Implementasi Kriptografi Visual Berwarna dengan Menciptakan *Share* dengan Model Warna HSV

Randi Chilyon Alfianto | 13513087
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
randichil@gmail.com

***Abstrak*—Kriptografi visual merupakan metode dari pengembangan teknik kriptografi yang digunakan untuk berbagi pesan rahasia dengna menggunakan citra yang terenkripsi dan dapat dipecahkan menggunakan mata manusia. Dalam kriptografi visual berwarna, penggunaan berbagai macam model warna akan menghasilkan hasil citra yang berbeda-beda. Dalam *paper* ini akan dibahas mengenai penggunakan model warna HSV (*Hue, Saturation, Value)* yang diimplementasikan dalam kriptografi visual berwarna.**

Keywords—kriptografi visual, model warna HSV, secret sharing

I. PENDAHULUAN

Pada zaman ini, perkembangan teknologi sudah membawa perubahan pada manusia baik dari segi gaya hidup maupun kebiasaan. Kemudahan dalam mengakses informasi saat ini mengharuskan kita untuk mengamankan informasi rahasia yang akan kita bagikan kepada orang lain. Salah satu teknik pengamanan yang dapat dilakukan adalah dengan menggunakan teknik kriptografi. Penggunaan kriptografi dimaksudkan untuk meningkatkan keamanan dalam pembagian informasi dari satu orang kepada orang lain.

Perkembangan kriptografi saat ini juga sudah sangat maju. Saat ini, penggunaan kriptografi telah memasuki era kriptografi modern. Kriptografi modern menggunakan gagasan yang sama seperti kriptografi klasik, namun penekanannya berbeda. Dalam kriptografi klasik, penggunaan algoritma yang sederhana memungkinkan ciphertext dapat dipecahkan dengan mudah. Oleh karena itu, diciptakan kriptografi modern agar kriptanalis sulit untuk memecahkan ciphertext yang berhasil dibuat. Kriptografi modern biasanya beroperasi dalam bit.

Salah satu jenis kriptografi modern adalah kriptografi visual. Kriptografi visual merupakan suatu teknik yang menggunakan informasi visual (citra, text, dll) untuk dienkripsi dengan cara tertentu dan hanya dapat didekripsi oleh manusia dengan menggunakan penglihatan. Kriptografi visual akan menghasilkan n *shares* yang merupakan citra yang terlihat *noise*. Teknik ini ditemukan oleh Moni Naor dan Adi Shamir pada tahun 1994[1]. Mereka mendemonstrasikan skema *secret sharing* visual, di mana sebuah citra dibagi menjadi n *shares* dan hanya orang yang memiliki n *shares* tersebut dapat mendekripsi citra tersebut, sedangkan orang lain yang hanya memiliki n-1 *shares* tidak mendapatkan apapun dari citra yang dimilikinya. Setiap *share* dicetak dalam tingkat transparan yang berbeda, dan proses dekripsi dilakukan dengan menggabungkan semua *shares* yang ada (*overlay*). Ketika seluruh *shares* telah digabungkan satu sama lain dan saling menimpa, citra asli akan dapat terlihat[2][3].

Pada awalnya kriptografi visual diciptakan hanya untuk citra yang berwarna hitam-putih saja. Seiring berjalannya waktu setelah *paper* mengenai kriptografi visual dipublikasi, banyak peneliti yang melakukan penelitian dalam bidang ini. Banyak teknik kriptografi visual yang bermunculan setelah itu, dimulai dari citra hitam-putih, berkembang menjadi citra *greyscale*, dan untuk citra berwarna. Pada zaman sekarang, telah ditemukan teknik kriptografi visual yang dapat menghasilkan *share* yang memiliki makna, tidak hanya merupakan *noise*.

Dalam *paper* ini tidak akan dihasilkan suatu teknik kriptografi visual yang baru. *Paper* ini akan dijelaskan mengenai implementasi dari kriptografi visual berwarna yang menggunakan model warna HSV (*Hue, Saturation, Value)*. Dalam hal ini, akan digunakan metode kriptografi visual berwarna yang diciptkana oleh Young-Chang Hou pada tahun 2002 yang akan menghasilkan skema (2, 2).

II. DASAR TEORI

A. Visual Cryptography

Kriptografi visual merupakan suatu teknik yang menggunakan informasi visual (citra, text, dll) untuk dienkripsi dengan cara tertentu dan hanya dapat didekripsi oleh manusia dengan menggunakan penglihatan. Kriptografi visual akan menghasilkan n *shares* yang merupakan citra yang terlihat *noise*. Teknik ini ditemukan oleh Moni Naor dan Adi Shamir pada tahun 1994[1]. Mereka mendemonstrasikan skema *secret sharing* visual, di mana sebuah citra dibagi menjadi n *shares* dan hanya orang yang memiliki n *shares* tersebut dapat mendekripsi citra tersebut, sedangkan orang lain yang hanya memiliki n-1 *shares* tidak mendapatkan apapun dari citra yang dimilikinya. Setiap *share* dicetak dalam tingkat transparan yang berbeda, dan proses dekripsi dilakukan dengan menggabungkan semua *shares* yang ada (*overlay*). Ketika seluruh *shares* telah digabungkan satu sama lain dan saling menimpa, citra asli akan dapat terlihat[2][3].

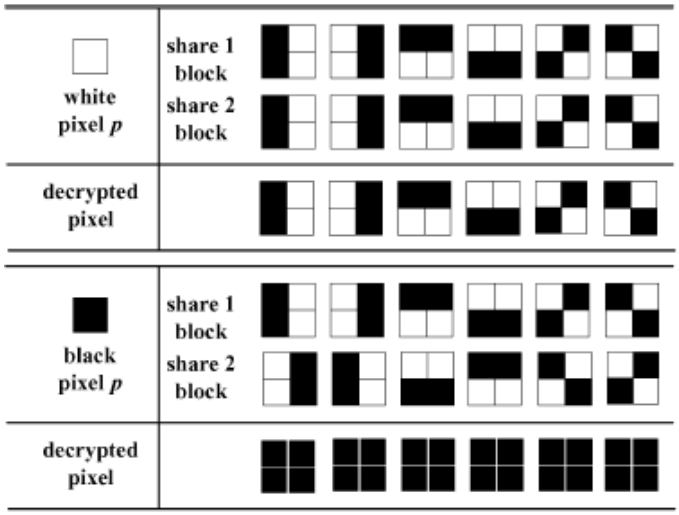
Pada awalnya kriptografi visual diciptakan hanya untuk citra yang berwarna hitam-putih saja. Seiring berjalannya waktu setelah *paper* mengenai kriptografi visual dipublikasi, banyak peneliti yang melakukan penelitian dalam bidang ini. Banyak teknik kriptografi visual yang bermunculan setelah itu,

dimulai dari citra hitam-putih, berkembang menjadi citra *greyscale*, dan untuk citra berwarna. Pada zaman sekarang, telah ditemukan teknik kriptografi visual yang dapat menghasilkan *share* yang memiliki makna, tidak hanya merupakan *noise*.

B. *Metode Kriptografi Visual*

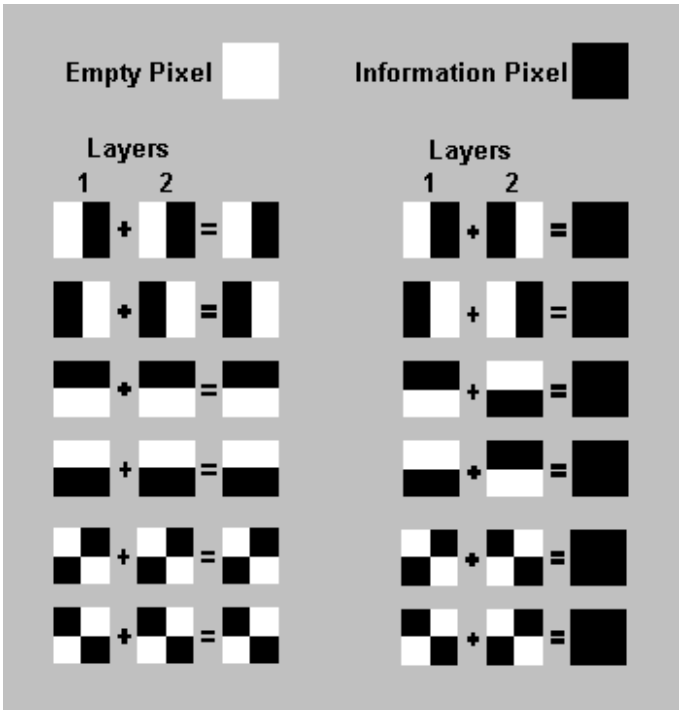
Kriptografi visual menggunakan citra dengan masing-masing pixel berwarna hitam atau putih. Pada model yang diperkenalkan oleh Shamir dan Naor, tiap pixel tidak direpresentasikan sebagai sebuah elemen matriks pada tiap *share*, melainkan menggunakan m elemen matriks. Jadi, setiap pixel dibagi menjadi m sub-pixel.

Metode standar kriptografi visual merujuk pada metode asli yang diajukan oleh Shamir dan Naor. Metode ini bekerja pada citra hitam-putih. Prosedur untuk kriptografi visual (2, 2) adalah sebagai berikut. Setiap pixel pada citra rahasia akan dienkripsi menjadi pixel 2x2 pada kedua *shares*, jadi tinggi dan lebar dari citra hasil enkripsi akan menjadi dua kali citra asli. Tabel sandi dapat dilihat pada gambar 1.



Gambar 1. Tabel Sandi Kriptografi Visual (Sumber: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Makalah2-2015/Makalah2_Kripto_IF4020_2015_018.pdf)

Gambar di bawah merupakan contoh dari model kriptografi visual. Pada gambar tersebut terlihat bahwa satu pixel pada gambar dapat dibentuk dari dua sub-pixel. Pixel dengan warna putih pada citra direpresentasikan dengan pixel berwarna setengah hitam dan setengah putih, sedangkan pixel dengan warna pada citra direpresentasikan dengan pixel berwarna hitam utuh. Karena representasi tersebut, pixel berwarna putih pada citra yang dihasilkan setelah melakukan dekripsi mengandung warna hitam. Hal ini akan mengurangi akurasi pada citra yang dihasilkan apabila dibandingkan dengan citra asli. Perubahan pixel putih menjadi setengah hitam dan setengah putih pada citra hasil disebut *noise*.



Gambar 2. Model Kriptografi Visual (Sumber : http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2012-2013/KriptografiVisual%20(2013).ppt)

C. *Model Warna*

Model warna merupakan model matematika abstrak yang mendeskripsikan warna dalam bentuk angka, biasanya direpresentasikan dalam tiga hingga empat nilai atau komponen warna. Ketika model ini dikaitkan dengan deskripsi yang tepat mengenai bagaimana komponen harus ditafsirkan, kumpulan warna yang dihasilkan disebut *color space*.

Terdapat beberapa jenis model warna yang telah ditemukan, antara lain:

- RGB (*Red*, *Green*, *Blue*)

  Model warna RGB merupakan suatu *additive color model*. Dalam hal ini, warna merah, hijau, dan biru dikombinasikan untuk mereproduksi spektrum warna yang luas. Tujuan utama dari model warna RGB adalah untuk menampilkan gambar dalam sistem elektronik, seperti layar TV dan monitor komputer dan juga digunakan dalam fotografi digital.

  Untuk menciptakan suatu warna dengan RGB, tiga cahaya (merah, hijau, biru) harus ditumpangkan. Tanpa intensitas, masing-masing dari ketiga warna dianggap sebagai warna hitam, sedangkan dengan intensitas penuh mengarahkan ke persepsi warna putih. Perbedaan intensitas menghasilkan *hue* dari warna, sementara perbedaan antara intensitas tertinggi dan terendah dari warna menghasilkan warna menjadi lebih atau kurang jenuh.

- CMYK (*Cyan, Magenta, Yellow*)

  Model warna CMYK merupakan *subtractive color model* yang terutama digunakan dalam percetakan, CMYK bekerja dengan sebagian atau seluruhnya *masking color* pada latar putih. Tinta cetak akan mengurangi cahaya yang seharusnya dipantulkan. Oleh karena itu, model warna ini disebut *"subtractive*" karena tinta mengurangi kecerahan dari latar putih dari empat warna: *cyan, magenta, yellow,* dan *black.*

  K pada bagian terakhir dari CMYK sering disalah artikan sebagai huruf terakhir dari kata *"black*" dan dipilih karena huruf B telah digunakan untuk merepresentasikan warna *"blue"*. Pernyataan itu merupakan hal yang salah, karena huruf K pada CMYK merupakan *"key"* karena dalam empat piring cetak warna *cyan, magenta, yellow* secara hati-hati diselaraskan dengan kunci piring cetak hitam. Warna hitam digunakan karena kombinasi dari ketiga warna utama (CMY) tidak menghasilkan warna hitam sepenuhnya.

- HSV (*Hue, Saturation, Value*)

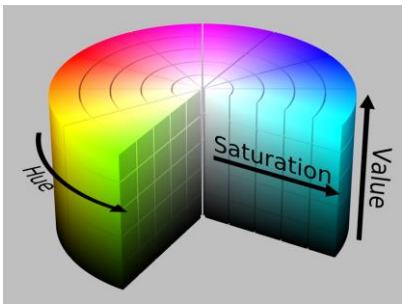
  HSV, yang merupakan singkatan dari *hue, saturation,* dan *value*, menggambarkan warna tiga dimensi. HSV berusaha menggambarkan hubungan antara warna, dan memperbaiki model warna RGB. Apabila HSV digambarkan sebagai roda, sumbu pusat bergerak dari warna putih yang berada di atas ke warna hitam yang berada di bawah, dengan warna-warna netral lain berada diantaranya. Sudut dari sumbu axis menggambarkan *hue*, jarak dari sumbu menggambarkan *saturation*, dan jarak sepanjang sumbu axis menggambarkan *value*.

- HSL (*Hue, Saturation, Lightness*)

  HSL, sama seperti HSV, merupakan representasi tiga dimensi dari warna. HSL merupakan singkatan dari *hue, saturation,* dan *lightness*. Model warna HSL memiliki keunggulan yang berbeda dengan model warna HSV, yaitu dalam komponen *saturation* dan *lightness* merentangkan keseluruhan rentang nilai.

D. Model Warna HSV (Hue, Saturation, Value)

HSV mendefinisikan sebuah tipe dari *color space*. Hal ini serupa dengan model warna RGB dan CMYK. Model warna HSV memiliki tiga komponen: *hue, saturation,* dan *value*.



Gambar 3. Model Warna HSV (Sumber: https://upload.wikimedia.org/wikipedia/commons/thumb/0/0d/HSV_color_solid_cylinder_alpha_lowgamma.png/800px-HSV_color_solid_cylinder_alpha_lowgamma.png)

- *Hue*

  Dalam HSV, *hue* merepresentasikan warna. Dalam model ini, *hue* merupakan sudut yang memiliki nilai antara 0 derajat hingga 360 derajat.

Angle	Color
0-60	Red
60-120	Yellow
120-180	Green
Angle	**Color**
180-240	Cyan
240-300	Blue
300-360	Magenta

Tabel 1. Tabel Representasi *Hue* Sebagai Warna (Sumber: http://www.tech-faq.com/hsv.html)

- *Saturation*

  Saturation mengindikasikan rentang warna abu-abu pada *color space*. Rentang tersebut bernilai 0 hingga 100%. Terkadang nilai tersebut dikalkulasi dari 0 hingga 1. Ketika nilai yang ditunjukkan adalah 0, maka warna yang ditunjukkan adalah abu-abu, sedangkan apabila nilai yang ditunjukkan adalah 1, warna yang ditunjukkan adalah warna utama. Suatu warna terlihat pudar dikarenakan tingkat *saturation* yang rendah, yang berarti warna tersebut mengandung lebih banyak abu-abu.

- *Value*

  Value merupakan tingkat kecerahan dari warna dan bervariasi dengan *saturation color*. *Value* memiliki rentang nilai dari 0 hingga 100%. Ketika *value* memiliki nilai '0', *color space* akan berwarna hitam total. Dengan penambahan nilai *value*, kecerahan dari *color space* akan meningkat dan akan menunjukkan berbagai warna.

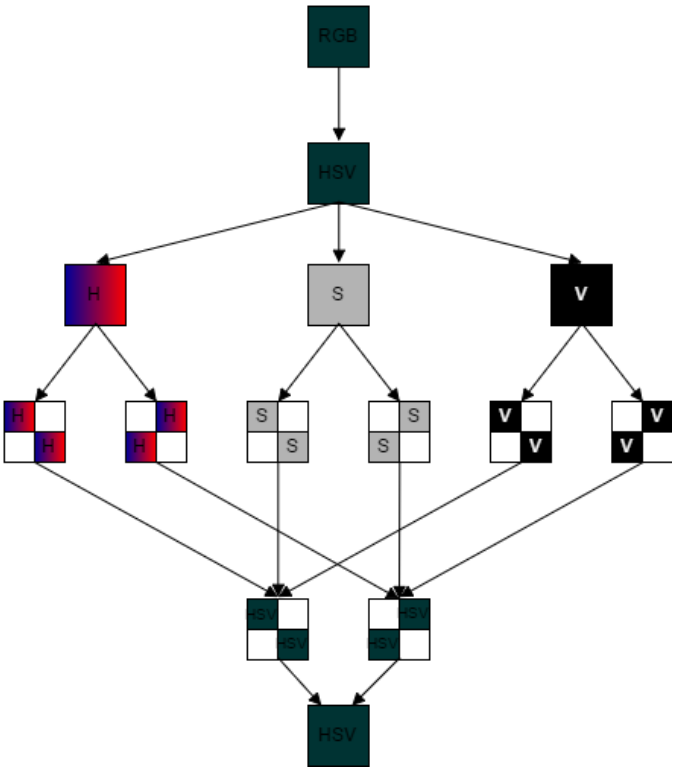
Model warna HSV sering digunakan untuk men-*generate computer graphics* berkualitas baik. Dalam istilah sederhana, HSV digunakan untuk memilih berbagai warna berbeda yang dibutuhkan untuk citra tertentu. Sebuah roda warna HSV digunakan untuk memilih warna yang diinginkan. Pengguna dapat memilih warna tertentu yang dibutuhkan pada roda warna HSV. Hal ini memberikan warna yang sesuai dengan persepsi manusia.

Kelebihan dari model warna HSV adalah *color space* pada HSV mirip dengan persepsi manusia terhadap warna. Model lain, selain HSL dan HSV, mendefinisikan warna dalam hubungan dengan warna utama. Warna pada HSV dapat dengan mudah dan jelas didefinisikan oleh persepsi manusia, tidak seperti pada model warna RGB dan CMYK.

III. METODE YANG DIAJUKAN

Dalam bab ini akan dijelaskan mengenai metode yang akan digunakan dalam mengimplementasikan kriptografi visual yang menggunakan model warna HSV. Langkah pertama yang

harus dilakukan adalah mendapatkan nilai RGB yang terdapat pada citra asli dan mengubah nilai tersebut menjadi model warna HSV. Selanjutnya dekomposisi citra sesuai dengan nilai model warna yang digunakan (dalam hal ini HSV). Langkah selanjutnya adalah lakukan enkripsi terhadap masing-masing citra H, S, dan V dengan menggunakan metode kriptografi visual standar yaitu metode kritpografi visual (2, 2) untuk citra *greyscale*, di mana setiap pixel akan menghasilkan pixel berukuran 2x2. Kemudian setiap pixel akan disandi menggunakan tabel sandi pada gambar 1. Setiap pixel akan menghasilkan empat subpixel lainnya. Untuk mendapatkan citra asli, lakukan *overlaping* terhadap setiap hasil *share* yang didapat.



Gambar 4. Diagram Proses Implementasi Kriptografi Visual dalam Model Warna HSV

Untuk mengubah nilai RGB menjadi HSV, terdapat formula khusus yang sering digunakan. Langkah-langkah pengubahan nilai RGB ke HSV antara lain:

1. Ubah rentang nilai RGB yang awalnya dari 0 hingga 255 menjadi 0 hingga 1 (pembagian dengan 255) dan tandai dengan variable R', G', dan H'.
2. Hitung Cmax dan Cmin dari R', G', dan H'.
3. Hitung delta dengan mengurangkan Cmax dengan Cmin.
4. Hitung nilai *Hue* dengan formula di bawah.
5. Hitung nilai *Saturation* dengan formula di bawah.
6. Nilai *Value* = nilai Cmax.

$$R' = R/255$$
$$G' = G/255$$
$$B' = B/255$$
$$Cmax = \max(R', G', B')$$
$$Cmin = \min(R', G', B')$$
$$\Delta = Cmax - Cmin$$

Formula untuk perhitungan *Hue*:

$$H = \begin{cases} 0^\circ & \Delta = 0 \\ 60^\circ \times \left(\frac{G'-B'}{\Delta} mod 6\right) & , C_{max} = R' \\ 60^\circ \times \left(\frac{B'-R'}{\Delta} + 2\right) & , C_{max} = G' \\ 60^\circ \times \left(\frac{R'-G'}{\Delta} + 4\right) & , C_{max} = B' \end{cases}$$

Formula untuk perhitungan *Saturation*:

$$S = \begin{cases} 0 & , C_{max} = 0 \\ \frac{\Delta}{C_{max}} & , C_{max} \neq 0 \end{cases}$$

Formula untuk perhitungan *Value*:

$$V = Cmax$$

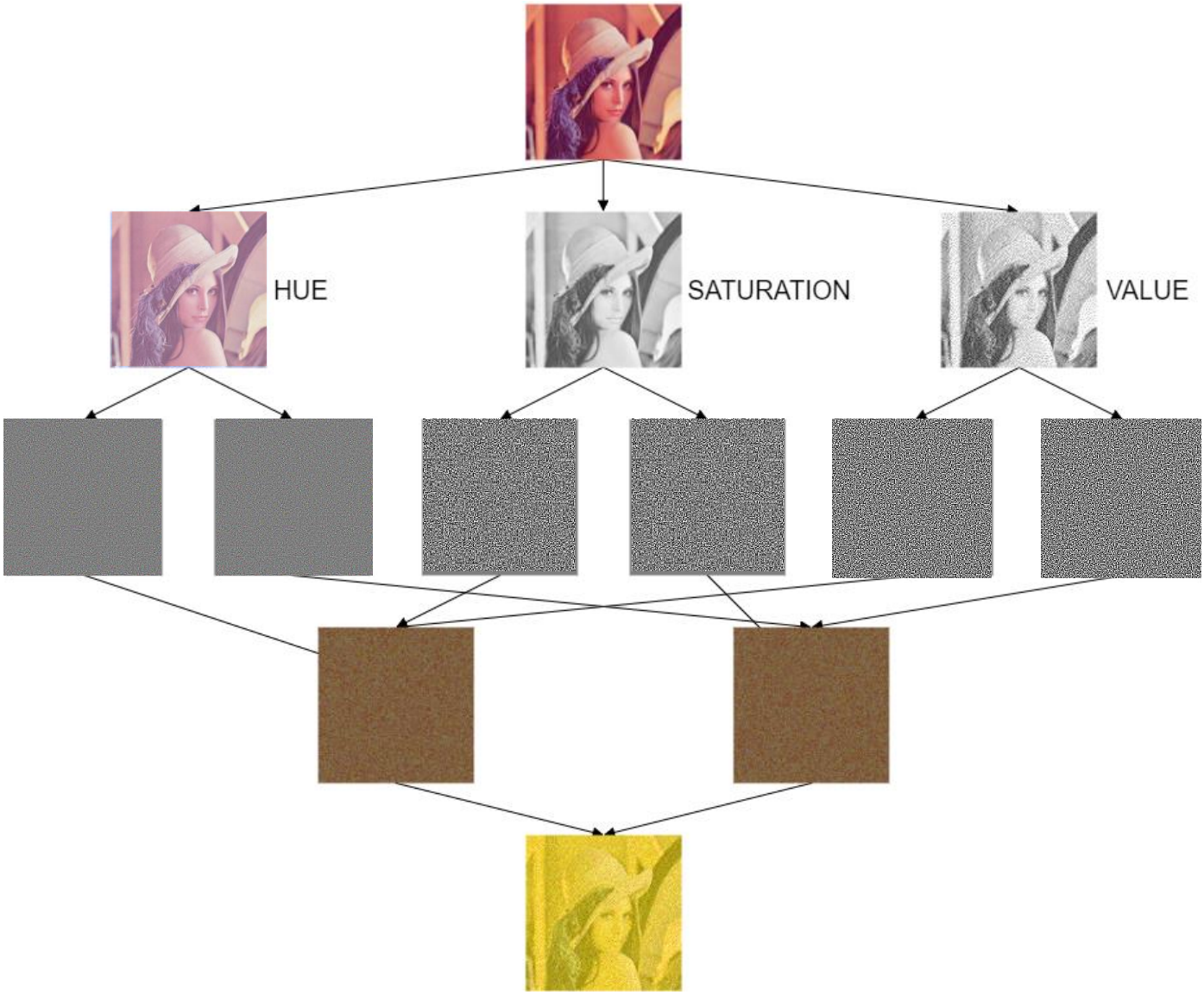
Sumber : http://www.rapidtables.com/convert/color/rgb-to-hsv.htm

IV. Hasil Eksperimen

Implementasi algoritma kriptografi visual pada *paper* ini menggunakan bahasa Java. Proses yang dilakukan antara lain:

1. Citra masukan yang diterima program dibaca sebagai *binary*.
2. Informasi mengenai nilai per pixel disimpan pada suatu *array* integer.
3. Nilai pixel pada citra kemudian diproses sesuai dengan metode yang dijelaskan pada bab III.
4. Citra yang telah diproses diubah kembali menjadi format citra semula untuk mendapatkan *share* yang dihasilkan.
5. Untuk proses penggabungan citra (dalam hal ini untuk mendapatkan hasil akhir), dilakukan proses OR untuk setiap *share* dan diubah kembali ke format citra semula sehingga didapatkan citra yang telah dikombinasikan dari *share-share* yang telah dihasilkan.

Dari hasil implementasi di atas, digunakan citra "lena.png" sebagai citra uji. Dari citra tersebut, didapatkan *share* dari masing-masing komponen dari model warna HSV, yaitu *hue*, *saturation*, dan *value*. *Share-share* tersebut kemudian disatukan menjadi 2 *share* yang masing-masing memiliki kombinasi yang berbeda. Setelah disatukan, didapatkan gambaran terhadap citra yang semula digunakan. Hasil eksperimen tersebut dapat dilihat pada gambar 5.



Gambar 5. Hasil Ekspreimen Kriptografi Visual dengan Model Warna HSV

Dari gambar di atas, dapat dilihat bahwa hasil eksperimen yang dilakukan menghasilkan citra yang memiliki kualitas yang kurang baik. Hasil perhitungan perbedaan akan dibahas pada bab analisis hasil berupa perhitungan PSNR. Walaupun memiliki kualitas yang kurang baik, namun hasil yang didapat masih menggambarkan citra asli yang digunakan.

V. ANALISIS HASIL

Terdapat beberapa faktor yang dapat dianalisis dari implementasi kriptografi visual menggunakan model warna HSV ini, antara lain:

1. Keamanan

   Suatu algoritma kriptografi visual dapat dikategorikan sebagai algoritma yang aman apabila kombinasi antara *share* dengan jumlah kurang dari jumlah *share* yang dihasilkan tidak menunjukkan gambaran apapun tentang citra asli. Dari hasil yang didapatkan pada eksperimen, dapat dilihat bahwa citra yang dihasilakan merupakan citra yang hanya menggambarkan *noise*. Hal ini menandakan bahwa algoritma kriptografi visual dengan model warna HSV tergolong aman.

2. Kualitas Citra yang Dihasilkan

   Dari citra yang terdapat pada gambar 5, dapat dilihat bahwa citra yang dihasilkan dari kombinasi antara *share* yang telah didapatkan dari algoritma kriptografi visual masih dapat dikenali oleh mata manusia sebagai citra yang mirip dengan citra asli yang digunakan. Namun, dari kualitas dapat dilihat perbedaan yang cukup jauh antara citra asli dengan citra hasil. Hal ini menandakan bahwa citra hasil dekripsi algoritma kriptografi visual dengan model warna HSV tidak baik digunakan untuk citra rahasia yang menganggap bahwa kualitas warna dari citra penting karena hal ini akan mengakibatkan kesalahan pesan yang didapat apabila pesan yang terdapat dalam citra tergambar dalam warna yang digunakan.

Perbedaan pada citra dapat dianalisis dengan perhitungan PSNR (*Peak signal-to-noise Ratio*). PSNR merupakan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya *noise* yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan decibel (db). PSNR digunakan untuk mengetahui perbandingan kualitas citra sebelum dan sesudah melalui kriptografi visual. Untuk menentukan PSNR, terlebih dahulu harus ditentukan nilai MSE (Mean Square Error). MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra hasil. Berikut ini adalah formula yang digunakan untuk menghitung MSE dan PSNR:

Formula untuk menghitung MSE:

$$MSE = \frac{1}{m\,n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Formula untuk menghitung PSNR:

$$\begin{aligned} PSNR &= 10 \cdot \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \\ &= 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \\ &= 20 \cdot \log_{10}(MAX_I) - 10 \cdot \log_{10}(MSE) \end{aligned}$$

Sumber: https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio

Perhitungan PSNR untuk citra hasil kriptografi visual dengan menggunakan model warna HSV adalah -34.17372. Dari hasil tersebut, terlihat bahwa masih terdapat perbedaan yang besar antara citra asli dengan citra yang dihasikan oleh algoritma kriptografi visual.

VI. Simpulan dan Saran

Kriptografi visual merupakan suatu algoritma yang berguna dalam pengiriman pesan rahasia menggunakan citra visual. Dari eksperimen yang telah dilakukan, dapat disimpulkan bahwa implementasi kriptografi visual menggunakan model warna HSV berhasil dilakukan. Hal ini menunjukkan bahwa algoritma ini dapat digunakan sebagai salah satu alternatif dalam pengiriman pesan rahasia menggunakan citra visual. Walaupun citra yang dihasilkan masih dapat dikenali secara visual, dari perhitungan PSNR, kualitas citra yang dihasilkan masih tergolong rendah. Hal ini menunjukkan bahwa algoritma ini tidak cocok untuk pengiriman pesan yang mementingkan kualitas citra yang dihasilkan. Selain itu, penggunaan *share* yang hanya menggambarkan *noise* akan menimbulkan kecurigaan dari pihak ketiga.

Untuk pengembangan selanjutnya, terdapat algoritma kriptografi visual yang lebih baik, yaitu kriptografi visual yang menghasilkan *share* yang juga memiliki makna. Algoritma ini sudah dikembangkan oleh Kang, InKoo et. al. dari Korea. Dengan menggunakan algoritma ini, citra yang dihasilkan akan memiliki kualitas yang lebih baik. Selain itu, *share* yang memiliki makna akan menghilangkan kecurigaan dari pihak ketiga.

Acknowledgment

Dengan diselesaikannya penulisan *paper* ini, penulis hendak mengucapkan puji dan syukur atas rahmat yang diberikan oleh Tuhan YME, sehingga penulisan *paper* ini dapat diselesaikan dengan baik dan tepat waktu. Selanjutnya, penulis juga ingin mengucapkan terima kasih kepada Bapak Rinaldi Munir selaku dosen mata kuliah IF4020 Kriptografi, yang telah memberikan pengetahuan mengenai kriptografi visual yang sangat berguna dalam penyelesaian *paper* ini. Penulis juga ingin mengucapkan terima kasih kepada teman-teman yang secara langsung ataupun tidak langsung membantu dalam penulisan *paper* ini.

Referensi

[1] Naor, M. and A. Shamir. Visual cryptography, Advances in cryptology. Eurocrypt '94 Proceeding LNCS, 950:1–12, 1995.

[2] Verheul, E.R. and H.C.A.van Tilborg. Constructions and properties of k out of n visual secret sharing schemes. Design Codes and Cryptography, 11(2):179–196, 1997.

[3] Ateniese, G., C. Blundo, A. De Santis, and D. R. Stinson. Extended capabilities for visual cryptography. Theoretical Computer Science, 250:143–161, 2001.

[4] http://www.slideshare.net/junaidikun/algoritma-kriptografi-modern (diakses pada 14 Mei 2016)

[5] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2012-2013/KriptografiVisual%20(2013).ppt (diakses pada 14 Mei 2016)

[6] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Makalah2-2015/Makalah2_Kripto_IF4020_2015_005.pdf (diakses pada 14 Mei 2016)

[7] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Makalah2-2015/Makalah2_Kripto_IF4020_2015_018.pdf (diakses pada 14 Mei 2016)

[8] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Makalah2-2015/Makalah2_Kripto_IF4020_2015_035.pdf (diakses pada 14 Mei 2016)

[9] http://www.designersinsights.com/designer-resources/understanding-color-models (diakses pada 14 Mei 2016)

[10] http://www.tech-faq.com/hsv.html (diakses pada 14 Mei 2016)

[11] http://www.rapidtables.com/convert/color/rgb-to-hsv.htm (diakses pada 15 Mei 2016)

[12] https://github.com/azaky/VisualCryptography (diakses pada 15 Mei 2016)

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiarisme.

Bandung, 17 Mei 2016

Randi Chilyon Alfianto
13513087