fitur untuk mengekstrak gambar hasil steganografi berdasarkan *imageprocessing* yang dilakukan, salah satu contohnya *imageprocessing* rotasi 90^0. *Imageprocessing* rotasi 90^0 dapat diatasi dengan mengubah urutan pengambilan pixel yang awalnya dari pojok kiri atas berjalan ke kanan menjadi pojok kanan atas berjalan ke bawah saat akan diubah menjadi biner dan diambil pesan rahasianya pada proses ekstak dari metode.

IV. KESIMPULAN

Pengimplementasian steganografi metode LSB pada pemberkasan arsip untuk menjamin keamanan dan menghilangkan kecurigaan pesan rahasia yang disimpan. Terdapat dua proses dalam pengimplementasian steganografi metode LSB, yaitu penyisipan pesan dan pengektrakan pesan. Proses penyisipan pesan diawali dengan *user* sekretaris memasukkan gambar pada sistem, langkah ini dilakukan untuk menyiapkan gambar *cover*. Langkah selanjutnya yaitu *user* admin memasukan *key* untuk proses enkripsi, dimana *chypertext* hasil enkripsi akan disisipkan pada gambar *cover* dengan proses steganografi metode LSB. Gambar hasil dari proses steganografi kemudian disimpan pada *database*. Proses pengektrakan pesan diawali dari gambar stego yang tersimpan pada *database* diektrak menjadi *chypertext*. Langkah selanjutnya *user* admin memasukan *key* untuk dekripsi, dimana *plaintext* hasil dekripsi akan ditampilkan.

Gambar hasil dari proses steganografi metode LSB tidak memiliki ketahan tehadap *imageprocessing*. Gambar stego yang melalui tindakan (*resize*, *rotation*, *brightness*, *contrast*) tidak dapat mengembalikan pesan rahasia yang telah disisipkan didalamnya. Gambar stego yang telah melalui *imageprocessing* dengan tindakan *resize*, *rotation*, dan *brightness* tergolong gambar dapat tidak digunakan karena nilai PSNR dihasilkan dibawah 20 db, sedangkan gambar stego yang telah melalui *imageprocessing* dengan tindakan *contrast* tergolong tidak baik karena nilai PSNR diatas 20 db.

DAFTAR PUSTAKA

[1] Ariyus, D., 2006. *Kriptografi: Keamanan Data dan Komunikasi*. Yogyakarta: Graha Ilmu.

[2] Ardhyana, d., 2008. Aplikasi Steganografi Pada Mp3 Menggunakan Teknik LSB.

[3] Randi, A., 2012. Studi Perbandingan Algoritma Blowfish dan Twofish.

[4] Pressman, R.S., 2012. *Rekayasa Perangkat Lunak*. Yogyakarta: Andi.

[5] Cheddad A, C.J.d., 2010. Digital Image Steganography: Survey and Analysis of Current Methods.

[6] Krisnawati, 2008. Metode Least Significant Bit (LSB) dan End Of File (EOF) Untuk Menyisipkan Teks Ke Dalam Citra Grayscale.

[7] Saefullah, A.d., 2012. Aplikasi Steganografi untuk Menyembunyikan Teks dalam Media Image dengan Metode LSB.

.