ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

PENGEMBANGAN PERANGKAT LUNAK PENYEMBUNYIAN PESAN TERENKRIPSI MENGGUNAKAN ALGORITMA MARS PADA CITRA DIGITAL DENGAN METODE ADAPTIF

Dewi Sartika[1)]

[1)] *Program Studi Informatika Universitas Indo Global Mandiri*
Jl. Jend. Sudirman No. 629 KM.4 Palembang Kode Pos 30129
Email : dewiq.ifa@gmail.com[1)]

ABSTRACT

Steganography and cryptography are security method of secret message from third party who curious to see it. Steganography secures the message by hiding it on digital media. While for cryptography, it secures the message by coding it so the message will be understandable only by the message sender and the receiver. In this research, the secret text message shall be encrypted first by using MARS cryptography algorithm, then it'll be embedded on bitmap extended grayscale image digital media with adaptive steganography method. Adaptive steganography method consisted of three phases: capacity assessment, minimum error replacement (MER) and false contouring. While MARS cryptography algorithm also has three phases: forward mixing, cryptographic core and backward mixing. After being implemented into the program, the resulted stego-images were assessed subjectively by sharing questionnaires, where out of 33 respondents 72% said that before and after embedded, the images don't have any differences from its brightness, 48% from its noise, and 67% couldn't choose which one stego-image is. The objective assessment was done by calculating the value of Root Mean Square Error (RMSE) and Peak Signal to Noise Rational (PSNR), where out of 8 tested stego-images had low RMSE and the PSNR were above 30dB. From both assessment, it's concluded that the resulted stego-images had good quality (no changement significantly).

Keywords : *Cryptography, Steganography, MARS algorithm, adaptive method*

1. Pendahuluan

A. Latar Belakang

Steganografi merupakan teknik menjaga kerahasiaan pesan yang sudah digunakan sejak berabad-abad yang lalu. Steganografi adalah ilmu dan seni menyembunyi-kan pesan rahasia didalam suatu media sehingga keberadaan pesan tidak diketahui oleh orang lain. Steganografi merupakan salah satu teknik yang digunakan dalam menjaga suatu pesan rahasia dengan cara menyembunyikannya pada suatu media penampung. Steganografi membutuhkan dua properti yaitu media penampung dan pesan rahasia. Media penampung yang umum digunakan adalah gambar, suara, video, atau teks. Pesan yang disembunyikan dapat berupa artikel, gambar, daftar barang, kode program atau pesan lain.

Steganografi pada citra digital dibedakan menjadi dua jenis berdasarkan cara penyisipan pesan, yaitu *spatial-domain* dan *frequency-domain*. *Spatial-domain* merupakan teknik steganografi yang menyisipan pesan secara langsung pada intensitas setiap piksel citra digital. Sedangkan *frequency-domain* merupakan teknik steganografi yang menyisipkan pesan pada koefisien dari hasil transformasi intensitas setiap *pixel* citra digital ke *frequency-domain* tertentu.

Metode adaptif termasuk dalam teknik steganografi *spatial-domain*. Metode ini mengoptimalkan penggunaan ruang pada citra digital untuk penyisipan pesan serta mengkorelasikan modifikasi yang dilakukan pada setiap *pixel* citra digital. Kelebihan dari metode ini adalah mampu menanggulangi perubahan kualitas citra digital yang signifikan setelah dilakukan penyisipan pesan. Kanal warna pada *pixel* citra digital yang digunakan untuk penyisipan akan dipilih secara acak untuk mempersulit steganalisis mengekstraksi pesan rahasia

Kriptografi adalah seni dan ilmu untuk menjaga keamanan pesan (Schneier 1996). Sebelum disisipkan pada media citra digital, pesan yang akan dikirimkan terlebih dahulu dienkripsi menggunakan algoritma kriptografi kunci simetri yaitu algoritma *chiper* blok MARS. Pengenkripsian pesan sebelum disisipkan pada citra digital diharapkan mempersulit steganalisis, walaupun pesan berhasil diekstraksi.

Sebagai pertimbangan dalam penelitian ini akan dicantumkan penelitian terdahulu yang dilakukan oleh peneliti lain. Y.K.Lee dan L.H.Chen pada tahun 1999 melakukan penelitian yang berjudul *High Capacity Image Steganographic model* dapat disimpulkan bahwa penelitian ini memiliki tujuan untuk memaksimalkan ruang penyisipan menggunakan teknik penyisipan LSB dengan tetap memperhatikan kualitas *stego-image* yang dihasilkan dengan menggunakan tiga tahapan yaitu memaksimalkan kapasitas, memperkecil kesalahan penyisipan dan mengurangi *false contours* (Lee & Chen 2000). Manoj Kumar Meena dkk pada tahun 2011 melakukan penelitian yang berjudul *Image Steganography tool with Adaptive Encoding Approach to maximize Image hiding capacity* dapat disimpulkan bahwa sebelum melakukan penyisipan pesan, dilakukan pengitungan bit yang dapat disisipi pada *pixel* citra. Kemudian dilakukan perubahan hasil penyisipan untuk

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

mengurangi *embedding error* dengan menggunakan *minimum –error replacement* (MER). Terakhir dilakukan penghilangan *false contouring* menggunakan *improved Grey-Scale Compensation* (IGSC) (Meena et al. 2011).

B. Rumusan Masalah

Berdasarkan uraian pada latar belakang, maka permasalahan yang dapat diangkat dalam penelitian ini adalah kecurigaan orang lain terhadap *stego-image* akibat perubahan kualitas citra digital yang signifikan dan mudahnya steganalisis membaca pesan rahasia setelah berhasil diekstraksi

2. Landasan Teori

A. Metode Steganografi Adaptif

Steganografi sudah dikenal oleh bangsa Yunani sejak lama, Penguasa Yunani dahulu mengirimkan pesan rahasia melalui kepala budak atau prajurit sebagai media, dengan menuliskan pesan pada kepala budak yang rambutnya dibotaki terlebih dahulu dan pesan dikirimkan apabila rambut telah tumbuh kembali.

Saat ini steganografi sudah banyak diimplementasikan pada media digital sebagai penampung, seperti citra digital, video dan audio. Pesan yang disembunyikan pun berbentuk digital seperti teks, citra data, audio dan video.

Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia di dalam pesan lain sehingga keberadaan pesan rahasia tersebut tidak dapat diketahui. Steganografi membutuhkan dua properti yaitu media penampung dan pesan rahasia (Munir 2006). Keuntungan yang diperoleh menggunakan steganografi adalah pesan tersebut tidak menarik perhatian sehingga tidak menimbulkan kecurigaan bagi pihak ketiga.

Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah :

1. *Fidelity*. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Orang lain tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
2. *Robustness*. Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung. Seperti pengubahan kontras, rotasi, pemotongan, perbesaran gambar, pemampatan dan sebagainya.
3. *Recovery*. Data yang disembunyikan harus dapat diungkapkan kembali. Tujuan dari steganografi adalah *data hiding*, maka sewaktu-waktu data rahasia dalam citra penampung harus dapat diambil kembali.

Metode adaptif termasuk ke dalam metode *spatial-domain*. Metode adaptif merupakan metode yang mengoptimalkan penggunaan ruang pada gambar untuk penyisipan pesan dan mengkorelasikan modifikasi yang dilakukan pada setiap *pixel* gambar (Meena et al. 2011). Metode adaptif terdiri dari 3 tahapan yaitu :

1. CE (*Capacity Evaluation*)

Tahapan ini merupakan tahapan pertama yang dilakukan pada steganografi adaptif. Tahapan ini bertujuan untuk menentukan kapasitas maksimum *Least Significant Bit* (LSB) dari masing-masing pixel *cover-image*. Asumsikan bahwa *grayscale* dari satu *pixel* P pada koordinat (x,y) yang akan dianalisis, dinotasikan f(x,y). Pada gambar 1 dapat dilihat delapan *pixel* tetangga dari *pixel* P yang akan digunakan dalam perhitungan kapasitas penyisipan yang dapat dilakukan pada *pixel* P tersebut :

B (x-1,y-1)	C (x-1,y)	D (x-1,y+1)
A (x,y-1)	P (x,y)	E (x,y+1)
H (x+1,y-1)	G (x+1,y)	F (x+1,y+1)

Gambar 1. *Delapan pixel tetangga*

Nilai dari *pixel* P akan diubah berdasarkan kapasitas penyisipan, dimana bergantung pada nilai variasi keabuan dari tetangga atas dan kiri dari *pixel* P. Sehingga dapat dihitung dengan persamaan berikut ini :

$$Max(x,y) = \max\{f(x-1,y-1), f(x-1,y), f(x-1,y+1), f(x,y1)\}$$
$$Min(x,y) = \min\{f(x-1,y-1), f(x-1,y), f(x-1,y+1), f(x,y-1)\}$$
$$D(x,y) = Max(x,y) - Min(x,y)$$

penyisipan Kn(x,y) dari setiap *pixel* (x,y) didefinisikan sebagai :

$$Kn(x,y) = [\ Log_2 D(x,y)]$$

$$U(x,y) = \begin{cases} 4, \text{ jika } f(x,y) \le t \text{ ,dimana } t = 191 \\ 5, \text{ selainnya} \end{cases}$$

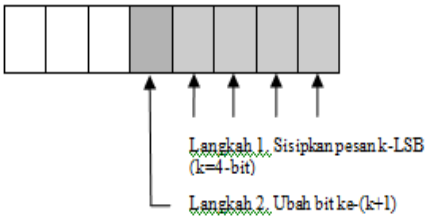
$$K(x,y) = \min\{\max\{Kn(x,y),4\},U(x,y)\}$$

Dimana :
Min(x,y) : nilai intensitas keabuan terkecil
Max(x,y) : nilai intensitas keabuan terbesar
D(x,y) : selisih nilai variasi keabuan
Kn(x,y) : kapasitas penyisipan tiap pixel dari cover-image
U(x,y) : batas kapasitas penyisipan
K(x,y) : kapasitas penyisipan

2. MER (*Minimum Error Replacement*).

MER digunakan untuk memperkecil tingkat kesalahan saat penyisipan. Langkah yang dilakukan adalah dengan mengevaluasi nilai dari setiap *pixel* yang telah disisipi dengan metode LSB, dengan mengubah nilai tersebut dari 1 menjadi 0. Langkah tersebut dapat dilihat pada gambar dibawah ini :

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786



Gambar 2. *Langkah MER*

Jika, f(x,y) adalah *pixel* asli, g(x,y) adalah *pixel* setelah disisipi k-LSB dan g'(x,y) adalah *pixel* yang bit ke-(k+1) telah diubah dari g(x,y), dan e(x,y) menyatakan *error* antara f(x,y) dan g(x,y) sedangkan e'(x,y) menyatakan *error* antara f(x,y) dan g'(x,y), maka jika e(x,y) lebih kecil dari e'(x,y) maka g(x,y) digunakan untuk menggantikan f(x,y), selainnya g'(x,y) yang akan menggantikan f(x,y).

3. IGSC (*Improved Grayscale Compensation*).

IGSC digunakan untuk mengurangi *false contouring* (jika terjadi kesalahan). Pada IGSC, *error embedding* biasanya disebarkan pada *pixel* tetangga bagian kanan dan bawah *pixel*. Jadi, keempat pixel tetangga tersebut dimodifikasi dengan persamaan berikut :

$$f(x, y + 1) = f(x, y + 1) + \tfrac{1}{4}\, e(x, y),$$
$$f(x + 1, y - 1) = f(x + 1, y - 1) + \tfrac{1}{4}\, e(x, y),$$
$$f(x + 1, y) = f(x + 1, y) + \tfrac{1}{4}\, e(x, y),$$
$$f(x + 1, y + 1) = f(x + 1, y + 1) + \tfrac{1}{4}\, e(x, y).$$

B. Algoritma Kriptografi MARS

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Tujuan dari kriptografi atau disebut juga aspek- aspek keamanan sebagai berikut :

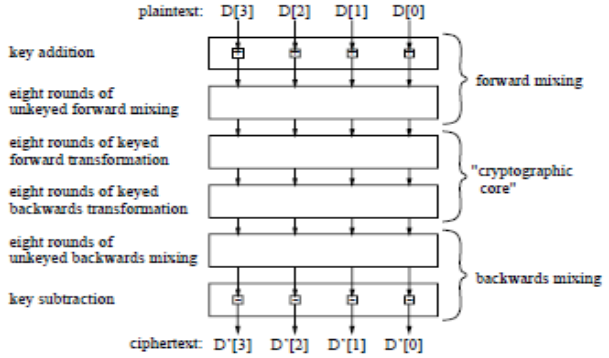
1. Kerahasiaan (*confidentiality*), adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data (*data integrity*), adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi (*authentication*), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi maupun mengidentifikasi kebenaran sumber pesan.

Nirpenyangkalan (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

MARS merupakan salah satu algoritma kriptografi *chiper* blok, dengan ukuran blok 128 bit dan ukuran kunci yang bervariasi dari 128 bit sampai 400 bit (Burwick et al. 1998). Notasi yang digunakan dalam *chiper* adalah :

- D[ ] adalah suatu array dari 4 32 bit data word. Array ini berisikan *plaintext* dan pada akhir proses enkripsi berisikan *chipertext*.
- K[ ] adalah array untuk *expended key*, terdiri dari 40 32 bit.
- S[ ] adalah array yang berisikan *S-box*, terdiri dari 512 bit word.

Struktur umum dari *chiper* blok MARS terdiri dari 3 tahapan (Halevi 2015) yang dapat dilihat pada gambar :



Gambar 3. *Struktur chiper blok MARS*

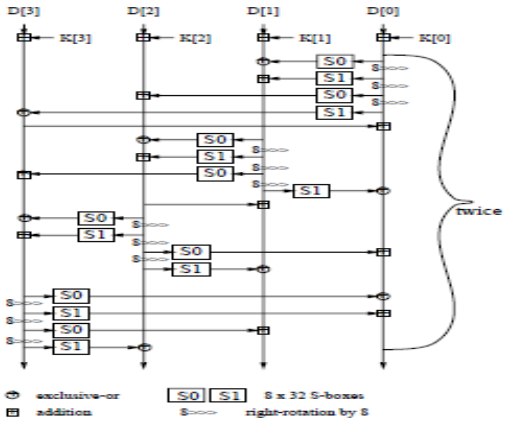
1. Forward mixing

Pertama-tama sub kunci ditambahkan pada setiap word data dari *plaintext*, kemudian dilakukan delapan iterasi mixing tipe-3 *feistel network* yang dikombinasikan dengan operasi *mixing* tambahan. Setiap iterasi digunakan sebuah word data (*source word*) untuk memodifikasi tiga word data (*target word*).

Keempat byte dari *source word* dinotasikan dengan b0, b1, b2, b3 (dimana b0 adalah byte terendah dan b3 adalah byte tertinggi) dan digunakan untuk index *S-box*, dimana b0 dan b2 untuk index S0 sedangkan b1 dan b3 untuk index S1. Pertama S0[b0] di XOR-kan dengan *target word* pertama, kemudian S1[b1] ditambahkan dengan *target word* pertama. S0[b2] ditambahkan dengan *target word* kedua dan S1[b3] di XOR-kan dengan *target word* ketiga. Terakhir *source word* dirotasikan sebanyak 24 posisi ke kanan.

Iterasi berikutnya keempat word data dirotasikan, sehingga *target word* pertama akan menjadi *source word* berikutnya, *target word* kedua menjadi *target word* pertama, *target word* ketiga jadi *target word* kedua, dan *source word* sebelumnya menjadi *target word* ketiga.

Pada iterasi pertama dan ke-lima, tambahkan *target word* ketiga dengan *source word* dan pada iterasi kedua dan ke-enam, tambahkan *target word* pertama dengan *source word*.



Gambar 4. *Struktur forward mixing*

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

2. Cryptographic core

Cryptographic core pada MARS menggunakan tipe-3 *feistel network* yang terdiri dari enam belas iterasi. Dalam setiap iterasi digunakan *E-function* (E untuk *expansion*) yang mengkombinasikan penjumlahan, perkalian, *data dependent rotation* dan *S-box look up*.fungsi ini menerima input satu word data dan menghasilakn tiga word data sebagai output. Setiap iterasi digunakan satu word data sebagai input *E-function* dan ketiga output word dari *E-function* ditambahkan atau di-XOR-kan ke ketiga word data yang lain. Kemudian source word dirotasikan 13 posisi ke kiri.

Delapan iterasi pertama, output pertama dan kedua dari *E-function* ditambahkan dengan *target word* pertama dan kedua, output ketiga di-XOR-kan dengan *target word* ketiga. Pada delapan iterasi terakhir, output pertama dan kedua dari *E-function* ditambahkan dengan *target word* ketiga dan kedua, output ketiga di-XOR-kan dengan *target word* pertama.

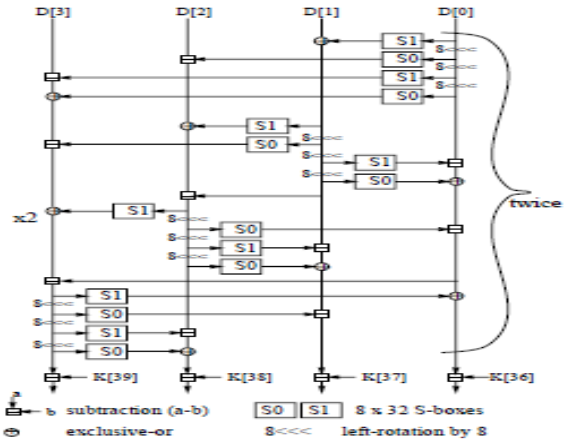
E-function

E-function menerima satu input word data dan menggunakan dua atau lebih sub kunci untuk menghasilkan output tiga word data (Burwick & Coppersmith. 1999). Fungsi ini menggunakan tiga variabel sementara L, M dan R (*left*, *middle* dan *right*). R berfungsi untuk menampung nilai *source word* yang dirotasikan 13 posisi ke kiri, M berfungsi untuk menampung nilai *source word* yang dijumlahkan dengan sub kunci pertama, dimana sembilan bit terendah dari M digunakan sebagai indeks untuk *S-box*. L berfungsi untuk menampung nilai yang sesuai dengan *S-box entry*. Sub kunci kedua dikalikan dengan R, kemudian R dirotasikan 5 posisi ke kiri. L di-XOR-kan dengan R, lima bit terendah dari R digunakan untuk nilai rotasi r (0-31), dan M dirotasikan ke kiri sebanyak r posisi. R dirotasikan sebanyak 5 posisi ke kiri dan di-XOR-kan dengan L. Terakhir, lima bit terendah dari R diambil sebagai nilai rotasi r dan L dirotasikan ke kiri sebanyak r posisi. Output word pertama dari *E-function* adalah L, kedua adalah M, dan ketiga adalah R.

3. Backward mixing

Tahap ini merupakan invers dari tahap *forward mixing*. Digunakan sebuah *source word* untuk memodifikasi tiga *target word*. Keempat byte dari *source word* dinotasikan dengan b0, b1, b2, b3 (dimana b0 adalah byte terendah dan b3 adalah byte tertinggi) dan digunakan sebagai indeks untuk *S-box*. S1[b0] di-XOR-kan dengan *target word* pertama, S0[b3] dikurangkan dengan *target word* kedua, S1[b2] dikurangkan dengan *target word* ketiga dan S0[b1] di-XOR-kan dengan *target word* ketiga. Terakhir *source word* dirotasikan 24 posisi ke kiri.

Setiap sebelum iterasi ke-empat dan ke-delapan, kurangkan *source word* dengan *target word* pertama dan setiap sebelum iterasi ketiga dan ke-tujuh, kurangkan *source word* dengan *target word* ketiga.



Gambar 5. *Struktur backward mixing*

Perluasan Kunci

Perluasan kunci berfungsi untuk membangkitkan sub kunci dari kunci yang diberikan yakni K[ ] terdiri dari n 32 bit dan diperluas menjadi 40 32 bit sub kunci K[ ]. Tahapan yang dilakukan pada perluasan kunci adalah :

1. Kunci disimpan pada variabel sementara T[ ] yang diset menjadi :
   T[0 . . n-1] = K[0 .. . n-1], T[n] = n, T[n+1 ...14] = 0

2. Kemudian diikuti dengan proses sebagai berikut :

a. Transformasikan T[ ] dengan persamaan linier sebagai berikut :
   Untuk i = 0 ...14,
   T[i] = T[i] $\oplus$ ((T[i-7mod 15] $\oplus$ T[i-2 mod 15]) <<< 3) $\oplus$ (4i+j)
   Dimana : j merupakan jumlah iterasi

b. Lakukan 4 iterasi tipe-1 *feistel network* sebagai berikut :
   Untuk i = 0 ... 14,
   T[i] = (T[i] + S[low 9 bits dari T[i-1 mod 15]]) <<<9

c. Ambil 10 word data dari T[ ] ke K[ ] :
   K[10j + 1] = T[4i mod 15], i = 0 ...9

3. Terakhir, nilai K5, K7 ... K35 diubah dengan ketentuan j digunakan untuk menampung dua bit terendah dari K[i], w menampung K[i] yang dua bit terendahnya diubah menjadi 1. Bit mask ke l akan diset menjadi 1 jika ml terdapat 10 bit 1 atau bit 0 yang berurutan. r digunakan untuk menyimpan lima bit terendah dari K[i-1], lalu B[ ] (tabel B[ ] = {0xa4a8d57b, 0x5b5d193b, 0xc8a8309b, 0x73f9a978}) dirotasikan sebanyak r posisi ke kiri yang hasilnya ditampung dalam p. Terakhir p di-XOR-kan dengan w dibawah kontol M dan disimpan di dalam K[i].

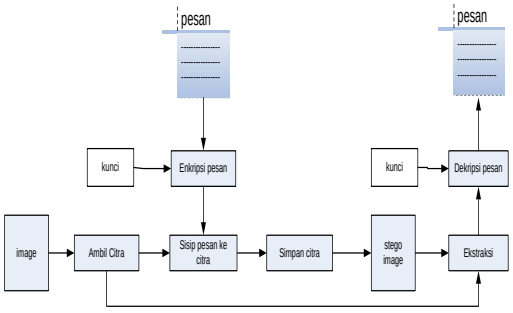
Algoritma MARS ini telah berhasil dipecahkan menggunakan salah satu jenis serangan yaitu *amplified boomerang attack* yang berbasis *differential cryptanalysis*. *Amplified boomerang attack* ini merupakan pengembangan dari *boomerang attack* yang diperkenalkan oleh David Wagner pada tahun 1999 dan *inside-out attack*. Namun, algoritma MARS yang dapat

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

diserang oleh *amplified boomerang attack* adalah algoritma MARS yang roundnya sudah dikurangi yaitu *full mixing* dengan 5 *core*, *full mixing* dengan 6 *core*, 6 *mixing* dengan 6 *core* dan 0 *mixing* dengan 11 *core* (Kelsey & Schneier 2000)

Implementasi

Pada tahapan implementasi dilakukan pengambilan *image grayscale* berekstensi .bmp beserta menuliskan pesan berupa *text* yang akan disisipkan, kemudian pesan rahasia tersebut akan dienkripsi menggunakan kunci. pesan yang telah terenkripsi akan disisipkan ke *image*, hasilnya berupa *stego-image*. *Stego-image* tersebut dapat disimpan guna didistribusikan untuk penyampaian pesan rahasia. Untuk mengetahui isi pesan rahasia didalam *stego-image*, maka *stego-image* akan diekstraksi pesan rahasia yang masih berupa *chipertext* yang akan didekripsi dengan kunci yang sama saat pengenkripsian untuk memperoleh pesan rahasia kembali. Pada pengambilan citra, akan terdeteksi otomatis jika *image* yang diambil berupa *stego-image* maka pesan dapat langsung diekstraksi dan didekripsi.



Gambar 6. *Skema umum sistem*

Hasil

Pengujian dilakukan secara subjektif dan objektif. Pengujian secara subjektif dilakukan dengan membagikan kuisioner kepada sejumlah responden untuk berpendapat mengenai dua buah gambar yang sama persis, dimana salah satu dari gambar tersebut merupakan *stego-image*. Responden yang dipilih merupakan mahasiswa/i ilmu komputer yang telah memahami secara umum tentang steganografi dan kriptografi. Melalui kuisioner ini diharapkan secara visual manusia tidak dapat membedakan antara *stego-image* dan *cover-image*. Pada pengujian ini diperoleh sebanyak 33 Responden yang telah menjawab kuisioner, dari hasil yang diperoleh dapat disimpulkan bahwa sebesar 72% responden menyatakan dari segi kecerahan warna gambar 1 dan gambar 2 tidak memiliki perbedaan yang signifikan (sama saja). Sebesar 48% responden menyatakan dari segi *noise* gambar 1 dan gambar 2 sama/tidak memiliki perbedaan yang signifikan. Pada pertanyaan ketiga responden diminta untuk memilih menurut visual mereka yang mana dari kedua gambar tersebut yang merupakan *stego-image*, hasilnya adalah sebesar 67% dari responden memilih gambar 2 (*cover-image*) dan menyatakan bahwa kedua citra tersebut sama

Tabel 1. *Hasil Uji kuisioner*

Pertanyaan	Jawaban		
	Gambar 1	Gambar 2	Sama
Menurut anda apakah Gambar 1 atau Gambar 2 yang lebih terang (cerah) atau sama saja?	5	4	24
Menurut anda apakah Gambar 1 atau Gambar 2 yang lebih banyak noise (bintik-bintik) atau sama saja?	7	10	16
Salah satu dari kedua gambar diatas telah disisipkan pesan text, menurut anda apakah Gambar 1 atau Gambar 2 yang telah disisipkan pesan text?	11	18	4

Penilaian secara objektif didasarkan pada *error* yang terdapat pada citra yang telah diolah. Untuk citra asal f(x,y) dan hasil citra proses g(x,y) dengan ukuran pixel M x N, maka beberapa parameter yang dapat digunakan adalah sebagai berikut :

1. *Root Mean Square Error* (RMSE)

$$\text{RMSE} = \sqrt{\frac{1}{\text{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} |\big(f(x,y) - g(x,y)\big) 2|}$$

2. *Peak Signal to Noise Ratio* (PSNR)

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

Tabel 2. Pengujian RSME dan PSNR

Cover-Image	*Stego-Image*	RSME	PSNR
Wrangler.bmp	Ujiwrangler.bmp	2.75	39.33
Rainbowcake.bmp	Ujirainbowcake.bmp	0.13	65.80
Lena512.bmp	Ujilena512.bmp	0.35	57.31
Boat.bmp	Ujiboat.bmp	0.26	59.80
Bear.bmp	Ujibear.bmp	0.13	65.69
Barbara.bmp	Ujibarbara.bmp	0.31	58.27
Peppers.bmp	Peppersquis.bmp	0.49	54.30
Girlface.bmp	Ujiquisioner.bmp	0.33	57.66

3. Kesimpulan

Stego-image yang dihasilkan, dinyatakan tidak mengalami perubahan kualitas citra. Pada pengujian secara subjektif yang dilakukan dengan membagikan kuisioner kepada 33 responden. Penilaian kualitas citra digital secara objektif dilakukan dengan cara menghitung nilai *Root Mean Square Error* (RMSE) dan *Peak Signal to Noise Rational* (PSNR), dimana dari 8 *stego-image* yang diujikan dapat disimpulkan tidak mengalami

ISSN PRINT : 2302-500X
ISSN ONLINE : 2477-3786

perubahan kualitas yang signifikan, terbukti dengan nilai RMSE yang rendah dan nilai PSNR berada diatas 30 dB. Penelitian dapat diperluas lagi agar bisa menggunakan citra digital dengan format yang lain, selain citra bitmap 8 bit serta dalam segala ukuran. Perangkat lunak ditambahkan fitur ekspansi wadah agar pesan yang ingin disisipkan menjadi tidak terbatas. Perangkat lunak dikembangkan lagi agar *stego-image* tetap tangguh ketika mendapatkan serangan *resize image*, *cropping image* dan lain-lain

Daftar Pustaka

[1] R. Frinkel, R. Taylor, R. Bolles, R. Paul, "An overview
[2] Burwick, C. et al., 1998. MARS - a Candidate Cipher for AES. *NIST AES Proposal*, pp.8–23.
[3] Burwick, C. & Coppersmith, D., 1999. The Mars Encryption Algorithm. , pp.1–12. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.35.5887&rep=rep1&type=pdf.
[4] Halevi, S., 2015. Key Agility in MARS. *Statewide Agricultural Land Use Baseline 2015*, 1(May).
[5] Kelsey, J. & Schneier, B., 2000. MARS Attacks! Preliminary Cryptanalysis of Reduced-Round MARS Variants. *The Third {Advanced Encryption Standard} Candidate Conference, April 13--14, 2000, New York, NY, USA*, pp.169–185. Available at: http://csrc.nist.gov/encryption/aes/round2/conf3/aes3conf.htm;\nhttp://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings.pdf;\nhttp://csrc.nist.gov/encryption/aes/round2/conf3/papers/AES3Proceedings-1.pdf;\nhttp://csrc.nist.gov/encryption/a.
[6] Lee, Y.K. & Chen, L.H., 2000. High capacity image steganographic model. *IEE Proceedings - Vision, Image, and Signal Processing*, 147(3), p.288. Available at: http://digital-library.theiet.org/content/journals/10.1049/ip-vis_20000341.
[7] Meena, M.K., Kumar, S. & Gupta, N., 2011. Image Steganography tool using Adaptive Encoding Approach to maximize Image hiding capacity. *Soft Computing*, (2), pp.7–11.
[8] Munir, R., 2006. *Kriptografi*, Informatika.
[9] Schneier, B., 1996. Applied cryptography: Protocols, algorithm, and source code in C. *Government Information Quarterly*, 13(3), p.336.