

# Pemanfaatan Kriptografi Visual untuk Pengamanan Foto pada Sistem Operasi Android

Raka Mahesa - 13508074

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia

the\_legacy99@hotmail.com

**Abstrak**—Akhir-akhir ini sedang marak berita mengenai aplikasi *mobile* untuk Android ataupun iOS yang rupanya mengunggah data pribadi penggunaannya ke server pembuat aplikasi tersebut. Hal ini merupakan salah satu contoh pelanggaran privasi karena mungkin saja terdapat berbagai data milik pengguna yang tidak boleh diketahui orang lain. Apalagi ponsel merupakan perangkat yang cukup personal sehingga besar kemungkinan terdapat data yang hanya boleh diketahui pemiliknya saja. Foto-foto merupakan salah satu contoh data yang mungkin cukup personal, apalagi ponsel zaman sekarang selalu dilengkapi dengan kamera. Karena itu penulis mencoba mengaplikasikan kriptografi visual, sebuah metode kriptografi yang dikhususkan untuk mengenkripsi gambar, untuk mengamankan berbagai foto atau gambar yang terdapat pada ponsel Android agar tidak jatuh ke tangan yang salah.

**Kata Kunci**—Enkripsi gambar, Android, Kriptografi Visual.

## I. PENDAHULUAN

Kriptografi merupakan sebuah ilmu tentang bagaimana cara menjaga agar data yang dikirimkan oleh pengirim dapat mencapai penerima pesan tanpa mendapat gangguan dari pihak ketiga.

Istilah kriptografi sendiri berasal dari dua buah kata dalam bahasa Yunani yaitu kata "cryptos" yang berarti rahasia dan kata "graphein" yang berarti tulisan. Dengan demikian, dari segi bahasa, kriptografi memiliki arti tulisan rahasia. Istilah tersebut amat tepat ketika kriptografi mulai digunakan, karena pada zaman-zaman tersebut pengiriman pesan dilakukan menggunakan tulisan sehingga untuk menjaga keamanannya, tulisan tersebut harus dirahasiakan. Dewasa ini, pesan atau data dapat memiliki berbagai wujud seperti tulisan, gambar, suara ataupun bentuk lainnya, sehingga kriptografi bukan hanya ilmu mengenai cara membuat tulisan rahasia saja tetapi juga ilmu menjaga kerahasiaan data dalam wujud lainnya.

Selain perubahan pada wujud pesan yang perlu dirahasiakan, saat ini kriptografi juga memiliki tujuan lain selain menjaga kerahasiaan pesan, yaitu menjaga kerahasiaan data pribadi. Kedatangan teknologi internet telah memudahkan manusia untuk mencari informasi mengenai orang lain, sehingga zaman sekarang ini,

kerahasiaan diri merupakan suatu hal yang amat penting.

Seiring dengan berkembangnya zaman, berbagai macam tindak kejahatan baru yang memanfaatkan teknologi modern pun muncul. Salah satu tindak kejahatan yang muncul pada zaman modern ini dan menjadi marak ialah pencurian data pribadi. Data pribadi yang diincar biasanya merupakan data kartu kredit, password, ataupun alamat e-mail karena data tersebut mudah memberikan keuntungan bagi sang pencuri. Karena hal tersebut, kini data-data yang berharga itu biasanya sudah dienkripsi sehingga sulit untuk dicuri.

Di zaman *smartphone* ini, banyak orang yang menyimpan data pribadi pada perangkat seluler miliknya. Hal ini menjadikan *smartphone* sebagai barang incaran para pencuri data, apalagi masyarakat masih terbiasa dengan ponsel zaman dahulu yang tidak terhubung dengan internet dan lebih aman dari pencurian data pribadi. Selain itu ekosistem *smartphone* sekarang memungkinkan penggunaannya untuk memasang berbagai aplikasi pada perangkat selulernya sehingga memudahkan pencuri data untuk mendistribusikan aplikasi jahat (*malware*) dengan tujuan mendapatkan data penggunaannya. Bahkan kini aplikasi yang valid pun mengambil data pemakainya dan menggunggahnya ke server agar pembuat aplikasi tersebut dapat memahami konsumennya lebih jauh.

Dengan makalah ini, penulis mencoba untuk membantu menjaga kerahasiaan pemakai *smartphone*, khususnya *smartphone* Android, dengan meng-enkripsi berbagai gambar yang terdapat pada perangkat tersebut agar gambar tersebut tidak dimengerti oleh para pengambil data.

## II. GAMBAR

Secara umum, gambar pada komputer terbagi menjadi dua jenis, yaitu gambar berbasis bitmap dan gambar berbasis vector. Gambar vector merupakan gambar yang terbuat dari kumpulan elemen yang didefinisikan dengan formula tertentu, misalnya elemen lingkaran, kurva dan lainnya. Sementara gambar bitmap terdiri dari kumpulan petak-petak berwarna yang disebut dengan nama pixel. Makalah ini hanya akan membahas mengenai gambar berbasis bitmap.

File berisi gambar bitmap dapat dibuat dengan berbagai tipe dan format. Ada gambar dengan format JPG, PNG, GIF, dan masih banyak format-format lain yang tidak umum seperti PSD atau TIF. Variasi gambar bukan hanya pada formatnya, bahkan sebuah file PNG dapat memiliki beberapa cara untuk menyimpan data gambarnya, misalnya PNG 16-bit, PNG 24-bit, ataupun PNG 32-bit yang memiliki jumlah kombinasi warna yang berbeda.

Meskipun gambar bitmap memiliki banyak format dan variasi, pada dasarnya gambar bitmap tetap merupakan kumpulan pixel berwarna. Warna pada pixel dapat direpresentasikan dengan berbagai cara, salah satu cara yang paling umum ialah dengan RGB. Representasi warna dengan RGB dilakukan dengan membagi warna menjadi tiga buah komponen, yaitu warna merah (R), hijau (G), dan biru (Blue) dimana kombinasi ketiga warna ini dapat menghasilkan hampir semua warna yang ada (terdapat lebih dari 16 juta kombinasi warna yang dapat dihasilkan dari ketiga komponen warna tersebut). Setiap komponen warna dapat memiliki nilai antara 0-255 dimana masing-masing komponen memiliki ukuran 8 bit.

Cara lain dalam merepresentasikan warna ialah dengan menggunakan format CMY. Apabila representasi RGB banyak digunakan oleh layar monitor, maka format CMY banyak digunakan oleh *printer*. Konsep format CMY sama dengan format RGB dimana setiap pixel merupakan kombinasi warna nila/cyan (C), Magenta (M), dan kuning (Y), hanya saja bila format RGB merupakan format bersifat aditif dimana warna yang dihasilkan merupakan hasil penambahan warna, maka format CMY bersifat subtraktif, dimana warna yang dihasilkan merupakan hasil pengurangan. Hal ini jelas terlihat pada penggabungan warna dasar, dimana penggabungan warna dasar pada model aditif menghasilkan warna putih, sementara penggabungan warna dasar pada model subtraktif menghasilkan warna hitam.

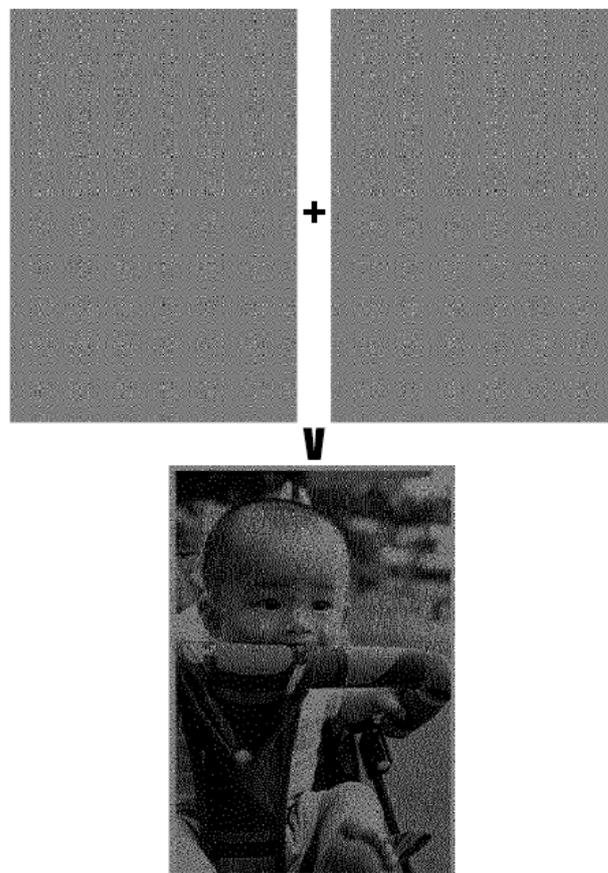
Karena format CMY dan RGB merupakan warna-warna yang komplementer, maka nilai CMY dari suatu warna yang menggunakan format RGB mudah didapat. Nilai CMY tersebut bisa didapat dengan mengaplikasikan rumus  $C = 255 - R$ ,  $M = 255 - G$ , dan  $Y = 255 - B$ . Sehingga sebuah pixel yang memiliki nilai warna (255, 255, 255) pada format RGB akan memiliki warna putih, sementara pada format CMY akan memiliki warna hitam.

### III. KRIPTOGRAFI VISUAL

Kriptografi visual merupakan sebuah teknik kriptografi yang digunakan untuk mengenkripsi sebuah informasi visual (biasanya merupakan gambar). Kriptografi visual berbeda dengan berbagai teknik kriptografi lainnya karena pendekripsian hasilnya memanfaatkan kemampuan mata manusia untuk mengenali bentuk-bentuk dan simbol-simbol tertentu. Karenanya, dekripsi pada kriptografi visual bukan merupakan sebuah operasi yang membutuhkan komputer sehingga lebih fleksibel dan dapat digunakan tanpa fasilitas yang memadai. Selain itu, hasil dekripsi yang dihasilkan juga cenderung sulit dideteksi maknanya oleh komputer (karena komputer

tidak memiliki kemampuan visual sebaik manusia) sehingga keberadaannya lebih sulit diketahui oleh pihak yang tidak mengerti.

Salah satu teknik kriptografi visual yang paling umum diketahui dikembangkan oleh Moni Naor dan Adi Shamir pada tahun 1994. Menggunakan teknik mereka, sebuah gambar dipecah menjadi menjadi beberapa bagian (share), dan ketika semua bagian tersebut ditumpuk, akan terlihat gambar asalnya.



**Gambar 1. Teknik Kriptografi Visual Naor & Shamir.**

Pada dasarnya, dengan teknik kriptografi tersebut, sebuah pixel pada gambar dibagi menjadi menjadi 4 buah sub-pixel dengan ukuran 2x2. Ketika dienkripsi, setiap share memiliki pola subpixel yang berbeda, namun ketika pola subpixel dari semua share digabungkan, akan membentuk pixel semula. Meskipun begitu, dengan memanfaatkan teknik ini, ukuran gambar akan menjadi 2 kali lipat ukuran semua karena jumlah pixel-nya juga digandakan. Selain itu, pixel transparan tidak memiliki pola subpixel yang dapat menghasilkan pixel utuh yang berwarna transparan (karena penambahan warna apapun akan membuat pixel tersebut tidak transparan) sehingga untuk memperkuat enkripsi pada gambar, sebuah pixel transparan akan menjadi subpixel semi-transparan dimana setengah dari subpixel transparan dan setengah lagi tidak.

Secret image	Share1	Share2	Stacked image
			
			

Gambar 2. Pembagian menjadi sub-pixel.

Untuk memanfaatkan teknik kriptografi visual tersebut dibutuhkan gambar hitam putih karena terbuat dari nilai yang diskrit, hitam dan putih atau 1 dan 0. Karenanya, agar gambar *grayscale* (gambar yang memiliki berbagai intensitas hitam putih / abu-abu) dapat dienkripsi menggunakan teknik tersebut, gambar tersebut harus diubah agar hanya memiliki warna hitam dan putih. Gambar hitam putih tersebut bisa didapatkan dengan menggunakan teknik halftone, dimana tingkat kehitaman suatu bagian gambar direpresentasikan dengan intensitas jumlah pixel hitam. Sehingga, bagian gambar yang berwarna gelap akan memiliki lebih banyak pixel hitam dibandingkan dengan bagian gambar yang berwarna lebih terang.



Gambar 3. Gambar dengan *tone* yang kontinyu.



Gambar4. Gambar dengan teknik halftone.

#### IV. IMPLEMENTASI

Dalam mengimplementasikan kriptografi visual untuk gambar berwarna, gambar perlu dipecah menjadi tiga buah komponen CMYnya terlebih dahulu sehingga terdapat tiga gambar yang masing-masing hanya memiliki satu warna dasar saja. Seperti yang sudah disebutkan sebelumnya, komponen CMY bisa didapatkan dengan rumus  $CMY = 255 - RGB$ , berikut implementasi kode untuk mendapatkan komponen warna cyan saja.

```
//Buka gambar
Bitmap Image = BitmapFactory.decodeFile(Path);

//Buat array
byte[] Colors = new byte[Width * Height * 3];
for (int x = 0; x < Width; x++) {
    for (int y = 0; y < Height; y++) {
        //Ambil warna cyan saja
        int Index = ((x + (y * Width)) * 3)
        Colors[Index + 0] = 0xFF - Red(getPixel(x, y));
        Colors[Index + 1] = 0xFF;
        Colors[Index + 2] = 0xFF;
    }
}
```

Pada Android, gambar hanya dapat dibuat dari komposisi warna RGB saja, jadi untuk membuat gambar, komponen warna pixel perlu dikonversi menjadi RGB kembali. Konversi mudah dilakukan karena hanya perlu membalik rumus, sehingga untuk mendapatkan komponen RGB hanya perlu melakukan kalkulasi  $RGB = 255 - CMY$ . Apabila hal tersebut dilakukan untuk ketiga komponen warna dasar, maka akan didapat gambar-gambar berikut dari sebuah gambar asal.



Gambar 5. Gambar asal.



Gambar 6. Gambar hanya dengan komponen cyan.

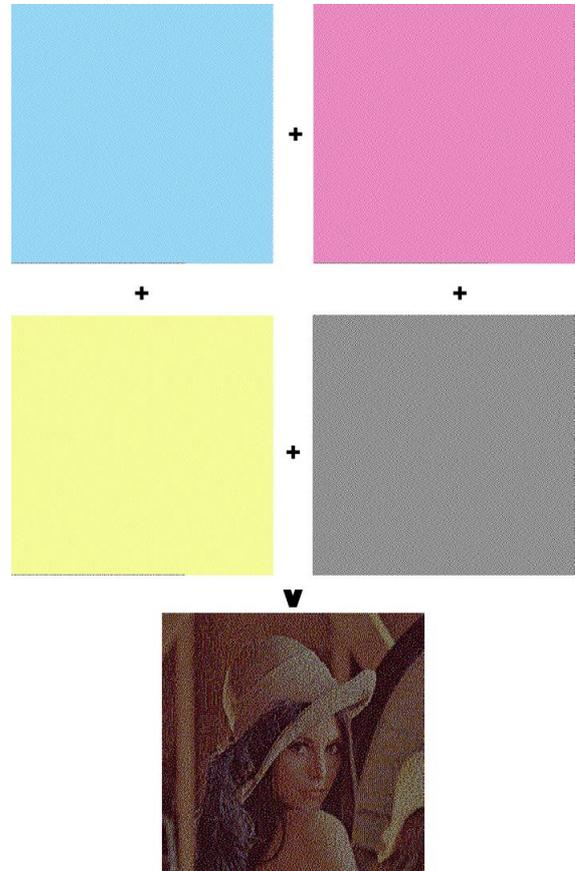


Gambar 7. Gambar hanya dengan komponen magenta.



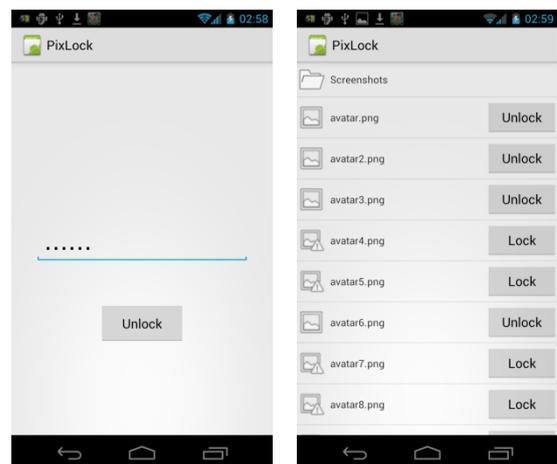
Gambar 8. Gambar hanya dengan komponen kuning.

Enkripsi kemudian dilanjutkan dengan menerapkan teknik halftone pada ketiga gambar tersebut agar hanya memiliki dua nilai, 1 dan 0 untuk setiap gambar. Kemudian dibuat *mask* berukuran 2x2 dengan warna setengah transparan dan setengah lagi hitam, dimana posisi warna hitam dibuat acak. *Mask* ini kemudian digabung dengan ketiga gambar komponen dasar untuk mendapatkan tiga buah share gambar yang bila ditumpuk akan menghasilkan warna semula.



Gambar 9. Proses dekripsi gambar.

Berikut tampilan-tampilan lain dari aplikasi Android yang sudah dibuat:



Gambar 10. Tampilan aplikasi.

## V. KESIMPULAN

Terdapat beberapa hal yang dapat diamati dari pengaplikasian kriptografi visual pada *file* gambar di Android.

Hal pertama ialah mengenai kualitas gambar. Kualitas gambar yang dihasilkan pada dekripsi tidaklah persis dengan gambar awal yang dienkripsi. Meskipun gambar masih dapat dikenali, namun berbagai detil yang ada pada suatu foto akan menghilang.

Hal kedua yang berhasil diamati ialah mengenai jumlah gambar. Dengan menggunakan kriptografi visual, jumlah gambar yang ada akan menjadi berlipat ganda. Hal ini dikarenakan teknik kriptografi visual membagi gambar menjadi beberapa bagian tidak seperti teknik kriptografi lainnya dimana sebuah data yang terenkripsi tidak terbagi-bagi menjadi beberapa bagian.

Dari hal-hal tersebut, dapat disimpulkan bahwa kriptografi visual tidak cocok untuk diterapkan untuk mengamankan file gambar pada sistem operasi Android karena menghilangkan detil pada gambar, sementara gambar yang disimpan pada Android sebagian besar merupakan gambar foto. Selain itu, teknik tersebut juga melipatgandakan jumlah gambar sehingga membutuhkan tempat penyimpanan dengan kapasitas yang besar juga.

## REFERENCES

- [1] Hou, Young-Chang. Visual cryptography for color images. 2002
- [2] SaiChandana. A New Visual Cryptography Scheme for Color Images. 2000
- [3] [http://en.wikipedia.org/wiki/Visual\\_cryptography](http://en.wikipedia.org/wiki/Visual_cryptography).
- [4] <http://developer.android.com/reference/android/graphics/Bitmap.html>.

## 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 plagiasi.

Bandung, 19 Maret 2012

ttd

Raka Mahesa  
13508074