Peningkatan Keamanan Citra Warna Dengan Model Warna HSI dan Password pada Kriptografi Visual Skema((N-1,1), N)

Ronsen Purba[1], Sunario Megawan[2], Anisah[3], Kardika Sidabariba[4]
STMIK Mikroskil, Jl. Thamrin No. 112, 124, 140, Telp. (061) 4573767, Fax. (061) 4567789
Jurusan Teknik Informatika, STMIK Mikroskil, Medan
[1]ronsen@mikrsokil.ac.id, [2]sunario@mikroskil.ac.id, [3]nisaborreg@gmail.co.id,
[4]kardikasidabariba@gmail.com

Abstrak

Skema kriptografi visual ((n-1,1),n) menggunakan (n-1) natural image untuk menghasilkan n buah shares. Skema ini dapat mengatasi ekspansi piksel dan rekonstruksi dapat dilakukan tanpa distorsi. Namun, share yang dihasilkan akan menimbulkan kecurigaan pihak lain karena bersifat acak. Untuk itu perlu dilakukan pengamplopan dengan teknik steganografi untuk menyembunyikan shares yang sudah diacak tersebut. Dalam penelitian ini dilakukan pengamplopan share dengan teknik steganografi model warna Hue-Saturation-Intensity (HSI) berbasis LSB. Kelebihan dari model HSI adalah sesuai untuk menggambarkan warna berdasarkan interpretasi manusia dan komponen intensitas tidak berkorelasi dengan komponen hue dan saturation. Lebih jauh, model HSI dapat menampung yang lebih banyak serta proses ekstraksi yang lebih rumit disbanding warna lain. Namun, pengamanan tersebut tidaklah cukup, karena pihak yang tidak berkepentingan dapat memperoleh secret image hanya dengan melakukan konversi dan rekonstruksi. Oleh karena itu, sistem dilengkapi dengan password, sehingga tidak sembarang orang dapat membuka amplop yang berisi share. Hasil pengujian menunjukkan penyembunyian shares model warna HSI dan penambahan password dapat meningkatkan keamanan kriptografi visual. Terhadap stego image juga dilakukan serangan noise dengan empat jenis distribusi dan pengujian menunjukkan bahwa distribusi Gauss lebih tangguh disbanding yang lain.

Kata kunci*— kriptografi visual, skema secret sharing, steganografi, model warna hsi*

Abstract

Visual cryptography ((n-1,1),n) scheme uses (n-1) natural images to produce n shares. This scheme can resolve pixel expansion problems and reconstruction can be done without distortion. Furthermore, the amount of bits embedded using HSI color model is bigger than other color model and extraction process is more difficult. However, the resulting share can arouse a suspicion to other party because of its randomness. In this research we do enveloping process with steganography techniques using Hue-Saturation-Intensity (HSI) color model based on LSB to hide share. The advantages of this color model is appropriate to describe the color based on human interpretation. However, image security using these method is not enough because anyone can take bits of share and obtain secret image by converting and reconstruction processes. Therefore, it takes other security by adding a password. Based on the analisys of test result, hiding share by using HSI color model and addition a password can improve visual cryptography security. We also test the stego image with four noise distributions and shows that Gaussian distribution is the more robust than the others.

Keywords*— visual cryptography, secret sharing scheme, steganography, his color model*

1. PENDAHULUAN

Sejak pertama kali diperkenalkan oleh Naor dan Shamir pada tahun 1995, kriptografi visual terus mendapat perhatian para akademisi dan peneliti di bidang keamanan citra [1]. Salah satu penelitian yang dilakukan oleh Park et al., pada tahun memperkenalkan sebuah metode kriptografi visual dengan menggunakan codebook [2]. Namun, shares yang dihasilkan terlihat seperti titik-titik acak, sehingga dapat menimbulkan masalah manajemen sharing karena semua shares terlihat sama dan dapat menimbulkan resiko kecurigaan pihak ketiga dalam proses transmisi [2]. Pada tahun 2009, Wang et al.

memperkenalkan sebuah metode kriptografi visual skema (k,n) dengan menggunakan gambar kamuflase (gambar tersamar) yang berbeda untuk mengidentifikasi shares sehingga dapat meningkatkan kemudahan manajemen. Namun, metode ini memiliki kelemahan yaitu ekspansi piksel yang besar sehingga hasil share mengalami perbesaran dari secret image dan kualitas rekonstruksi yang buruk [3]. Pada tahun 2013, Liu et al. memperkenalkan sebuah skema kriptografi visual untuk citra warna yaitu skema ((n-1,1),n), dimana (n-1) natural image digunakan sebagai input untuk menghasilkan n buah shares. Hasil pengujian yang dilakukan oleh Liu et al. menunjukkan bahwa enkripsi menggunakan skema ini dapat mengatasi masalah ekspansi piksel dan rekonstruksi share dapat dilakukan tanpa distorsi [4]. Namun, share yang dihasilkan akan menarik perhatian pihak lain dan menimbulkan kecurigaan karena sifatnya acak.

Untuk mengurangi kecurigaan pihak lain terhadap share, maka perlu dilakukan teknik pengamanan lain yaitu pengamplopan dengan memanfaatkan teknik steganografi [5]. Pada tahun 2015, Muhammad et al. memperkenalkan teknik steganografi dengan menggunakan warna Hue-Saturation-Intensity berbasis LSB [7]. Kelebihan dari model warna ini adalah sesuai untuk menggambarkan warna berdasarkan interpretasi manusia dan komponen intensitas tidak berkorelasi dengan komponen Hue dan Saturasi [6]. Selanjutnya jumlah bit yang dapat disembunyikan lebih banyak serta proses ekstraksi lebih rumit disbanding model warna lain [7, 8]. Hasil analisis oleh Muhammad et al., pengamanan data menggunakan model warna HSI menunjukkan data tidak dapat dikenali (good imperceptibility) [9]. Namun, metode ini masih memiliki kelemahan, yaitu proses ekstraksi dapat dilakukan oleh siapa saja yang mengetahui jumlah bit sisip dengan melakukan konversi dari RGB ke HSI dan sebaliknya. Kemudian, konversi dari HSI ke RGB terkadang memberikan nilai RGB di atas 255. Oleh karena itu, dalam penelitian ini dilakukan modifikasi rumus konversi HSI ke RGB dan sebaliknya serta penambahan password untuk meningkatkan keamanan kriptografi visual. Selanjutnya dilakukan pemberian jumlah bit sisip yang berbeda untuk menambah tingkat keamanan kriptografi visual. Kemudian dilakukan pengujian imperceptibility dengan mengkukur nilai MSE dan PSNR serta pengujian aspek robustness dengan pemberian noise.

2. KAJIAN PUSTAKA

2.1. Model Warna HSI

Model warna HSI (hue, saturation, intensity), memisahkan komponen intensitas dari informasi warna yang dibawa (hue dan saturasi) dalam warna citra. Sebagai hasilnya, model HSI adalah tool yang ideal untuk mengembangkan algoritma pengolahan citra berdasarkan pada deskripsi warna yang alami dan intuitif terhadap manusia, pengembang dan user-nya. Adapun penjelasan dari ketiga komponen HSI diuraikan berikut ini [8]:

a. *Hue.* Menyatakan warna sebenarnya, seperti merah, violet, dan kuning. *Hue* digunakan untuk membedakan warna-warna dan menentukan kemerahan (*redness*), kehijauan (*grenness*), dan sebagainya dari cahaya. *Hue* berasosiasi dengan panjang gelombang cahaya, dan bila menyebut warna merah, violet, atau kuning, sebenarnya menspesifikasikan nilai *hue*-nya. Nilai *hue* merupakan sudut dari warna yang mempunyai rentang dari 0° sampai 360°. 0° menyatakan warna merah, lalu memutar nilai-nilai spektrum warna tersebut kembali lagi ke 0° untuk menyatakan merah lagi [7, 8, 9].
b. *Saturation.* Menyatakan tingkat kemurnian warna cahaya, yaitu mengindikasikan seberapa banyak warna putih diberikan pada warna. Warna merah adalah 100% warna-warna jenuh (*saturated color*), sedangkan warna *pink* adalah warna merah dengan tingkat kejenuhan sangat rendah (karena ada warna putih di dalamnya). Jadi, jika *hue* menyatakan warna sebenarnya, maka *saturation* menyatakan seberapa dalam warna tersebut [7, 8, 9].
c. *Intensity/brightness/luminance.* Intensitas merupakan atribut yang menyatakan banyaknya cahaya yang diterima oleh mata tanpa mempedulikan warna. Kisaran nilainya adalah antara gelap (hitam) dan terang (putih). Tingkatan nilai *intensity* adalah dari 0% sampai dengan 100% [7, 8, 9].

2.1.1. Konversi Model Warna RGB ke HSI

Komponen warna RGB pada citra dapat dikonversi menjadi model warna HSI. Untuk mendapatkan nilai Hue, Saturasi dan Intensitas, besarannya dapat dihitung secara langsung dengan rumus berikut [7]:

$$r = \frac{R}{R+G+B}; \qquad g = \frac{G}{R+G+B}; \qquad b = \frac{B}{R+G+B} \tag{1}$$

$$h = cos^{-1}\left[\frac{0.5\,x\,\{(r-g)+(r-b)\}}{[(r-g)^2+(r-b)(g-b)]^{\frac{1}{2}}}\right], h \in [0,\pi];\ for\ b \le g$$

$$h = 2\pi - cos^{-1}\left[\frac{0.5\,x\,\{(r-g)+(r-b)\}}{[(r-g)^2+(r-b)(g-b)]^{\frac{1}{2}}}\right], h \in [0,2\pi];\ for\ b > g$$

$$s = 1 - 3\,x\,Min(r,g,b), s \in [0,1]$$

$$i = \frac{R+G+B}{3\,X\,255}, i \in [0,1] \tag{2}$$

$$I = i\,x\,255 \tag{3}$$

2.1.2. Konversi Model Warna HSI ke RGB

Sementara komponen warna HSI dapat dikonversi menjadi model warna RGB. Untuk mendapatkan nilai R, G dan B, besarannya dapat dihitung secara langsung dengan rumus berikut [7]:

$$i = \frac{I}{255} \tag{4}$$

$$o = i \times (1 - s); \qquad p = I \times \left[1 + \frac{s\,x\cos(h)}{\cos\left(\frac{\pi}{3}h\right)}\right]; \qquad q = 3 \times i - (o + p); \tag{5}$$

If $h < \frac{2\pi}{3}$ then $b = o;\quad r = p;\ g = q;$ (6)

If $\frac{2\pi}{3} \le h < \frac{4\pi}{3}$ then $h = h - \frac{2\pi}{3};\ r = o;\ g = p;\ b = q;$ (7)

If $\frac{4\pi}{3} < h \le 2\pi$ then $h = h - 240;\ g = o;\ b = p;\ r = q;$ (8)

2.2. Kriptografi Visual

Kriptografi visual yaitu teknik kriptografi untuk gambar atau citra dengan membagi gambar tersebut menjadi beberapa bagian. Kriptografi visual diperkenalkan pertama kali oleh Moni Naor dan Adi Shamir dalam paper mereka yang berjudul Visual Cryptography, dimuat dalam jurnal Eurocrypt'94, pada tahun 1995 [1]. Berbeda dengan kebanyakan teknik kriptografi, algoritma ini tidak membutuhkan perhitungan rumit untuk mendekripsi pesan, tetapi hanya menggunakan sistem penglihatan manusia. Versi dasar kriptografi visual mempresentasikan secret sharing (2, 2). Maksudnya skema tersebut menghasilkan 2 (dua) citra pembagi dari gambar aslinya (P) yaitu sebuah gambar hitam putih. Dimana gambar P1 untuk bagian gambar 1 dan P2 untuk bagian gambar 2. P1 dan P2 merupakan distribusi acak dari piksel hitam putih dan tidak menunjukkan informasi apapun. Namun saat P1 dan P2 dilapiskan/ ditumpuk, maka akan didapat informasi seperti gambar aslinya. Apabila hanya ada P1, maka informasi P tidak dapat diketahui tanpa ada P2 [2, 3, 5].

2.2.1. Kriptografi Visual Skema (k,n)

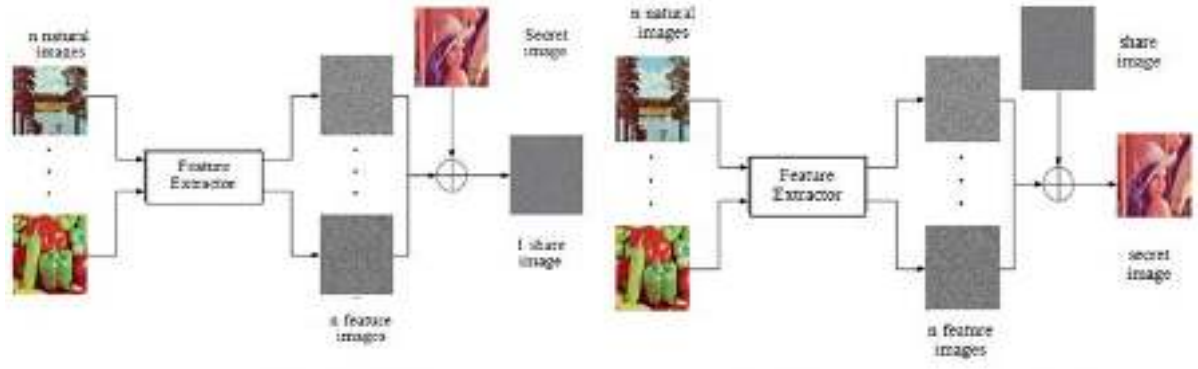
Skema kriptografi visual (k, n) adalah sebuah teknik kriptografi dimana citra digital dibagi ke dalam n *shares* yang dilakukan dengan komputasi kriptografi dimana untuk mendekripsi citra diperlukan minimal k buah citra hasil tersebut. Jika terdapat q citra hasil, dimana $q < k$, maka tidak ada informasi apapun yang dapat diperoleh tentang citra asli [10].

Solusi untuk skema k dari n terdiri dari dua buah matriks *Boolean* yang berukuran $n \times m$, C_0 dan C_1. Untuk membagi *pixel* putih, dipilih salah satu dari matriks C_0, dan untuk membagi *pixel* hitam dipilih salah satu dari matriks C_1. Matriks yang telah dipilih merupakan representasi dari *m subpixel* yang terletak pada masing-masing *n* transparansi. Solusi benar apabila memenuhi seluruh kondisi berikut[10]:

1. Untuk sembarang matriks m padaC_0, hasil operasi "or" dengan V pada sembarang baris k dari n memenuhi $H(V) < d - \alpha m$.
2. Untuk sembarang matriks m pada C_1, hasil operasi "or" dengan V pada sembarang baris k dari n memenuhi $H(V) < d - \alpha m$.
3. Untuk sembarang $j < k$ baris yang dipilih, submatriksnya muncul dengan frekuensi yang sama pada C_0 dan C_1

2.2.2. *Kriptografi Visual Skema* $((\boldsymbol{n-1},\boldsymbol{1}),\boldsymbol{n})$

Kriptografi visual skema ((n-1,1),n) merupakan skema kriptografi dimana (n-1) natural image digunakan sebagai input untuk menghasilkan n buah shares, angka 1 menunjukkan jumlah secret image, sementara n menunjukkan jumlah shares yang dihasilkan yaitu natural share image dan share image hasil pembentukan share. Proses pembentukan share dilakukan dengan melakukan ekstraksi fitur untuk masing-masing dari (n-1) natural image sehingga menghasilkan (n-1) natural share image, kemudian dilakukan penggabungan. Hasil penggabungan kemudian dilakukan operasi XOR dengan secret image sehingga menghasilkan share image [4]. Sedangkan untuk proses rekonstruksi, (n-1) natural share image digabungkan kemudian dilakukan operasi XOR dengan share image sehingga menghasilkan secret image. Natural share image yang berbeda atau kurang dari (n-1) tidak akan mendapatkan informasi apapun tentang secret image [4]. Adapun proses pembentukan share dan rekonstruksi dijelaskan pada gambar di bawah ini.



Gambar 1. Proses Pembentukan dan Rekonstruksi Share (Sumber: Liu et al., 2013)

3. METODE PENELITIAN

Dalam Penelitian ini terdapat 2 proses utama yaitu proses penyisipan dan ekstraksi dengan . menggunakan gabungan metode kriptografi visual skema ((n-1,1),n) dan model warna HSI berbasis LSB. Untuk meningkatkan keamanan, maka dalam proses penyisipan dan ekstraksi diharuskan memberikan password dan jumlah bit sisip yang akan menentukan ukuran minimum sampul (amplop) yang harus digunakan. Akan tetapi dalam penerapan model warna HSI terdapat kelemahan yaitu nilai RGB setelah konversi dari HSI melebihi 255. Oleh karena itu dilakukan penambahan subproses yaitu perulangan konversi dan penyisipan data yang sama hingga diperoleh nilai RGB hasil konversi maksimal 255. Cara kerja kedua proses utama tersebut dijelaskan sebagai berikut:

3.1. *Kriptografi Visual Skema* $((\boldsymbol{n-1},\boldsymbol{1}),\boldsymbol{n})$

Proses penyisipan (embedding) bertujuan untuk menghasilkan stego image, yaitu melakukan pembentukan share dari secret image kemudian membungkusnya ke dalam amplop (cover image). Tahapan proses penyisipan (embedding) terdiri dari pembentukan share dan penyisipan share seperti pada Gambar 2 (a). Adapun penjelasan dari tiap tahapan proses penyisipan adalah sebagai berikut:

1. Pembentukan *Share*. Proses pembentukan *share* bertujuan untuk menghasilkan *share* dari *secret image*. Proses ini menggunakan skema $((n-1,1),n)$. Proses pembentukan *share* terdiri dari dua tahap, yaitu Ektraksi Fitur dan Enkripsi. Pada Ekstraksi Fitur, $(n-1)$ *natural image* diekstrak

menjadi $(n-1)$ *natural share image,* kemudian dilakukan penggabungan. Pada proses enkripsi hasil penggabungan *natural share image* dilakukan operasi XOR dengan *secret image* sehingga menghasilkan *share image*.

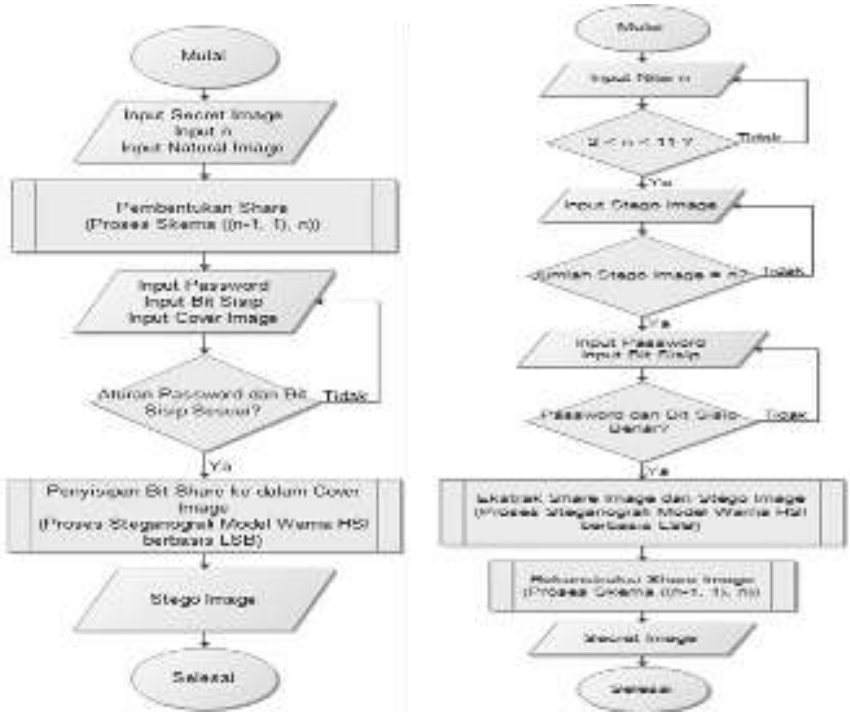
2. Penyisipan *Share.* Proses penyisipan *share* bertujuan untuk menghasilkan *stego image*, yaitu citra yang berisi sisipan *share image* dan *natural share image*. Proses ini dilakukan dengan mengkonversi *cover image* (RGB) menjadi citra HSI, kemudian menyisipkan bit *share, natural share image* dan *password* pada nilai intensitas citra HSI menggunakan teknik LSB. Jumlah bit nilai intensitas yang akan digantikan oleh bit *share, natural share image* dan *password* tergantung nilai *b* yang di-*input* $(1 \leq b \leq 4)$. Semakin besar nilai *b* maka *cover image* yang dibutuhkan akan semakin kecil, dan sebaliknya.

3.2. Proses Ekstrak

Proses ekstrak bertujuan untuk mendapatkan kembali secret image setelah proses penyisipan. Tahapan proses ekstrak terdiri dari ekstrak share dan rekonstruksi share seperti pada Gambar 2 (b). Adapun penjelasan dari tiap tahapan proses ekstrak adalah sebagai berikut

1. Ekstrak *Share*. Proses ini bertujuan untuk mendapatkan *share* yang telah disisipkan pada *stego image*. Untuk mendapatkan *share*, *stego image* (RGB) dikonversi ke warna HSI kemudian mengambil bit *share* yaitu *b* bit trakhir nilai intensitas, dimana *b* merupakan jumlah bit nilai intensitas yang digantikan dengan bit *share*.
2. Rekonstruksi *Share*. Proses ini bertujuan untuk mendapatkan kembali *secret image* setelah pembentukan *share* pada proses *embedding*. Untuk mendapatkan *secret image* dilakukan rekonstruksi *share* yaitu dengan melakukan penggabungan $(n-1)$ *natural share image,* hasil penggabungan kemudian dilakukan operasi XOR dengan *share image.*

Proses penyisipan dan ekstraksi share dalam penelitian ini dapat dilihat pada gambar berikut:



(a) Proses Penyisipan (b) Proses Ekstraksi

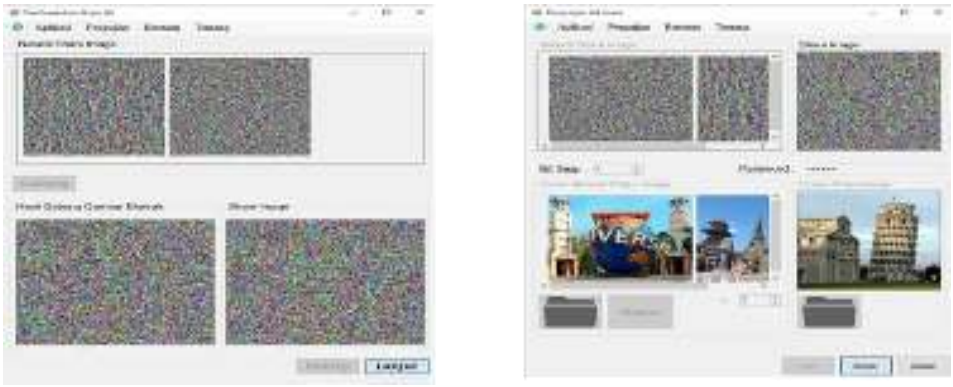
Gambar 2. Bagan Alir Proses Penyisipan dan Proses Ekstrak

3. HASIL DAN PEMBAHASAN

3.1. Hasil

a. Proses Penyisipan

Untuk melakukan proses penyisipan, mula-mula dilakukan input *secret image* kemudian nilai *n* dan *natural image* sebanyak $(n-1)$. Kemudian dilakukan proses ekstraksi fitur dengan mengklik *button* 'Ekstraksi Fitur' sehingga menghasilkan $(n-1)$ *natural share image*. Klik *button* 'Gabung' untuk melakukan proses penggabungan $(n-1)$ *natural share image*. Hasil penggabungan kemudian digunakan untuk proses enkripsi yatu dengan mengklik *button* 'Enkrip' sehingga menghasilkan *share image* seperti pada Gambar 3 (a). Gabungan semua proses di atas disebut Pembentukan *Share.* Tahap selanjutnya yaitu dengan melakukan proses penyisipan. Klik button 'Lanjut' untuk masuk ke *form* 'Penyisipan Bit Share'. Untuk melakukan proses penyisipan langkah pertama yaitu *input* bit sisip dan *password*, kemudian *input cover image* sejumlah *n*. Klik *button* 'Sisip' untuk melakukan proses penyisipan sehingga menghasilkan *stego image* seperti pada Gambar 3 (b). *Stego image* dapat disimpan dengan mengklik *button* 'Simpan'.

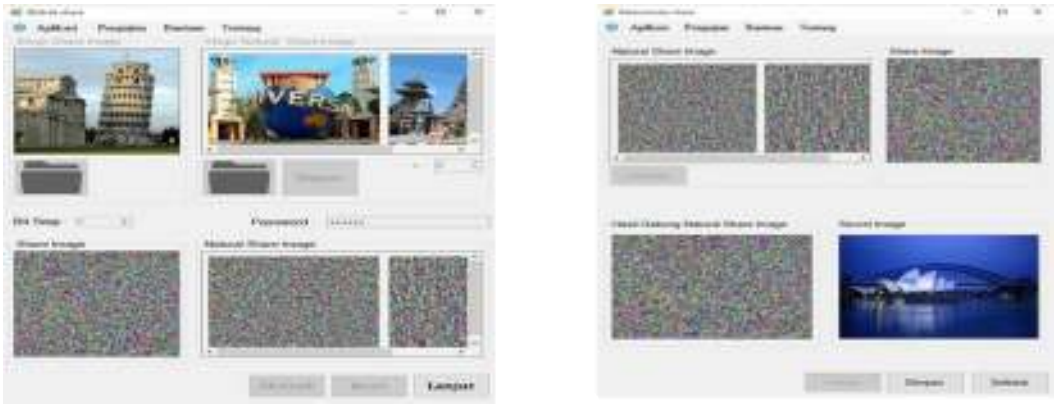


(a) Hasil Proses Pembentukan Share (b) Hasil Proses Penyisipan

Gambar 3. Tahapan Proses Penyisipan (Embedding)

b. Proses Ekstrak

Untuk melakukan proses ekstrak, mula-mula *input stego share image* dan *stego natural share image* yang akan diekstrak. *Input* bit sisip dan *password* yang sama dengan bit sisip dan *password* pada saat proses penyisipan kemudian klik *button* 'Ekstrak' untuk mengekstrak bit *share* dari *stego image* sehingga menghasilkan *n* buah *share* seperti pada Gambar 4 (a). Klik *button* 'Lanjut' untuk masuk *form* 'Rekonstruksi'. Lakukan proses penggabungan $(n-1)$ *natural share image* dengan mengklik *button* 'Gabung', kemudian tahap yang terakhir yaitu klik *button* 'Dekrip' sehingga menghasilkan *secret image* seperti pada Gambar 4 (b). *Secret image* dapat disimpan dengan mengklik *button* 'Simpan'.



(a) Hasil Proses Ekstraksi (b) Hasil Proses Rekonstruksi

Gambar 4. Tahapan Proses Ekstraksi

4.2. Pembahasan

Pada pembahasan ini dilakukan pengujian yang terdiri dari dua jenis yaitu pengujian parameter dan pengujian kualitas citra.

4.2.1. Pengujian Paramater

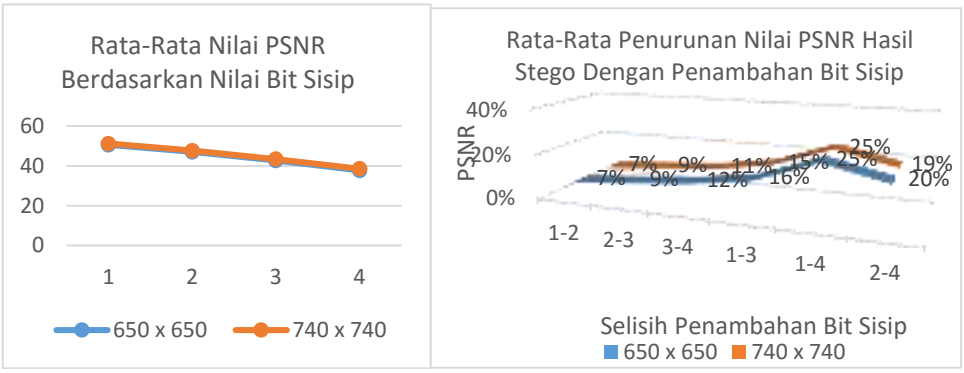
Pengujian ini dilakukan untuk mengetahui pengaruh parameter bit sisip dan kontras amplop yang berbeda terhadap hasil stego dengan ukuran MSE dan PSNR

1. Pengujian Bit Sisip, terdiri dari:
   a. Pengujian dengan sampul yang sama. Pada pengujian ini digunakan *secret image* dan *natural image* dengan ukuran 128 x 128 piksel dan *password* adalah "Mikro2016!". Proses pengujian dilakukan dengan memberikan nilai bit sisip 1, 2, 3 dan 4 dan dengan ukuran amplop 650 x 650 dan 740 x 740 dan hasil pengujian dapat dilihat pada Tabel 1 berikut:

Tabel 1. Perbandingan Nilai MSE dan PSNR Dengan Ukuran Cover Sama

Ukuran Cover	Nama Stego	Bit Sisip							
		1		2		3		4	
		MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
740 x 740	15_1024x1024	0.42	51.94	0.99	48.17	2.68	43.85	8.01	39.1
	9_1024x1024	0.61	50.26	1.35	46.83	3.61	42.56	11	37.72
	17_1024x1024	0.46	51.47	1.01	48.11	2.72	43.79	8.16	39.02
650 x 650	1_1280x1280	0.65	49.98	1.41	46.65	3.47	42.72	10.17	38.06
	3_1280x1280	0.54	50.8	1.25	47.15	3.41	42.8	10.03	38.12
	4_1280x1280	0.53	50.9	1.21	47.31	3.65	42.51	13.26	36.9

Adapun rata-rata nilai PSNR dari *stego* dapat dilihat pada Gambar 5(a) dan 5(b) berikut:



(a) (b)

Gambar 5. (a) Rata-rata nilai PSNR Berdasarkan Nilai Bit Sisip (b) Rata-rata Penurunan Nilai PSNR dengan Penambahan Jumlah Bit Sisip

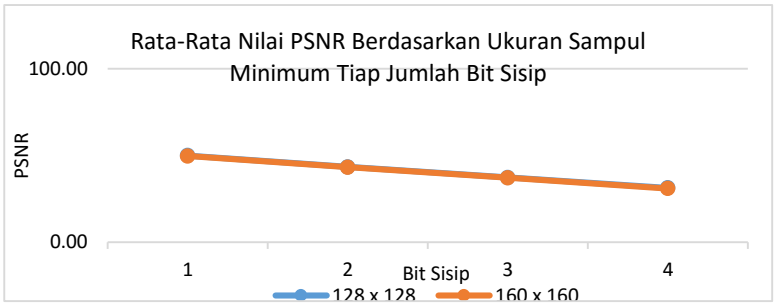
   b. Pengujian dengan ukuran sampul minimum untuk tiap jumlah bit sisip. Pada pengujian ini digunakan 2 buah *share* dengan ukuran 128 x 128 dan 160 x 160 serta 6 buah amplop yang memiliki ukuran yang berbeda, tergantung ukuran *share* dan bit sisip. Adapun *password* yang akan disisip adalah "Mikro2016!". Sama seperti pengujian sebelumnya, jumlah bit sisip adalah 1, 2, 3 dan 4. Amplop yang digunakan adalah ukuran minimum untuk melihat nilai MSE dan PSNR. Hasil pengujian dapat dilihat pada Tabel 2 berikut:

Tabel 2. Perbandingan Nilai MSE dan PSNR dengan Ukuran Amplop Minimum

Ukuran Share	Bit Sisip	Ukuran Amplop Minimal	Nama Stego	MSE	PSNR
128 x 128	1	628 x 128	universal	0.7	49.67
	2	444 x 444		3.14	43.15
	3	363 x 363		12.49	37.17
	4	314 x 314		49.54	31.18
	1	628 x 128	Taman bunga	0.68	49.82
	2	444 x 444		2.98	43.39
	3	363 x 363		12.05	37.32
	4	314 x 314		48.22	31.3
	1	628 x 128	64_15_1024x1024	0.58	50.53
	2	444 x 444		2.74	43.76
	3	363 x 363		10.98	37.72
	4	314 x 314		43.81	31.72
160 x 160	1	784 x 784	16_1280x1280	0.7	49.68

	2	555 x 555		3.04	43.3
	3	453 x 453		12.52	37.16
	4	392 x 392		51.13	31.04
	1	784 x 784	THE GRAND CANYON	0.57	50.54
	2	555 x 555		2.66	43.89
	3	453 x 453		10.77	37.81
	4	392 x 392		43.27	31.77
	1	784 x 784	Petronas	0.83	48.96
	2	555 x 555		3.44	42.77
	3	453 x 453		13.91	36.7
	4	392 x 392		63.36	30.11

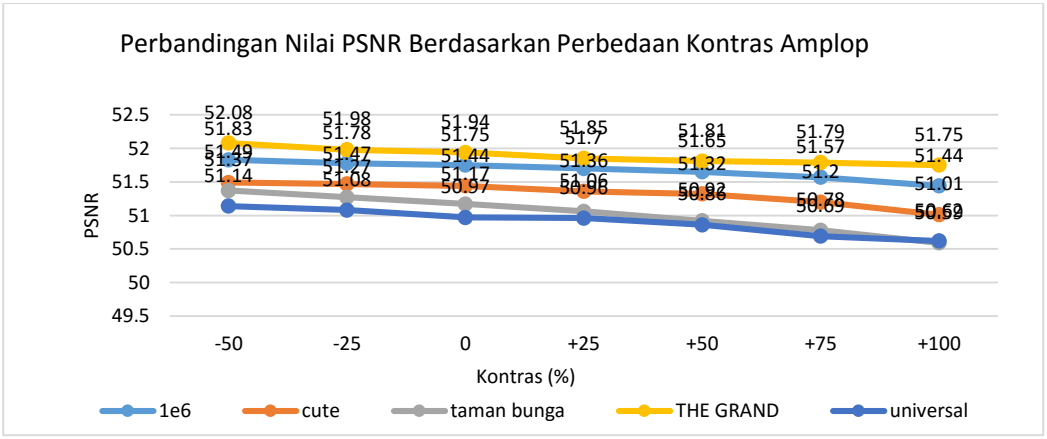
Adapun rata-rata nilai PSNR dari 6 *stego* dengan ukuran amplop berbeda dapat dilihat pada Gambar 6 berikut:



Gambar 6. Rata-rata Nilai PSNR Berdasarkan Ukuran Amplop dan Jumlah Bit Berbeda

2. Pengujian Konstras Amplop

Pada pengujian ini digunakan 5 buah amplop (*cover*), dimana masing-masing sampul (amplop) memiliki konstras yang berbeda yang dilakukan dengan mengubah nilai kontras menggunakan *paint*. Adapun *share* yang akan disisip memiliki ukuran 128 x 128 dan *password* adalah "Mikro2016!". Proses pengujian dilakukan penyisipan *secret image*, kemudian melakukan perbandingan *stego image* dengan menghitung nilai PSNR. Adapun bit sisip yang digunakan dalam proses *embedding* adalah 1. Hasil pengujian dapat dilihat pada Gambar 7 berikut:



Gambar 7. Perbandingan Nilai PSNR Berdasarkan Perbedaan Kontras Amplop

4.2.1. Pengujian *Robustness*

Pengujian ini dilakukan untuk mengetahui kembali atau tidak secret image hasil rekonstruksi setelah stego image diberi noise dengan persentasi kembali minimum sekitar 85%. Secret image yang digunakan memiliki ukuran 128 x 128 dimana password pada saat penyisipan adalah "Mikro2016!" dengan bit sisip 1 dan 2. Ukuran amplop yang digunakan adalah minimum untuk jumlah bit sisip 1 dan 2. Sementara distribusi pemberian noise yang digunakan adalah uniform, Gauss, Salt & Pepper dan Speckle. Hasil pengujiannya dapat dilihat pada Tabel 3 berikut:

Tabel 3. Hasil Pengujian Kualitas Citra Setelah Pemberian Noise

Bit Sisip	Ukuran Stego	Bit Sisip / Ukuran Stego		
		Jenis Noise	Nilai Probabilitas	Persentase Kembali (%)
1	444 x 444	Uniform	0,005	100
			0.015	99.35
			0.025	99.35
			0.035	98.32
			0,045	96,37
			0,055	93,48
			0,065	88,68
		Gaussian	0,02	100
			0,03	99,84
			0,04	99,65
			0,05	99,18
			0,06	98,12
			0,07	97,95
			0,08	96,43
			0,09	93,97
			0,1	93,79
		Salt & Pepper	0,000001	100
			0,005001	98,01
			0,010001	96,12
			0,015001	88,56
			0,020001	92,14
			0,025001	90,45
			0,030001	88,39
			0,035001	86,72
			0,040001	85,06
		Speckle	0,000004	100
			0,005004	98,09
			0,010004	96,04
			0,015004	94,31
			0,020004	92,39
			0,025004	90,53
			0,030004	88,76
			0,035004	87,02
			0,040004	85,27
2	628 x 628	Uniform	0,005	100
			0.015	99,9
			0.025	99,56
			0.035	98,68
			0,045	96,95
			0,055	94,63
			0,065	90,69
			0,075	86,06
		Gaussian	0,01	100
			0,02	99,96
			0,03	99,91
			0,04	99,74
			0,05	99,05
			0,06	98,76
			0,07	98,54
			0,08	96,84
			0,09	95,5
			0,1	95,27
		Salt & Pepper	0.000001	100
			0.005001	98,5
			0.010001	97,06
			0.015001	95,59
			0.020001	94,15
			0.025001	92,66
			0.030001	91,42
			0.035001	89,77
			0.040001	88,55
			0.045001	87,33
			0.050001	85,73
			0.000004	100

		Speckle	0.005004	98,55
			0.010004	97,01
			0.015004	95,57
			0.020004	94,15
			0.025004	92,57
			0.030004	91,34
			0.035004	89,97
			0.040004	88,55
			0.045004	86,94
			0.050004	85,88

Hasil pengujian di atas menunjukkan distribusi Gauss masih kuat terhadap penambahan noise sampai dengan probabilitas 0,01. Sementara untuk distribusi Uniform tahan sampai dengan nilai probabilitas sekitar 0,07. Sedangkan distribusi Salt & Pepper dan Speckle hanya tahan pada nilai sekitar 0,05

4. KESIMPULAN

Berdasarkan hasil pengujian yang dilakukan, maka ditarik kesimpulan sebagai berikut:

1. Penambahan 1 bit sisip menyebabkan penurunan nilai PSNR hasil *stego* sebesar 2% sampai 3%
2. *Stego image* dengan ukuran amplop minimum untuk masing-masing jumlah bit sisip tidak menimbulkan kecurigaan dengan nilai PSNR di atas 30 dB
3. Semakin kecil nilai kontras amplop semakin tinggi nilai PSNR citra *stego*
4. Ketangguhan *stego image* yang dihasilkan terhadap serangan diurutkan dari probabilitas terbesar ke terkecil adalah Gauss, *Uniform, Speckle* dan *Salt & Pepper*

5. SARAN

Untuk memberikan hasil yang lebih baik, maka saran yang dapat dilakukan antara lain:

1. Penyisipan bit *share* ke dalam amplop dapat dilakukan dengan cara yang acak seperti pemanfaatan generator modulo bilangan prima yang lebih kecil dari ukuran citra amplop untuk meningkatkan keamanan
2. Rumus konversi RGB ke HSI dan sebaliknya masih perlu pengujian lebih lanjut dan penyisipan dilakukan ke dalam intensitas yang sebenarnya
3. Perlu dilakukan pengujian terhadap perubahan *password* untuk melihat perubahan terhadap nilai PSNR dari *stego image*

DAFTAR PUSTAKA

[1] Naor, M. dan Shamir, A., 1995, Visual Cryptography, Advances in Cryptology-Eurocrypt'94
[2] Park, G. D., Yoon, E. J dan Yoo, 2008, A New Copyright Protection Scheme with Visual Cryptography, Future Generation Communication and Networking Symposia (FGCNS)
[3] Wang D, Yi, F. dan Li, X., 2009, On General Construction for Extend Visual Cryptography Schemes
[4] Liu, X., Chen, M. dan Zhang, Y., 2013, A New Color Visual Cryptography Scheme with Perfect Contrast, 8th International Conference on Communication and Networking in China, http://www.computer.org/csdl/proceedings/chinacom/2013/9999/00/06694638.pdf
[5] Li, P., Kong, Q. dan Ma, Y., 2014, Image Secret Sharing and Hiding with Authentication Based on PSNR Estimation, JIHMSP, http://bit.kuas.edu.tw/~jihmsp/2014/vol5/JIH-MSP-2014-03-003.pdf
[6] Plataniotis, K.N. dan Venetsanopoulos, A.N, 2000, Color Image Processing and Application, Berlin Heidelberg New York
[7] Kaur, G. dan Deep, E. 2015, To Study Scope of Data Hiding in Various Image Color Models, IJRE, vol. 2, 2027 – 2029, http://www.ijtre.com/manuscript/2015020962.pdf
[8] Kaur, G. dan Deep, E. 2015, HSI Color Space Conversion Steganography using Electric Curve, IJIAACS, vol. 4, 63 – 67, http://www.academicscience.c~er/f201506141434302413.pdf

[9] Muhammad, K., Ahmad, J., Farman, H., Zubair, M., 2015, A Novel Image Steganographic Approach for Hiding Text in Color Image using HSI Color Model, http://arxiv.org/ftp/arxiv/papers/1503/1503.00388.pdf

[10] Kandar, S. dan Maiti, A., 2011, K-N Secret Sharing Visual Cryptography Scheme For Color Image Using Random Number, International Journal of Engineering Science and Technology (IJEST), vol 3, 1851-1857: http://www.ijcaonline.org/volume25/number11/pxc3874377.pdf