

Analisis *Fidelity* untuk Implementasi Kriptografi Visual pada *QR Code*

Tino Eka Krisna Sambora (13510062)¹

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

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

¹13510062@std.stei.itb.ac.id

Abstrak—Pada paper ini, penulis akan menganalisis dampak dari implementasi kriptografi visual pada QR code. Bagaimana hasil dekripsi dari tiap share yang telah digabung mempengaruhi fidelity atau hasil pembacaan QR code yang telah dienkripsi. Karena biasanya hasil dekripsi sebuah citra baik biner maupun tidak mengandung noise, penulis tertarik untuk meneliti bagaimana dampak tersebut mempengaruhi pembacaan QR code yang dienkripsi. Mula-mula, penulis akan memaparkan apa itu QR code dan bagaimana QR code bekerja. Kemudian penulis akan menjelaskan bagaimana kriptografi visual diimplementasikan pada QR code, dan menganalisis dampaknya pada pembacaan QR code lalu menganalisis kriptografi visual seperti apa yang aman untuk fidelity QR code.

Kata Kunci—Kriptografi Visual, *fidelity*, *QR code*.

I. PENDAHULUAN

Quick response code (QR code) adalah label optik yang dapat dibaca oleh mesin untuk memberi instruksi tertentu. QR code memiliki prinsip kerja yang sama dengan barcode, hanya saja QR code memiliki bentuk matriks dua dimensi, bukan batang-batang seperti barcode. Penggunaan QR code tumbuh cepat karena dapat dibaca dengan cepat oleh mesin. Selain itu, QR code juga memiliki kapasitas penyimpanan yang lebih tinggi dari UPC barcode. QR code dapat digunakan untuk memantau produk, mengidentifikasi sebuah barang, memantau waktu, pengaturan dokumen, dan yang paling banyak digunakan adalah marketing produk. Untuk marketing produk, banyak sekali implementasi dari QR code. Contohnya adalah referral URL yang mengeksekusi browser, referral kontak yang mengeksekusi messenger tertentu, atau berbagai referral yang mengeksekusi berbagai aplikasi lainnya.

Karena popularitasnya, tidak menutup kemungkinan bahwa gambar dari QR code perlu dienkripsi dengan menggunakan metode kriptografi visual terlebih dahulu sebelum dikirimkan ke penerima pesan. Sebagai contoh, apabila ada URL atau kontak rahasia yang hendak dikirimkan pada seorang penerima, seorang pengirim terlebih dahulu mengirimkan QR code yang mengeksekusi pemrosesan URL atau kontak tersebut dalam bentuk citra yang terenkripsi dengan menggunakan kriptografi visual melalui saluran umum yang tidak

dipermasalahan keamanannya, karena citra yang ada telah dienkripsi.

Akan tetapi, diduga terdapat masalah pada enkripsi citra QR code dengan menggunakan kriptografi visual. Noise yang dihasilkan oleh kriptografi visual pada citra QR code dicurigai dapat mengganggu pembacaan QR code tersebut oleh mesin. Atas dasar itulah penulis hendak menganalisis *fidelity* dari kriptografi visual yang dilakukan pada QR code. Pada paper ini penulis akan menganalisis dampak kriptografi visual pada QR code, bagaimana noise yang dihasilkan dari proses enkripsi tersebut mempengaruhi pembacaan QR code oleh komputer dengan menganalisis bagaimana kriptografi visual dan QR code bekerja, lalu menganalisis bagaimana hubungan antara keduanya.

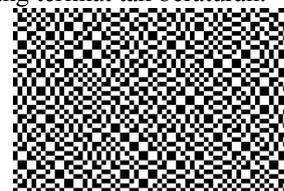
II. DASAR TEORI

A. Kriptografi Visual

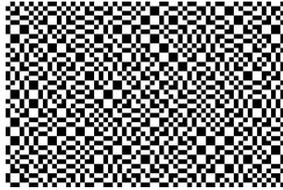
Kriptografi visual adalah teknik untuk menyembunyikan informasi didalam citra digital. Kriptografi visual menggunakan sistem enkripsi yang dapat dipecahkan hanya dengan indera visual, dengan kata lain, tidak membutuhkan komputer untuk mendekripsi informasinya ke keadaan semula.

Cara melakukan kriptografi visual pertama kali dikemukakan oleh Moni Naor dan Adi Shamir [1]. Caranya adalah dengan membagi sebuah citra menjadi beberapa bagian. Setiap bagian penting untuk merekonstruksi ulang citra asli, sehingga kepemilikan hanya salah satu bagian citra rahasia tidak berguna untuk mengetahui isi pesan rahasia.

Cara dasar dari teknik kriptografi visual adalah dengan memanfaatkan superposisi atau pelapisan dua lapis citra yang semi transparan. Sebagai contoh, diberikan dua lembar citra semi transparan yang terisi oleh beberapa piksel hitam yang terlihat tak beraturan:

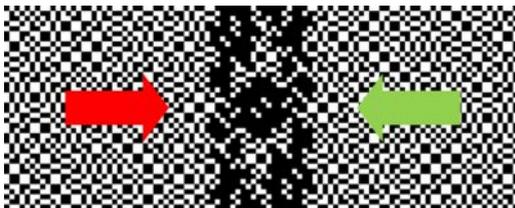


Gambar 1 Citra pertama yang hendak digabungkan



Gambar 2 Citra kedua yang hendak digabungkan

Apabila tidak digabungkan, tidak ada makna yang ada pada kedua citra tersebut. Namun, dengan menumpuk kedua citra tersebut, terjadi penggabungan antara piksel atau subpiksel yang seolah-olah menghasilkan citra yang berbeda.



Gambar 3 Penggabungan sebagian citra pertama dari kanan dan citra kedua dari kiri

Ketika kedua citra tersebut tergabung dengan posisi yang tepat, pesan rahasia yang hendak disembunyikan akan muncul. Dengan kata lain, kedua citra tersebut mengandung pola piksel hitam sedemikian sehingga menghasilkan makna ketika digabungkan.



Gambar 4 Hasil penggabungan citra dengan posisi yang tepat

B. QR Code

Sebuah QR code terdiri atas beberapa modul yang berisi titik-titik hitam yang terangkai pada sebuah *grid* berbentuk persegi dan memiliki latar belakang berwarna putih. Modul-modul tersebut dapat dibaca oleh perangkat interpretasi citra seperti kamera dan diproses dengan menggunakan pengoreksi error Reed-Solomon sampai citra tersebut dapat diinterpretasi dengan benar. Data-data yang dibutuhkan dari hasil interpretasi kemudian diekstraksi dari pola-pola yang ada pada komponen-komponen citra, baik komponen vertikal maupun komponen horizontal.

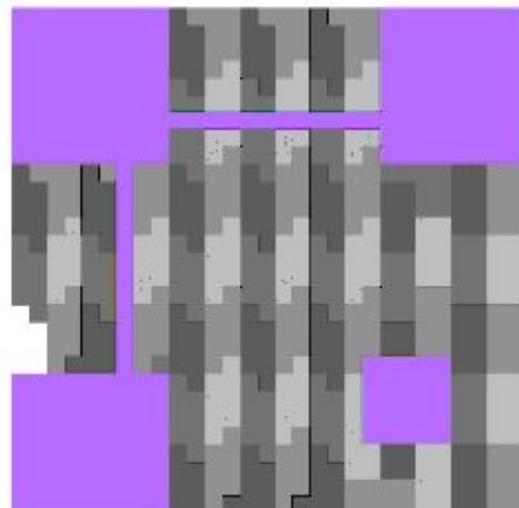
Dalam setiap QR code, sebuah persegi baik berwarna putih maupun hitam disebut sebuah modul. Modul-modul pada QR code dikelompokkan kedalam beberapa bagian (*sections*). Terdapat bagian yang boleh diedit dan terdapat bagian yang apabila diedit membuat QR code tersebut menjadi tidak bisa dibaca.



Gambar 5 Bagian-bagian QR code yang tidak boleh diubah

Pada gambar diatas, bagian yang tidak boleh diubah adalah bagian yang diwarnai:

1. Bagian berwarna merah adalah bagian yang menandai posisi, bagian ini mendefinisikan ujung-ujung dari bagian yang dapat dibaca dan penjarangan dari modul-modul.
2. Bagian berwarna hijau adalah bagian yang mengandung informasi perihal format QR code. Bagian ini memberitahu software pembaca QR code apakah data yang terkandung dalam QR code adalah URL, plainteks, nomor, dll.
3. Bagian berwarna biru adalah bagian yang mengandung informasi tentang versi QR code. Versi QR code menentukan jumlah dari modul-modul dalam code. Versi 1 adalah versi yang paling kecil, sebesar 21 x 21.



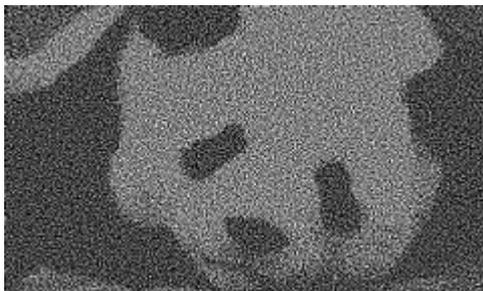
Gambar 6 Bagian QR code yang boleh diedit

Gambar diatas menunjukkan bagian yang boleh diedit dalam QR code, bagian ini akan menentukan isi dari pesan dalam QR code. Modul-modul yang dapat diedit

dikelompokkan kedalam *cluster* yang masing-masing berisi 8 buah modul, dan *cluster-cluster* tersebut tersambung seperti sebuah *puzzle*. Isi tiap *cluster* tersebut menjadi digit-digit biner dimana modul berwarna putih berarti 0 dan modul berwarna hitam berarti 1.

C. Analisis Fidelity Kriptografi Visual pada QR Code

Fidelity yang baik berarti mutu QR code yang telah dienkripsi dan dikembalikan kembali tidak jauh berubah akibat kriptografi visual. Cara paling efektif untuk menguji *fidelity* QR code setelah dienkripsi dengan kriptografi visual adalah dengan mencoba menggunakan QR code tersebut. Apabila QR code tersebut dapat dibaca oleh mesin, maka mutu dari QR code tersebut masih baik. Namun apabila QR code menjadi tidak dapat dibaca oleh mesin setelah dienkripsi, maka mutu dari QR code tersebut telah jauh berubah, dengan kata lain, *fidelity*-nya menjadi rendah.



Gambar 7 Hasil dekripsi kriptografi visual yang mengandung noise

III. IMPLEMENTASI

Implementasi pengujian kriptografi visual pada QR code dilakukan dengan cara mencoba melakukan kriptografi visual pada QR code. Pada kesempatan ini, penulis mencoba untuk membagi gambar QR code menjadi dua buah gambar *share* yang terenkripsi. Dipilih hanya sebatas dua *share* karena dengan semakin banyak *share* maka semakin besar pula noise yang mungkin dihasilkan, apabila dengan dua *share* saja *fidelity* dari QR code yang telah didekripsi sudah menurun dan membuat QR code menjadi tidak bisa dibaca, maka dengan *share* yang lebih besar *noise* menjadi semakin besar dan *fidelity* akan semakin turun dan membuat QR code semakin tak bisa terbaca oleh mesin.

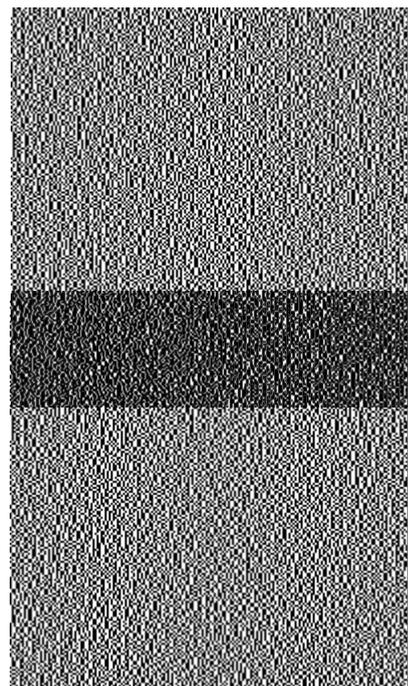
Setelah sebuah QR code dibagi menjadi dua buah *share*, kedua *share* tersebut digabungkan kembali menjadi sebuah QR code yang mengandung noise. Kemudian hasil dekripsi QR code tersebut dicoba dibaca dengan menggunakan aplikasi pembaca QR code pada platform mobile, dengan pertimbangan bahwa QR code memang sering dibaca dengan menggunakan smartphone.

Berikut adalah antarmuka aplikasi yang digunakan untuk mengenkripsi QR code:



Gambar 8 Antarmuka aplikasi kriptografi visual yang penulis gunakan

Untuk mendekripsi gambar, penulis menggunakan kaskas pengolahan teks seperti Microsoft Word. Penulis menggunakan kaskas tersebut untuk mencoba menggabungkan dua buah *share* menjadi satu gambar hasil dekripsi. Pertimbangan penggunaan kaskas pengolahan teks adalah karena kaskas tersebut dapat digunakan untuk menggerakkan dua buah gambar yang hendak digabungkan secara akurat



Gambar 9 Antarmuka penggunaan editor teks untuk mendekripsi dua buah share

IV. HASIL EKSPERIMEN

Sebuah QR code dicoba untuk dienkripsi dengan menggunakan teknik kriptografi visual. QR code yang digunakan akan merujuk pada sebuah URL tertentu. Pembacaan QR code dilakukan dengan menggunakan program yang didapatkan dari Google Play, yaitu QR Droid: aplikasi pembaca QR code untuk platform Android.



Gambar 10 Logo QR droid

Berikut adalah wujud dari QR code yang diuji:



Gambar 11 QR code yang diujikan

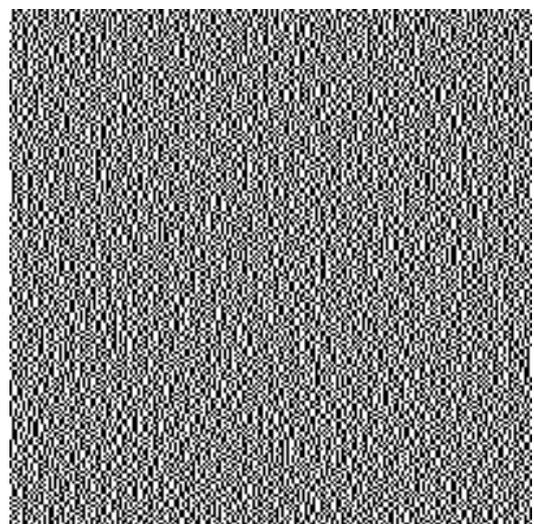
QR code diatas dicoba dibaca dengan menggunakan QR droid. Hasilnya, QR code berhasil dibaca, berikut adalah screenshot hasil pembacaan QR code sebelum dienkripsi:



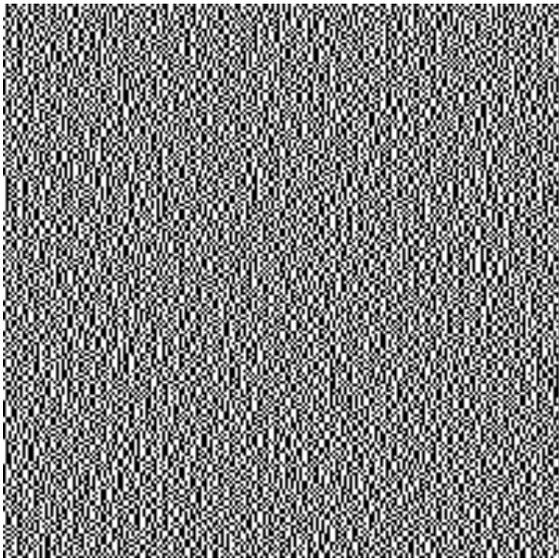
Gambar 12 Hasil QR code yang terbaca

Aplikasi QR Droid dapat dengan benar mengetahui URL yang terkandung dalam QR code.

Kemudian, QR code tersebut dienkripsi dengan menggunakan teknik kriptografi visual menjadi dua buah *share*. Berikut adalah masing-masing *share*-nya:

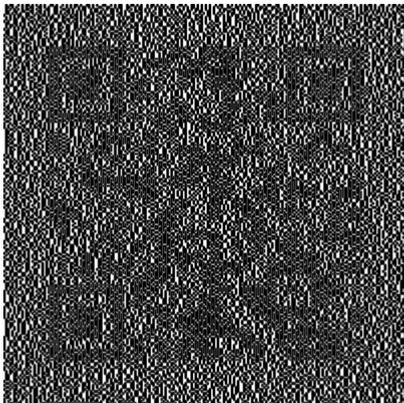


Gambar 13 Share QR code pertama



Gambar 14 Share QR code kedua

Kedua *share* tersebut lalu didekripsi sehingga didapatkan gambar semula ditambah dengan *noise*. Berikut adalah hasil dekripsi QR code-nya:



Gambar 15 Hasil dekripsi QR code

Hasilnya, QR droid tak dapat membaca hasil dekripsinya. QR droid terus-menerus mencoba membaca namun tetap diam pada layar pembacaan QR code dan tidak pindah ke layar hasil pembacaan seperti yang ditunjukkan pada gambar berikut:



Gambar 16 QR code yang tidak dapat dibaca akan terus-menerus dicoba untuk dibaca oleh aplikasi QR droid

Hal ini membuktikan bahwa kriptografi visual akan merusak mutu dari sebuah QR code secara fatal sampai sebuah QR code menjadi tak dapat dibaca oleh mesin pembaca QR code. Pada percobaan diatas penulis membagi gambar hanya menjadi dua buah *share* namun *noise*-nya telah begitu besar sampai QR code baru hasil dari dekripsi kedua *share* tersebut tidak dapat dibaca oleh mesin pembaca QR code. Apabila jumlah *share* yang dihasilkan ditambah, maka *noise* yang dihasilkan pun akan bertambah sehingga QR code semakin tidak dapat dibaca oleh pembaca QR code.

V. KESIMPULAN

Teknik kriptografi visual tidak dapat diimplementasikan pada QR code karena *noise*-nya mempengaruhi bagian-bagian pada QR code yang semestinya tidak diubah, seperti bagian yang menandai posisi, bagian yang mengandung informasi format, dan bagian yang mengandung informasi versi QR code. Ketiga bagian tersebut adalah bagian QR code yang berakibat fatal pada pembacaan apabila diganti, dan bagian tersebut tidak dilengkapi dengan algoritma pengoreksi apabila bagian tersebut mengalami perubahan.

REFERENCES

- [1] Hou, Young-Chang, "Visual Cryptography for Color Image", *Department of Information Management, National Central University, Taiwan, 2002.*
- [2] Nakajima, Mizuho, "Extended Visual Cryptography for Natural Images", *Department of Graphics and Computer Science, The University of Tokyo.*

- [3] http://datagenetics.com/blog/november32013/index.html?utm_medium=App.net&utm_source=PourOver diakses pada 5 Mei 2010.
- [4] <http://www.youthedesigner.com/2011/09/29/what-is-a-qr-code-and-how-does-it-work/> diakses pada 5 Mei 2010.
- [5] <http://www.codeproject.com/Tips/306039/Visual-Image-Cryptography-Generator> diakses pada 5 Mei 2010.

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, 16 Mei 2014



Tino Eka Krisna Sambora/13510062