Pengamanan *Quick Response* (QR) *Code* Berbasis Skema Kriptografi Visual

Daru Bagus Dananjaya – 13519080[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
[1]13519080@std.stei.itb.ac.id

***Abstract*—Seiring dengan meningkatnya aplikasi QR Code dalam berbagai aktivitas penyimpanan informasi, muncul isu keamanan dari QR Code seperti kebocoran informasi dan *data tampering*. Dalam menangani isu tersebut, makalah ini membahas mengenai Teknik pengamanan informasi dalam QR Code dengan memanfaatkan skema kriptografi visual. QR Code akan dibagi menjadi n buah *share* yang dapat ditransmisikan secara terpisah satu sama lain. Proses pembangkitan share yang dilakukan berbasis pada matriks pseudorandom sedemikian hingga nilai pixel yang ada pada share akan berkorespondensi dengan matriks pseudorandom tersebut. Proses dekripsi citra akan melibatkan penumpukan share yang terbentuk dari proses enkripsi kemudian dilakukan post-processing sehingga citra QR Code yang dihasilkan oleh proses dekripsi menjadi identik dengan citra QR Code sebelum dilakukan enkripsi.**

Keywords—QR Code; Kriptografi Visual; Secret Sharing

I. PENDAHULUAN

Pada era modern ini, *quick response* (QR) *code* sangat marak digunakan. Hal ini disebabkan oleh QR code memiliki beberapa kelebihan. Pertama, QR code mudah digunakan sebagai piranti identifikasi perangkat komputer, contohnya, telepon genggam dan *scanning guns*. Kedua, QR Code memiliki kapasitas penyimpanan yang besar, tidak mudah rusak, dan murah. Karena kelebihannya, QR code digunakan dalam berbagai aspek kehidupan. Sebagai contoh, autentikasi identitas pada *boarding pass* pesawat memanfaatkan QR Code untuk membuktikan kesamaan identitas. Dengan penggunaan yang luas dan menyangkut data-data sensitif, muncul ancaman keamanan yang serius pada QR Code seperti kebocoran informasi rahasia dan *data tampering.* Seiring berjalannya waktu, mulai banyak orang yang familiar dengan *coding rules* dari QR code ini. Bahkan, pelaku kejahatan dapat dengan mudah memanfaatkan pengetahuan atas *coding rules* ini untuk melakukan aktivitas kejahatan seperti mengambil informasi pribadi dan data-data sensitif lainnya. Penggunaan QR code tanpa protokol keamanan tambahan sudah tidak aman saat ini. Oleh karena itu, sangat dibutuhkan sebuah protokol keamanan baru yang dapat melindungi informasi-informasi yang dimuat dalam QR code dari tangan-tangan yang tidak bertanggung jawab.

Kriptografi visual merupakan sebuah alternatif baru dalam teknologi *secret sharing*. Kriptografi visual mengenkripsi informasi visual dengan sebuah cara tertentu sedemikian hingga proses dekripsi cukup dilakukan dengan melakukan persepsi informasi menggunakan indera pengelihatan manusia. Jika dibandingkan dengan skema kriptografi standar, kriptografi visual memiliki kelebihan dari sisi penyembunyian informasi serta kemudahan dalam pendekripsian informasi.

Dalam makalah ini, penulis membahas mengenai pemanfaatan skema kriptografi visual dalam pengamanan informasi pada QR code sehingga informasi sensitif yang terdapat di dalam QR code tidak dicuri oleh orang yang tidak bertanggung jawab. Skema ini dapat diterapkan dalam berbagai bidang, khususnya pada manajemen dokumen.

Makalah ini tersusun dari enam bagian. Pada bagian II, akan dibahas mengenai dasar teori dari QR code, kriptografi visual, serta metode enkripsi kriptografi visual menggunakan *modular arithmetic image encryption.* Pada bagian III, akan dijelaskan mengenai rancangan solusi dan implementasi dari pengamanan QR code menggunakan skema kriptografi visual yang kemudian dilanjutkan dengan pengujian dan analisis hasil pada bagian IV. Makalah ini ditutup kesimpulan pada bagian V.

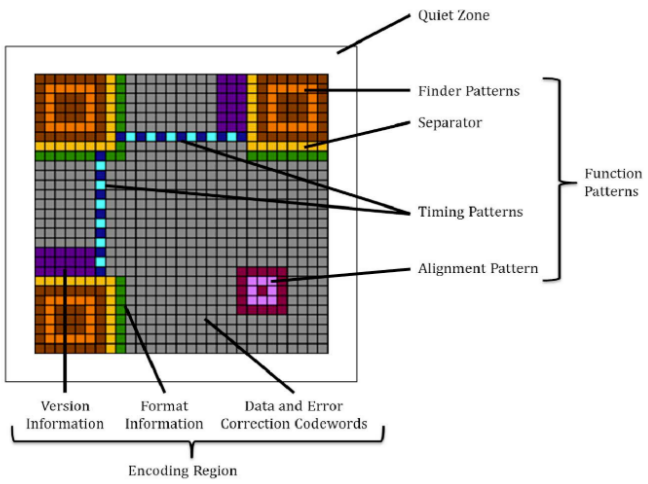
II. DASAR TEORI

A. *Quick Response* (QR) *Code*

Quick response (QR) code merupakan jenis *barcode* matriks atau kode dua dimensi yang dapat menyimpan informasi dan dibaca secara tepat dan cepat, serta didesain untuk dapat dipindai dengan perangkat *mobile*[1]. Informasi pada QR Code terdiri atas "modul" berwarna hitam yang terletak di atas latar belakang berwarna putih. Informasi yang dapat disimpan oleh sebuah QR Code dapat berupa teks, URL, maupun data lainnya[2], [3].

QR Code diciptakan oleh anak perusahaan dari Toyota, Denso Wave pada tahun 1994 untuk inventarisasi barang dalam industri otomotif. Ide dari pengembangan QR Code berasal dari keterbatasan kapasitas penyimpanan yang dimiliki oleh *barcode*.

Dalam implementasinya, QR Code terdiri atas kotak hitam yang disebut "modul" yang tersusun berdasarkan sebuah fungsi tertentu dengan latar belakang berwarna putih, yang dapat dengan mudah dibaca oleh perangkat penangkap citra seperti kamera. Data yang tersimpan dalam sebuah QR Code diekstrak melalui pola yang terdapat pada komponen horizontal dan vertikal gambar.



Gambar 1. Struktur dari sebuah QR Code
Sumber: *An introduction to QR code technology,* Tiwari (2017)

Terdapat enam komponen utama dalam sebuah QR Code, yaitu[1]:

1. *Finder Pattern*

   Finder patterns merupakan sebuah pola istimewa yang digunakan untuk mengidentifikasi orientasi dari sebuah QR Code sehingga *scanner* dapat mengenali posisi QR Code untuk proses *decoding. Finder patterns* terletak di tiga sudut dari sebuah QR Code, yaitu kiri atas, kanan atas, dan kiri bawah.

2. *Separators*

   Separator merupakan sebuah area kosong yang digunakan untuk membatasi Finder patterns dan area encoding.

3. *Timing Patterns*

   Timing pattern merupakan sebuah pola yang digunakan untuk mengenali kepadatan simbol, koordinat modul, serta *Version Information Area.* Terdapat dua macam Timing pattern, yaitu vertikal dan horizontal. Komponen ini terdiri dari sebuah pola modul gelap-terang yang bergantian. Timing pattern horizontal terletak pada baris ke-6 QR Code di antara dua buah separator. Timing pattern vertical terletak pada kolom ke-6 QR Code di antara dua buah separator.

4. *Alignment Patterns*

   Sebuah Alignment Pattern terdiri atas modul gelap berukuran 5x5, modul terang berukuran 3x3, serta 1x1 modul terang di tengahnya. Pola ini hanya dimiliki oleh QR Code versi 2 dan setelahnya. Jumlah alignment pattern untuk setiap versi akan berbeda.

5. *Encoding Region*

   Encoding region merupakan komponen dari sebuah QR Code yang digunakan untuk menyimpan format informasi, versi informasi, data, dan kode koreksi error.

6. *Quiet Zone*

   Merupakan sebuah are yang tidak berisi data apapun dan digunakan untuk memastikan bahwa hal-hal yang ada di sekitar QR Code tidak mengganggu penyimpanan dan pembacaan data dari QR Code.

Adapun kelebihan yang dimiliki oleh QR Code adalah sebagai berikut.

1. *Omnidirectional* dan Cepat.

   QR Code dapat dibaca dengan cepat dari segala arah. Dalam kata lain, Tidak perlu dilakukan *alignment* antara *scanner* dan QR Code.

2. Kapasitas penyimpanan yang besar

   Dibandingkan dengan *barcode* 1-D standar yang hanya dapat menyimpan 20 karakter alfanumerik, QR Code memiliki kapasitas penyimpanan yang jauh lebih besar dan dapat digunakan untuk menyimpan berbagai macam informasi. Sebuah QR Code mampu menampung hingga 7.089 karakter alfanumerik.

3. Minimum *error*

   Dengan adanya teknik koreksi *error* pada QR Code, informasi yang terkandung akan tetap dapat di-*decode* meskipun hingga 30% datanya kotor maupun rusak.

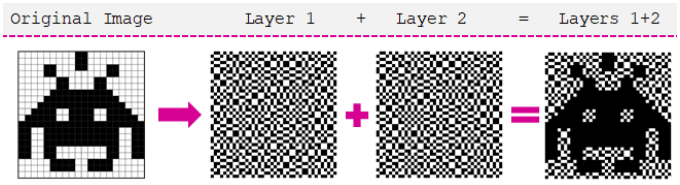
4. Ukuran yang kecil

   Dibandingkan dengan *barcode* 1-D standar, untuk menampung informasi yang sama, QR Code hanya membutuhkan 1/10 ukuran yang dibutuhkan oleh *barcode* 1-D standar.

Meskipun QR Code memiliki banyak kelebihan, namun terdapat pula kelemahan dari QR Code. Ketika sebuah QR Code tersebar dan QR Code tersebut menampung informasi sensitif, maka sama saja artinya dengan kebocoran informasi.

B. Kriptografi Visual

Pada dasarnya, kriptografi visual merupakan sebuah Teknik kriptografi di mana sebuah informasi seperti gambar, teks, dll dapat dienkripsi sedemikian hingga proses dekripsinya dapat dilakukan hanya dengan persepsi indera pengelihatan (mata) manusia[4]. Kriptografi visual pertama kali diperkenalkan pada tahun 1994 oleh M. Naor dan A. Shamir. Pada implementasinya, kriptografi visual tidak membutuhkan komputasi kriptografi yang kompleks untuk proses dekripsinya. Konsep dasar dari kriptografi visual adalah membagi sebuah gambar menjadi beberapa bagian yang disebut *share* sedemikian sehingga satu bagian menjadi cipher dan bagian lainnya menjadi *key*. Setiap *share* akan terlihat seperti citra acak yang tak bermakna sehingga disebut juga *shadow*. Seluruh *share* ini akan dikirim secara terpisah ke tujuan sehingga terhindar dari *interception* di tengah jalan. Untuk melakukan dekripsi, dilakukan penumpukan *share-share* yang ada sehingga penerima dapat melihat gambar asli.



Gambar 2. Contoh Kriptografi Visual
Sumber: https://www.101computing.net/visual-cryptography/

Cara kerja dari kriptografi visual adalah sebagai berikut[5]:

1. Setiap *pixel* pada citra diubah menjadi sejumlah *sub-pixel.*
2. Setiap *pixel* muncul pada setiap *share.*
3. Jika *sub-pixel* dari setiap *share* ditumpuk, hasilnya pixel yang dipersepsi sebagai "putih" atau "hitam".
4. Skema lainnya, satu *pixel* dibagi menjadi empat buah *sub-pixel*.
5. Satu *share* direpresentasikan sebagai satu transparansi.
6. Jika dua buah *share* ditumpuk, maka mata manusia mempersepsi *pixel* yang terbentuk sebagai "hitam" atau "putih".
7. *Pixel* hitam akan tampak hitam sempurna pada persepsi citra hasil penumpukan, sedangkan *pixel* putih akan terlihat mengandung *noise*, namun mata manusia masih dapat mempersepsi gambar semula.

Berdasarkan cara kerja di atas, dapat disimpulkan bahwa implementasi paling sederhana dari kriptografi visual adalah dengan menggunakan citra *black-and-white* di mana setiap *pixel* dapat dengan mudah ditangani secara terpisah. Kemudian, setiap *pixel* tersebut akan muncul pada setiap *share*. *Share* akan dimodelkan menggunakan sebuah matriks *Boolean* dengan ukuran n x m dalam satuan *pixel*. Jika suatu *pixel* memiliki warna hitam pada gambar aslinya, maka *pixel* tersebut akan bernilai 1, jika *pixel* memiliki warna putih pada gambar aslinya, maka *pixel* tersebut akan bernilai 0[6]. Ketika dilakukan penumpukan pada proses dekripsi, *pixel* hitam akan nampak hitam sempurna pada citra hasil penumpukan, sedangkan *pixel* putih akan mengandung *noise*, namun citra hasil dekripsi masih dapat dipersepsi oleh mata manusia[5].

C. *Modular Arithmetic Image Encryption*

Pada dasarnya, terdapat dua buah tipe aritmetika modular, yaitu *additive inverse* dan *multiplicative inverse*. Dalam sebuah Z_n, dua buah bilangan a dan b dinyatakan saling *additive inverse* jika memenuhi persamaan

$$a + b \equiv 0 (mod\ n)$$

Sedangkan dalam *multiplicative inverse*, dua buah bilangan dinyatakan saling *multiplicative inverse* jika memenuhi persamaan

$$ab \equiv 0 (mod\ n)$$

Namun, dalam *multiplicative inverse*, sebuah bilangan bulat bisa saja tidak memiliki *multiplicative inverse*. Sebagai contoh, *multiplicative inverse* dari a hanya ada jika dan hanya jika $\gcd(a, n) = 1$, atau dalam kata lain, a dan n adalah relatif prima. Sehingga, bilangan bulat a akan memiliki *multiplicative inverse* jika dan hanya jika $\gcd(a, n) = 1 (mod\ n)$.

Pada sebuah citra, kedalaman dari sebuah *pixel* memiliki nilai 0-255[7], oleh karena itu, nilai modulus yang dapat digunakan adalah 256. Teknik enkripsi kriptografi visual menggunakan aritmetika modular pada dasarnya memanfaatkan *additive inverse* karena untuk seluruh Z_{256}, semuanya memiliki *additive inverse*. Dalam metode enkripsi citra menggunakan aritmetika modular, sejumlah n *secret image* $I_i, i = 1,2, \dots, n$ akan di-encode ke dalam n buah share $S_i, i = 1,2, \dots, n$.[8]

Langkah yang dibutuhkan untuk melakukan enkripsi citra menggunakan metode ini adalah sebagai berikut:

1. Bangkitkan temporary share $T_i, i = 1,2, \dots, n$ dengan menggunakan operasi modulo aditif untuk secret image $I_i, i = 1,2, \dots, n$
2. Akan terbentuk n buah share $S_i, i = 1,2, \dots, n$ menggunakan operasi reverse bit.

Adapun algoritma untuk enkripsi adalah sebagai berikut.

Program Encrypt
Input: n buah secret images $\{I_1, I_2, \dots, I_n\}$
Output: n buah secret share $\{S_1, S_2, \dots, S_n\}$
Algoritma
1. Bangkitkan temporary share menggunakan operasi modulo aditif
   $T_1 = I_1 (mod\ 256)$
   $T_i = (I_i + T_i - 1)\ mod\ 256, \{i = 2,3, \dots, n\}$
2. Buat share menggunakan operasi reverse bit
   $S_i = ReverseBits(T_i), \{i = 2,3, \dots, n\}$

Proses dekripsi pada metode ini merupakan kebalikan dari proses enkripsinya. Waktu yang dibutuhkan untuk mengenkripsi n buah gambar akan sama dengan waktu yang dibutuhkan untuk mendekripsi n buah share[8]. Adapun algoritma untuk proses dekripsi adalah sebagai berikut.

Program Decrypt
Input: n buah secret images $\{I_1, I_2, \dots, I_n\}$
Output: n buah secret share $\{S_1, S_2, \dots, S_n\}$
Algoritma
1. Recover temporary images menggunakan operasi reverse bit
   $S_i = ReverseBits(T_i), \{i = 2,3, \dots, n\}$
2. Recover gambar menggunakan operasi modulo aditif

$$T_1 = I_1 (mod\ 256)$$
$$T_i = (I_i + T_i - 1)\ mod\ 256, \{i = 2,3, \dots, n\}$$

III. Rancangan Solusi dan Implementasi

A. Deskripsi Umum Solusi

Untuk menyembunyikan informasi dari sebuah QR Code pada saat transmisi, penulis memanfaatkan teknologi enkripsi dari kriptografi visual. Dengan melakukan enkripsi terhadap QR Code, akan sangat sulit terjadi kebocoran informasi dan *data tampering* ketika proses transfer QR Code terjadi. Sehingga informasi yang tersimpan di dalam QR Code lebih terjamin keamanannya.

B. Rancangan Solusi

Dengan menggunakan sebuah metode enkripsi yang mengkombinasikan matriks *pseudorandom* dengan protokol kriptografi visual, langkah-langkah untuk mengimplementasikannya adalah sebagai berikut[9]:

1. Terdapat dua buah matriks *boolean* pengkodean C_0 yang merepresentasikan *pixel* putih dan C_1 yang merepresentasikan *pixel* hitam.
2. Bangkitkan sebuah matriks *pseudorandom* dengan ukuran yang sama dengan ukuran gambar asli dengan nilai kisaran di antara 0-3. Masing-masing nilai akan berkorespondensi dengan matriks dasar C_0 dan matriks dasar C_1.
3. Matriks *pixel* pada *share* merupakan matriks dasar yang dipilih dari C_0 dan C_1, namun aturan pemilihannya ditentukan oleh partisipasi matriks *pseudorandom*. Pada tahap ini, terdapat dua buah kasus, yaitu.

a. Ketika membangkitkan *share* A, terdapat aturan sebagai berikut.

   i. Posisi *pixel* pada gambar asli akan dipetakan ke posisi yang sesuai dalam matriks *pseudorandom*, kemudian dipilih matriks dasar C_0 yang berkorespondensi dengan nilai yang terdapat dalam matriks *pseudorandom*.

b. Ketika membangkitkan *share* B, terdapat aturan sebagai berikut.

   i. Kasus *pixel* putih

   Posisi *pixel* putih pada gambar asli akan dipetakan ke posisi yang sesuai dalam matriks *pseudorandom*. Kemudian matriks dasar yang berkorespondensi dipilih dari C_0 sesuai dengan nilai yang ada dalam matriks *pseudorandom*.

   ii. Kasus *pixel* hitam

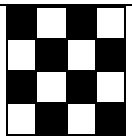
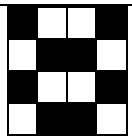
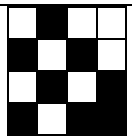
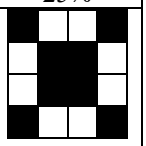
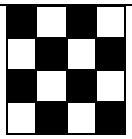
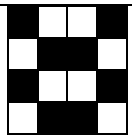
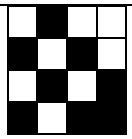
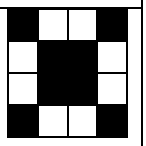
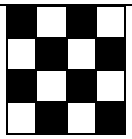
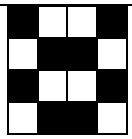
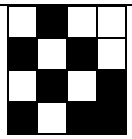
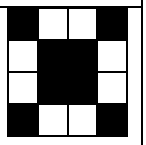
   Posisi *pixel* hitam pada gambar asli akan dipetakan ke posisi yang sesuai dalam matriks *pseudorandom*. Kemudian matriks dasar yang berkorespondensi dipilih dari C_1 sesuai dengan nilai yang ada dalam matriks *pseudorandom*

4. Pada gambar yang direkonstruksi, sebuah *pixel* hitam atau putih akan direpresentasikan oleh satu buah sub-*pixel*. Adapun matriks dasar dari kumpulan matriks pengkodean C_0 dan C_1 adalah sebagai berikut.

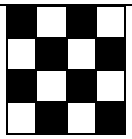
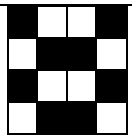
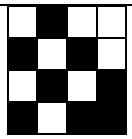
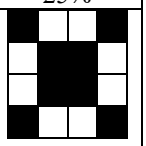
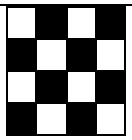
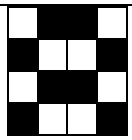
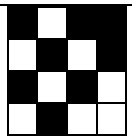
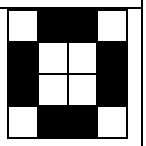
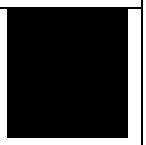
$$C_0 = \left\{ \begin{bmatrix} 0&1&0&1\\1&0&1&0\\0&1&0&1\\1&0&1&0 \end{bmatrix} \begin{bmatrix} 0&1&1&0\\1&0&0&1\\0&1&1&0\\1&0&0&1 \end{bmatrix} \begin{bmatrix} 1&0&1&1\\0&1&0&1\\1&0&1&0\\0&1&0&0 \end{bmatrix} \begin{bmatrix} 0&1&1&0\\1&0&0&1\\1&0&0&1\\0&1&1&0 \end{bmatrix} \right\}$$

$$C_1 = \left\{ \begin{bmatrix} 1&0&1&1\\0&1&0&1\\1&0&1&0\\0&1&0&1 \end{bmatrix} \begin{bmatrix} 1&0&0&1\\0&1&1&0\\1&0&0&1\\0&1&1&0 \end{bmatrix} \begin{bmatrix} 0&1&0&0\\1&0&1&0\\0&1&0&0\\1&0&1&1 \end{bmatrix} \begin{bmatrix} 1&0&0&1\\0&1&1&0\\0&1&1&0\\1&0&0&1 \end{bmatrix} \right\}$$

Tabel 1. Skema *Two-out-of-two* pada *pixel* putih

Peluang	25%	25%	25%	25%
Share A				
Share B				
Stack Share A&B				

Tabel 2. Skema *Two-out-of-two* pada *pixel* hitam

Peluang	25%	25%	25%	25%
Share A				
Share B				
Stack Share A&B				

Dari kedua skema di atas, *share* A dan B dapat dibangkitkan melalui teknik kriptografi visual yang berbasis pada operator *bitwise* AND.

Melalui teknik enkripsi yang melibatkan matriks *pseudorandom* ini, setiap *pixel* yang terbentuk pada *share* A

dan B akan terbangkitkan secara acak. Oleh karena itu, apabila terjadi serangan, dan jika penyerang berhasil memperoleh matriks dasar pun, mereka tidak akan dapat melakukan dekripsi maupun mengekstrak informasi yang ada. Namun, teknik ini memiliki kekurangan, yaitu gambar hasil *stack share* akan mengalami kehilangan kontras karena matriks dasar menggantikan *pixel* asli pada gambar asli. Oleh karena itu, dibutuhkan sebuah cara yang tepat untuk mendekripsi gambar sehingga gambar hasil dekripsi akan memiliki kualitas yang sama dengan gambar aslinya.

```
def encrypt(input_image, share_size):
    image = np.asarray(input_image)
    (row, column) = image.shape
    shares = np.random.randint(0, 256,
size=(row, column, share_size))
    shares[:, :, -1] = image.copy()
    for i in range(share_size - 1):
        shares[:, :, -1] = (shares[:, :, -1]
+ shares[:, :, i]) % 256

    return shares, image
```

Adapun langkah dekripsi yang diusulkan oleh penulis adalah sebagai berikut. Ketika terdapat k buah *share*, untuk setiap *share*, dilakukan pengurangan dari *share* lainnya dalam modulus 256 untuk mendapatkan gambar aslinya. Algoritma ini akan membutuhkan seluruh k *share* yang ada untuk mendekripsi sebuah citra. Pun ketika sebuah *share* hilang atau tidak tersedia, akan dibutuhkan 256^(m*n) *states* (m*n adalah ukuran dari citra asli) untuk melakukan dekripsi supaya citra awal kembali di mana setiap *state* memiliki peluang kemunculan yang sama sehingga sangat sulit untuk dilakukan dekripsi oleh penyerang.

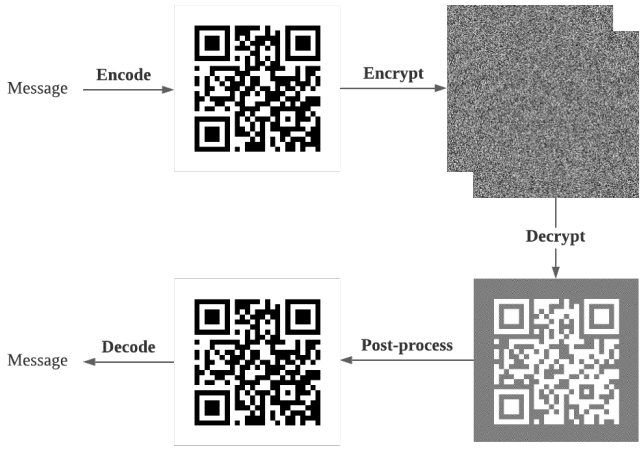
```
def decrypt(shares):
    (row, column, share_size) = shares.shape
    shares_image = shares.copy()
    for i in range(share_size - 1):
        shares_image[:, :, -1] =
(shares_image[:, :, -1] - shares_image[:, :,
i] + 256) % 256

    final_output = shares_image[:, :,
share_size - 1]
    output_image =
Image.fromarray(final_output.astype(np.uint8
))
    return output_image, final_output
```

C. *Implementasi Solusi*

Implementasi sistem pengamanan QR Code menggunakan skema kriptografi visual dibagi menjadi empat buah bagian yang saling independen satu sama lain, yaitu QR Code *encoding*, *decoding*, enkripsi, dan dekripsi kriptografi visual. QR Code dapat digunakan untuk menyimpan informasi dalam bentuk karakter alfanumerik, Kanji, Kana, simbol, *binary*, dan *control codes*.

Pada kasus ini, QR Code digunakan sebagai kontainer informasi dan dengan memanfaatkan sifat *noise tolerant* yang dimilikinya memastikan bahwa citra yang dihasilkan setelah proses dekripsi nantinya akan memiliki kualitas yang mirip dengan citra aslinya.

Melalui proses enkripsi QR Code akan meminimalisasi terjadinya kebocoran informasi dan *data tampering* ketika suatu QR Code menampung informasi sensitif. Dengan demikian, QR. Code tetap dapat digunakan untuk menyimpan informasi sensitif tanpa harus khawatir dengan isu keamanan. Adapun alur pengamanan yang diimplementasikan adalah sebagai berikut.



Gambar 3. Alur pengamanan QR Code menggunakan skema kriptografi visual
Sumber: Dokumen pribadi penulis

Dalam proses pengamanannya, sebuah informasi akan di-*encode* menggunakan sebuah QR Code, kemudian QR Code tersebut dienkripsi menjadi n buah *share* untuk pengamanan informasi. Apabila akan dilakukan *retrieval* dari informasi, maka dilakukan proses dekripsi dan *post-process* sehingga QR Code dapat dibaca dengan normal kembali.

IV. Analisis dan Pengujian

Berdasarkan penjelasan implementasi pengamanan QR Code pada bagian sebelumnya, akan dilakukan percobaan yang diimplementasikan dalam bahasa pemrograman Python untuk mengamankan sebuah informasi sensitif dengan menggunakan skema kriptografi visual.

Dalam percobaan kali ini, berkas yang akan dienkripsi adalah sebuah sertifikat vaksin yang berisi data berupa NIK, tanggal lahir, serta ID vaksin.

Surat Keterangan Vaksinasi COVID-19

Sertifikat ini diberikan kepada

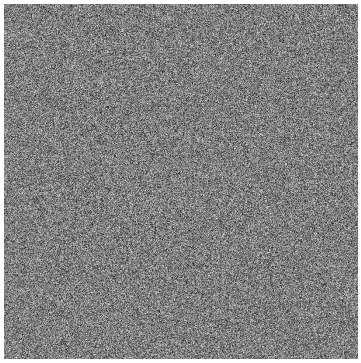
Nama: Tomi Gunawan
NIK: 5208926311971490
Tanggal lahir: 23/06/2001
ID Vaksin: 1LBqgn2rr4MxhxMXu1AXDBv4QHGzNUHnKo

telah dilakukan vaksinasi COVID-19 untuk dosis pertama pada tanggal 30 Juli 2021 sesuai dengan Peraturan Menteri Kesehatan Republik Indonesia.

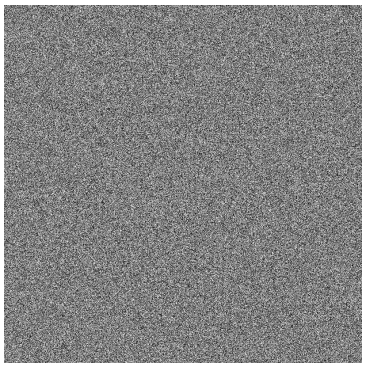
Setelah dilakukan *encoding* terhadap berkas di atas, dihasilkan sebuah QR Code sebagai berikut.

Gambar 4. QR Code hasil encoding berkas
Sumber: Dokumen pribadi penulis

Jika QR Code dalam keadaan tidak terenkripsi dan tersebar luas, maka terjadi kemungkinan penyalahgunaan data pribadi. Oleh karena itu, dilakukan enkripsi terhadap QR Code tersebut dengan *share* sejumlah dua buah (jumlah *share* dapat disesuaikan sesuai dengan kebutuhan). *Share image* yang dihasilkan adalah sebagai berikut.



Gambar 5. Share A
Sumber: Dokumen pribadi penulis

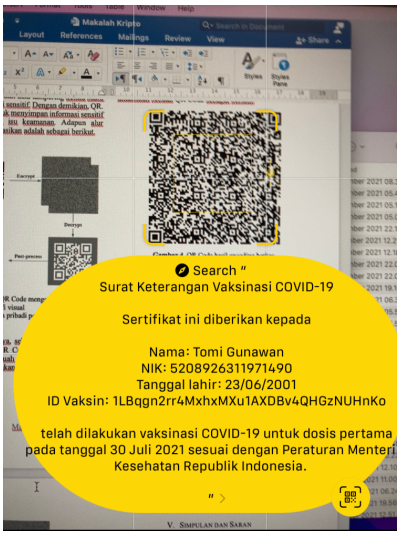


Gambar 6. Share B
Sumber: Dokumen pribadi penulis

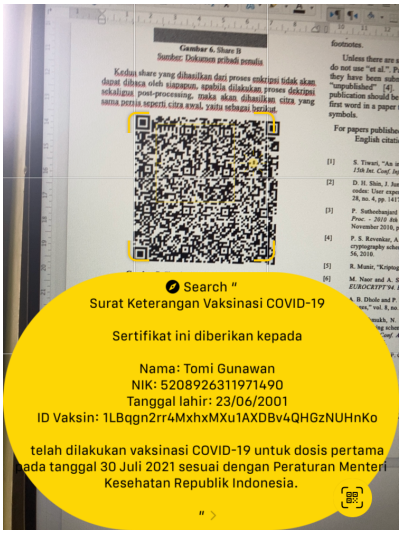
Kedua *share* yang dihasilkan dari proses enkripsi tidak akan dapat dibaca oleh siapapun, apabila dilakukan proses dekripsi sekaligus *post-processing*, maka akan dihasilkan citra yang sama persis seperti citra awal, yaitu sebagai berikut.

Gambar 7. Citra hasil dekripsi dan post-processing
Sumber: Dokumen pribadi penulis

Ketika hasil dekripsi dipindai, akan menghasilkan informasi yang sama persis dengan informasi yang terkandung dalam citra aslinya. Hal ini dapat dibuktikan melalui gambar berikut.



Gambar 8. Informasi dari QR Code sebelum dienkripsi
Sumber: Dokumen pribadi penulis



Gambar 9. Informasi dari QR Code setelah dekripsi
Sumber: Dokumen pribadi penulis

Berdasarkan hasil pengujian yang dilakukan, skema kriptografi visual dapat mengamankan informasi yang terkandung di dalam QR Code secara *lossless* dan hanya dibutuhkan dua buah partisipan untuk membawa *share*. Hal ini tentu saja memperlihatkan bahwa skema ini cukup layak untuk digunakan dalam pengamanan informasi meskipun masih banyak ruang untuk pengembangan ke depannya.

V. Simpulan dan Saran

Skema kriptografi visual dapat digunakan untuk mengamankan informasi yang terkandung dalam sebuah QR Code. Dengan menggunakan matriks *pseudorandom*, dapat disimpulkan bahwa.

1. Keamanan data yang terkandung dalam sebuah QR Code terjamin dan proses enkripsi/dekripsi yang dilakukan cukup efisien dari segi komputasi dan keamanannya.
2. Hasil dekripsi dari *share* akan menghasilkan kualitas citra yang sama persis dengan citra asli sebelum dienkripsi. Hal ini menunjukkan bahwa skema kriptografi visual yang diajukan pada makalah ini bersifat *lossless* sehingga keutuhan informasi terjamin.

Masih banyak ruang untuk pengembangan skema kriptografi visual dalam pengamanan informasi QR Code ini, terutama dari segi waktu dan *resource* komputasi. Dapat dilakukan optimasi pada proses enkripsi dan/atau dekripsi sehingga prosesnya dapat menjadi lebih cepat dan efisien.

VI. Ucapan Terima Kasih

Penulis mengucapkan terima kasih dan puji syukur kepada Tuhan Yang Maha Esa karena atas rahmat dan karunia-Nya, penulis dapat mengerjakan makalah ini dengan lancar dan tepat waktu. Penulis juga mengucapkan terima kasih kepada :

1. Bapak Ir. Rinaldi Munir atas bimbingan dan ilmu yang diajarkan selama perkuliahan Kriptografi.
2. Starbucks Citadel Square yang telah memberikan "bensin" untuk mengerjakan makalah ini.
3. Teman-teman mahasiswa IF'19 yang bersedia menjadi tempat berkeluh kesah serta membantu saya dalam menyelesaikan tugas ini.

References

[1] S. Tiwari, "An introduction to QR code technology," *Proc. - 2016 15th Int. Conf. Inf. Technol. ICIT 2016*, vol. 1, pp. 39–44, 2017.

[2] D. H. Shin, J. Jung, and B. H. Chang, "The psychology behind QR codes: User experience perspective," *Comput. Human Behav.*, vol. 28, no. 4, pp. 1417–1426, 2012.

[3] P. Sutheebanjard and W. Premchaiswadi, "QR-code generator," *Proc. - 2010 8th Int. Conf. ICT Knowl. Eng. ICT KE 2010*, no. November 2010, pp. 89–92, 2010.

[4] P. S. Revenkar, A. Anjum, and W. Z. Gandhare, "Survey of visual cryptography schemes," *Int. J. Secur. its Appl.*, vol. 4, no. 2, pp. 49–56, 2010.

[5] R. Munir, "Kriptografi Visual, Teori dan Aplikasinya (Bag. 1)." .

[6] M. Naor and A. Shamir, "Visual cryptography," *Adv. Cryptol. — EUROCRYPT'94. EUROCRYPT 1994.*, pp. 805–807, 1994.

[7] A. B. Dhole and P. N. J. Janwe, "Visual Cryptography in Gray Scale Images," vol. 8, no. 4, pp. 65–68, 2013.

[8] M. Deshmukh, N. Nain, and M. Ahmed, "An (n, n)-multi secret image sharing scheme using boolean XOR and modular arithmetic," *Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA*, vol. 2016-May, pp. 690–697, 2016.

[9] X. Cao, L. Feng, P. Cao, and J. Hu, "Secure QR Code Scheme Based on Visual Cryptography," vol. 133, pp. 433–436, 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 plagiasi.

Bandung, 20 Desember 2021

Daru Bagus Dananjaya - 13519080