Studi dan Eksperimen terhadap Kombinasi Warna untuk Kriptografi Visual Warna Kromatik

Ibnu Alam 13506024

Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung
Jl. Ganeca 10, Bandung, Jawa Barat
e-mail: if16024@students.if.itb.ac.id

Abstrak

Makalah ini menyajikan sebuah studi terhadap sifat-sifat warna untuk dikembangkan pada kriptografi visual dan mengusulkan sebuah rancangan untuk dasar pembagian gambar berwarna dan enkripsinya. Sebagai eksperimen sederhana, pendalaman yang dilakukan hanya pengembangan kriptografi warna yang membagi gambar asli menjadi 2 gambar *cipher* saja. Penulis mengharapkan ide ini dapat dikembangkan menjadi teknik ekstraksi warna menjadi subpiksel yang efektif sehingga dapat menghasilkan enkripsi yang baik tetapi kualitas gambar hasil penumpukan 2 gambar cipher tersebut tidak terlalu rusak karena *noise* yang dihasilkan pada proses enkripsi.

Latar Belakang

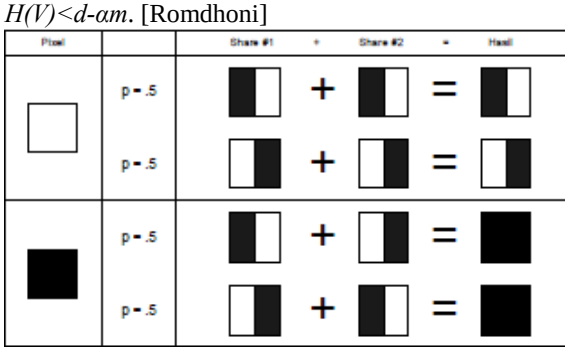
Sejak diperkenalkannya kriptografi visual oleh Moni Naor dan Adi Shamir pada tahun 1994 dalam *EUROCRYPT'94,* kriptografi visual masih belum bisa diaplikasikan ke dalam gambar berwarna secara efektif. Berbeda dengan kriptografi visual hitam putih, yang cukup diwakili oleh dua warna, sehingga bisa diwakilkan dengan angka biner, warna kromatik memiliki *range* nilai yang jauh lebih luas dibandingkan dengan hitam-putih. Superposisi warna juga menghasilkan warna lain yang tidak mudah diperhitungkan seperti hitam-putih, yang akan menjadi warna hitam pada semua kombinasi kecuali putih-putih. Hal inilah yang penulis anggap sebagai sumber kesulitan pengembangan kriptografi visual warna kromatik.

Kriptografi Visual Hitam Putih

Kriptografi Visual adalah teknik untuk menyamarkan sebuah informasi visual, bisa berupa gambar, tulisan, grafik, atau lainnya, dengan enkripsi sedemikian rupa sehingga pendekripsian bisa dilakukan tanpa komputasi, cukup dengan melihat memakai mata sendiri. Implementasi yang sudah berhasil sampai saat ini adalah dengan membagi sebuah gambar menjadi beberapa bagian, dimana jika masing-masing bagian dilihat tersendiri tidak akan memberikan informasi, tetapi jika ditumpuk dengan tepat akan menghasilkan informasi yang dibuat pada gambar aslinya.

Moni Naor dan Adi Shamir pertama kali mengemukakan ide ini berupa citra biner, yang hanya terdiri atas warna hitam dan putih. Setiap *pixel* pada citra rahasia akan diperlakukan secara terpisah. Masing-masing *pixel* tersebut akan muncul dalam *n* buah variasi, dinamakan *share*. Setiap *share* memiliki *m* buah *subpixel* berwarna hitam dan putih yang dicetak secara berdekatan sehingga sistem penglihatan manusia akan memandang rata distribusi warna hitam dan putih tersebut. Hasilnya dapat dimodelkan dalam matriks *Boolean S* berukuran *nxm*, di mana *S[i,j] = 1*, jika dan hanya jika *subpixel* ke-*j*, pada *share* ke-*i* berwarna hitam. Jumlah baris pada matriks tersebut menyatakan banyaknya *share* dihasilkan dan jumlah kolom menyatakan jumlah *subpixel* pada masing-masing *share*.

Dari model tersebut, penumpukan *share* dapat dianggap sebagai hasil fungsi *OR* pada baris-baris terkait dari matriks *S* tersebut. Hal ini sesuai bahwa warna hitam pada satu *subpixel* tidak dapat dihilangkan oleh warna putih pada *subpixel* lain yang bertumpuk dengannya. Tingkat keabu-abuan yang dihasilkan dari penumpukan ini akan dianggap sebagai warna hitam jika memenuhi bobot $H(V) \geq d$ dan dianggap warna putih jika memenuhi bobot $H(V) < d - \alpha m$. [Romdhoni]



***Share* Kriptografi Visual Biner**

Kriptografi Visual Berwarna

Pada kriptografi visual yang menggunakan warna yang banyak, kerumitan meningkat jauh meningkat karena banyak sekali nilai warna yang akan dikombinasikan, bukan hanya hitam dan putih.

Citra berwarna sulit untuk dienkripsi karena dua hal, yakni:

1. Sepertinya tidak mungkin untuk mengenkripsi sebuah citra berwarna dengan pengembangan *pixel* yang kecil.

2. Faktor kecerahan citra hasil rekonstruksi dibandingkan dengan citra aslinya.

Definisi Solusi:
Anggap kita dapat membangun seluruh warna pada citra rahasia (citra plain) dengan menggunakan himpunan warna $C = \{c1, c2, ..., cJ\}$. Sebuah koleksi dari J matriks Gi berukuran nxm dengan masukan berasal dari himpunan $\{0, 1, c1, c2, ..., cJ\}$ membangun sebuah skema visual kriptografi (k,n) jika memenuhi persyarat-persyaratan berikut ini:

1. Untuk sembarang i, di mana $(1 \leq i \leq J)$, vektor sepanjang m yang merupaka n hasil penumpukan sembarang k baris dari Gi minimal sejumlah Li berwarna ci; masing-masing warna cj lainnya muncul maksimal Uij dalam vektor ini.

2. Untuk sembarang subhimpunan $\{i1, i2, ..., ij\}$ dari $\{1, .., n\}$, submatriks Gi' diperoleh dengan melakukan restriksi masing-masing Gi pada baris-baris $i1, i2, ..., ij$ adalah identik sama dengan sebuah permutasi kolom [Romdhoni]

Enkripsi Kriptografi Visual Berwarna

Metode yang sudah dikembangkan sekarang sebenarnya sudah dapat mengenkripsi gambar berwarna walaupun dengan berbagai restriksi dan reduksi kualitas.

Secara umum, metode ini terbagi pada dua langkah, pertama adalah preproses untuk memberikan restriksi berupa pengelompokan warna-warna yang memiliki *range* di luar nilai yang ditentukan menjadi warna terdekat.

Gambar sebelum preproses

Langkah-langkah preproses:

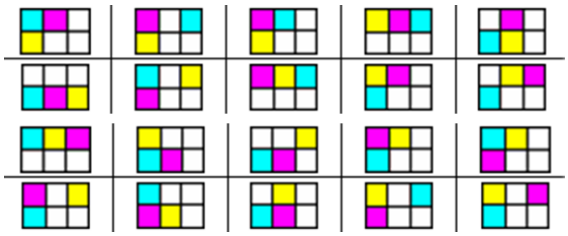
1. Tentukan variabel C, besar kluster warna
2. Ambil k dimana $(k-1)^3 < C < k^3$
3. Ruang warna RGB dibagi menjadi k^3 blok
4. Tiap titik tengah dari blok ditentukan menjadi titik awal dari rata-rata C (C-means)
5. Cari nilai C-means dengan kerangka *Euclid*
6. Setelah memproses C-means, urutkan menurun kluster-kluster berdasarkan nomor piksel dari kluster
7. Pilih warna-warna C pertama sebagai waran representasi
8. Ubah kembali warna piksel ke warna representasi terdekat dengan memakai kerangka *Euclid.*

Gambar setelah preproses

Kedua adalah enkoding dengan cara perhitungan representasi gambar dengan elemen warna CMYW (cyan, magenta, kuning, putih).

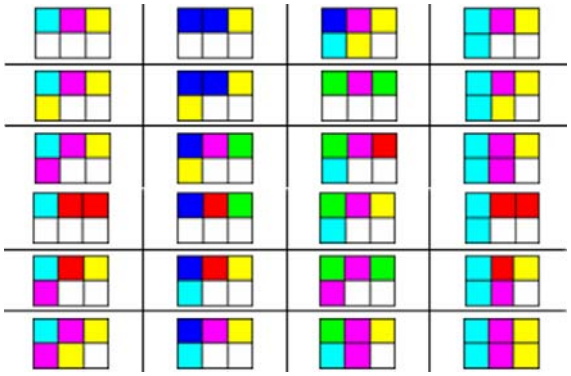
Langkah-langkah enkoding:

- Tentukan tinggi dan lebar dari pola
- Batasan
  - Hanya menggunakan warna CMYW
  - Jumlah warna CMY harus sama (W tidak harus)
- Hasilkan semua pola yang mungkin
  - Contoh: lebar = 3, tinggi = 2, terdapat 3!2! = 6x5x4 = 120 permutasi



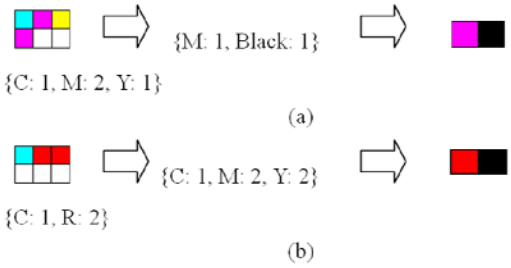
Beberapa contoh permutasi 3x2

- Hasilkan kombinasi dari penumpukan 2 pola dari semua pola yang ada.
- Pakai hukum eliminasi untuk menentukan warna pendekatan.



Kombinasi yang mungkin dari penumpukan 2 pola

- Hukum Eliminasi
  - Pada tiap kombinasi, pisahkan menjadi elemen {C, M, Y, W}. Hitung jumlah tiap warna
  - Jika salah satu (C, M, Y) berjumlah tiga dalam satu kombinasi, kurangi satu dan tambahkan 1 piksel warna hitam. Ulangi sampai tak bisa dilakukan eliminasi lagi
  - Jika tersisa satu C, M, Y, maka warna pendekatan adalah warna tersebut. Jika tersisa dua, warna pendekatan adalah gabungan dari dua warna tersebut



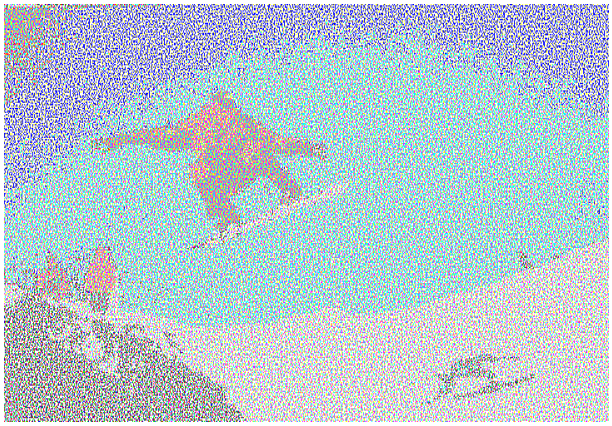
- Dasar hukum eliminasi adalah hanya boleh ada satu warna pendekatan (salah satu dari C, M, Y, R, G, B) yang tersisa
- Dalam tiap kombinasi, nilai RGB pada warna pendekatan adalah (R_i, G_i, B_i)dan nilai HSI (*Hue, Saturation, Intensity*) adalah (H_i, S_i, I_i)
- Intensitas akan dipengaruhi oleh piksel hitam yang dihasilkan, nilai I_i harus dihitung ulang

$$I' = 255 - 255 \times \frac{number\ of\ black\ pixel}{number\ of\ black\ pixel + number\ of\ white\ pixel}$$

- Konversi (H_i, S_i, I_i') menjadi (R_i', G_i', B_i') sebagai warna pendekatan yang baru
- Jika nilai dari salah satu (R_i', G_i', B_i') dalam satu kombinasi adalah sama, kombinasi itu dimasukkan kedalam kelompok *gray (*kelabu), selain itu dikelompokkan sebagai warna.
- Pada gambar setelah preproses, tiap piksel dihitung perbedaan relatif *rd* antara (R, G, B) :

$$rd = |R - G| + |G - B| + |R - B|$$

- Jika $rd >= 80$, digolongkan menjadi titik warna, selain itu menjadi titik kelabu
- Jika sebuah piksel tergolong kelabu, dipilih kombinasi dengan jarak terpendek
- Selain itu, grup warna, kombinasi yang dipakai adalah yang memiliki jarak *hue* terpendek.
- Acak posisi piksel dalam kombinasi. Dari kombinasi didapatkan pola 1 dan dimasukkan ke posisi yang bersesuaian pada *share* 1, 2. Ulangi untuk semua piksel.



Gambar setelah enkripsi

Kombinasi Warna

Salah satu hal yang perlu diperhatikan dalam kriptografi visual berwarna adalah warna memiliki sifat dapat saling bercampur. Sifat ini datang dari bentuk sebenarnya warna, yaitu cahaya tampak, merupakan gelombang. Tiap warna merupakan frekuensi berbeda dari gelombang cahaya. Pencampuran warna terjadi karena superposisi dua gelombang cahaya menghasilkan cahaya dengan frekuensi berbeda.

Hal penting pertama adalah adanya dua sistem cahaya bercampur. Pertama adalah warna **aditif**, yaitu warna yang pencampurannya akan menggeser warna dari hitam ke putih. Makin banyak warna dicampur, maka warna akan semakin terang dan akhirnya menjadi putih. Sistem inilah yang ada pada monitor komputer atau televisi. Kedua adalah warna **subtraktif**, yaitu warna yang pencampurannya akan menggeser warna dari putih ke hitam. Pencampuran lebih banyak warna akan menggelapkan gambar dan akhrinya menjadi warna hitam. Sistem ini ada pada cat, lukisan, dan hasil print.

Berhubung kriptografi visual menggunakan tinta printer untuk mencetak citra ke atas kertas transparansi, yang perlu diperhatikan adalah sifat subtraktif dari warna.

Skema warna aditif

Skema warna subtraktif

Komplemen Warna

Warna yang jika dicampurkan keduanya dalam ukuran yang tepat akan menghasilkan warna netral seperti hitam, abu-abu, atau putih.

Contohnya adalah merah dan cyan, hijau dan magenta, biru dan kuning.

Warna yang saling berseberangan dalam lingkaran adalah komplemen warna

Percobaan Penggunaan Kombinasi Warna

Percobaan ini mencoba menggunakan kombinasi warna yang tepat, mengikuti sifat-sifat warna yang ada, dibagi pada 2 citra *cipher*, untuk menghasilkan kembali citra yang bermakna.

Langkah percobaan:

1. Gambar yang dipakai berupa gambar *P* dalam format bmp dengan kedalaman warna 256-bit.
2. *P* akan dipisah menjadi 2 bagian berdasarkan *channel* CMYK menjadi *P1* dan *P2*.
3. Setelah itu 2 gambar tersebut akan dikonversi ke grayscale, *G1* dan *G2*.
4. *G1* dan *G2* akan displit secara grayscale dengan program kriptografi visual, *C11, C12, C21, C22*.
5. Gambar hasil split akan diubah kembali menjadi tone sebenarnya pada mode CMYK, C11 dan C12 mengikuti G1, C21 dan C22 mengikuti G2.
6. Semua gambar akan ditumpuk untuk melihat hasilnya.

Berikut eksperimen:

Citra P

Citra G1

Citra G2

Hasil Eksperimen

Penulis menggunakan program Visual Cryptography Kit yang ditulis dalam bahasa Python. Sayangnya program tersebut gagal mengkonversi citra-citra yang disediakan dalam percobaan. Kesalahan terletak pada kode program yang memerlukan tambahan modul untuk memenuhi spesifikasi yang diberikan. Percobaan ini gagal.

Kesimpulan

1. Kriptografi visual menghasilkan citra yang terenkripsi tetapi tidak butuh kalkulasi untuk mendekripsinya, cukup dengan menumpuk citra-citra ciphernya.
2. Pengenkripsian citra berwarna masih dapat dikembangkan untuk mendapatkan hasil dekripsi yang lebih jelas dan bersih gambarnya.

Saran

Penulis berharap tulisan ini dapat memberi inspirasi kepada para kriptografer-kriptografer di masa mendatang. Mungkin kesalahan yang tidak bisa penulis atasi dapat diatasi di masa mendatang.

Daftar Pustaka

[1] Visual Cryptography, http://en.wikipedia.org/wiki/Visual_cryptography
[2] Complementary Color, http://en.wikipedia.org/wiki/Complementary_color
[2] Martin, Ricardo. 1995. *Visual Cryptography: Secret Sharing without a Computer*. GWU Cryptography Group.
[3] Romdhoni, Arif. 2007. *Kriptografi Visual pada Citra Biner dan Citra Berwarna serta Pengembangannya dengan Steganografi dan Fungsi XOR.*
[4] 龔信嘉, *Color Visual Cryptography*. TWISC.