

Implementasi QR Code dengan Kriptografi Visual pada Produk Original di *Marketplace*

Ricky Yuliawan (13517025)¹

Program Studi Teknik Informatika

Sekolah Teknik Elektro dan Informatika

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

¹13517025@std.stei.itb.ac.id

Abstract—*E-commerce* atau *electronic commerce* merupakan segala aktivitas jual beli termasuk penyebaran, pembelian, penjualan, pemasaran barang dan jasa yang dilakukan melalui media elektronik yang kini lebih sering terjadi melalui internet. Transaksi jual beli secara *online* ini sudah digunakan oleh hampir penduduk di seluruh dunia, karena proses transaksinya yang dilakukan tanpa adanya pertemuan antar para pihaknya yang menggunakan media internet dan proses transaksinya yang sangat mudah. Namun, dalam pembelian produk pada *marketplace*, seringkali ditemukan penjualan produk yang mengaku sebagai produk berkualitas original padahal produk tersebut berkualitas KW (*kwalitas*) atau produk tiruan. Sehingga, pembeli sering sekali merasa bingung dan ragu untuk membeli suatu produk atau ada yang tertipu dengan produk yang mengaku kualitas original tersebut. Untuk membantu membedakan dan memverifikasi produk tersebut apakah produk berkualitas original atau bukan diperlukan penggunaan QR Code dengan kriptografi visual. Makalah ini akan menjelaskan bagaimana implementasi QR Code dengan kriptografi visual pada produk original di *marketplace*.

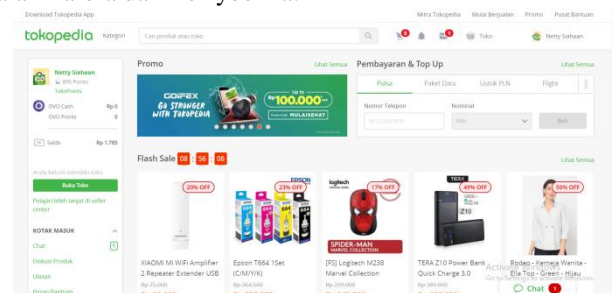
Keywords—QR Code, Kriptografi Visual, produk original, *e-commerce*, *marketplace*.

I. PENDAHULUAN

Transaksi perdagangan secara daring (*e-commerce*) di Indonesia memiliki masa depan yang cerah, karena nilai transaksinya yang terus meningkat selama lima tahun terakhir. Sehingga *marketplace* adalah salah satu pemain terbesar dalam bisnis *e-commerce* Indonesia. Hal ini dikarenakan salah satu *platform* yang paling banyak digunakan untuk berdagang secara daring di Indonesia adalah *marketplace*. *Marketplace* adalah perantara antara penjual dan pembeli di dunia maya. Situs *marketplace* bertindak sebagai pihak ketiga dalam transaksi secara daring dengan menyediakan tempat berjualan dan fasilitas pembayaran atau bisa dikatakan kalau *marketplace* adalah *department store online*.^[1]

Marketplace diklasifikasikan menjadi dua jenis kerja sama di situs *marketplace* Indonesia, yaitu *marketplace* murni dan konsinyasi. *Marketplace* murni adalah jenis kerja sama ketika situs *marketplace* hanya menyediakan lapak untuk berjualan dan fasilitas pembayaran. Penjual diberikan keleluasaan lebih banyak dan berkewajiban untuk menyediakan deskripsi dan foto produk secara mandiri. Contoh dari *marketplace* murni adalah Tokopedia dan Bukalapak. Sedangkan *marketplace*

konsinyasi adalah jenis kerja sama ketika penjual hanya menitipkan barang di *marketplace*. Penjual hanya perlu menyediakan produk dan detail informasi ke pihak *marketplace* dan pihak *marketplace* yang akan mengurus penjualan dari foto produk, gudang, pengiriman barang, hingga fasilitas pembayaran. Contoh dari *marketplace* konsinyasi adalah Zalora dan Berrybenka.

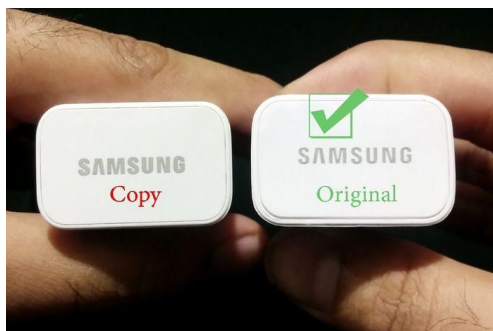


Gambar 1.1. Tokopedia

Sumber : www.tokopedia.com

Dalam membeli produk baik secara luring maupun daring, terdapat beberapa jenis kualitas suatu produk. Salah satu jenis kualitas produk adalah original. Produk dengan kualitas original adalah produk yang merupakan barang resmi dari pihak pembuatnya.^[2] Produk ini murni diproduksi, diseleksi, distandarisasi oleh produsen sendiri sehingga kualitas barang benar-benar terjaga dan tidak mengecewakan para pembelinya. Membeli produk original merupakan kebanggaan tersendiri bagi orang yang membelinya apalagi jika merk produk tersebut cukup terkenal di dunia. Namun sering sekali ditemukan produk yang mengaku kualitasnya original, padahal kualitasnya KW atau bahkan hanya produk tiruan original. Hal ini menyebabkan pembeli sering tertipu dengan produk-produk yang mengaku original tersebut dan membuat ragu dan bingung untuk menentukan apakah produk tersebut original atau bukan. Kejadian tersebut sangat marak terjadi di *marketplace*, dikarenakan kita tidak bisa melihat lebih detail secara langsung produk tersebut.

Dalam makalah ini, penulis akan mengimplementasikan QR Code dengan kriptografi visual pada produk original di *marketplace*. Dengan penggunaan QR Code dengan kriptografi visual ini diharapkan bisa terbantu untuk membedakan atau memverifikasikan suatu produk di *marketplace* yang berkualitas original.



Gambar 1.2. Produk Original dan Tiruan

Sumber : <https://hai.grid.id/read/07936890/jangan-ketipu-ini-cara-bedakan-charger-asli-dan-charger-palsu>

II. LANDASAN TEORI

2.1. Kriptografi

Secara etimologi, kata kriptografi (*Cryptography*) berasal dari bahasa Yunani, yaitu *'kryptos'* yang artinya 'yang tersembunyi' (*hidden/secret*) dan *'graphein'* yang artinya 'tulisan' (*write*) (Prayudi, 2005). Kriptografi atau sandisastra adalah ilmu dari cara-cara untuk komunikasi aman pada kehadirannya di pihak ketiga mengenai mengkonstruksi dan menganalisis protokol komunikasi yang dapat memblokir lawan berbagai aspek dalam keamanan informasi seperti data rahasia, integritas data, autentikasi, dan non-repudansi.^[3] Lebih sederhananya, kriptografi merupakan teknik mengenkripsi dimana *plaintext* (naskah asli) diacak menggunakan suatu kunci enkripsi menjadi *ciphertext* (naskah acak yang sulit dibaca) oleh seseorang yang tidak memiliki kunci dekripsinya.

Kriptografi dibagi menjadi dua, yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik merupakan teknik kriptografi yang sudah digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang yang caranya hanya melakukan pengacakan plaintext atau hanya melakukan pengacakan pada huruf A - Z. Salah satu contohnya adalah Caesar cipher, Vigenere cipher, Playfair cipher, dan lain-lainnya. Sedangkan, kriptografi modern merupakan teknik kriptografi yang beroperasi dalam mode bit ketimbang mode karakter dan pengoprasi kriptografi ini dalam mode bit berarti semua data dan informasi (*plaintext*, kunci, dan *ciphertext*) dinyatakan dalam rangkaian string ataupun bit biner 0 dan 1. Teknik enkripsi dan dekripsinya memproses semua data dan informasi dalam bentuk rangkaian bit dan kemudian rangkaian bit yang menyatakan plaintext dienkripsi menjadi ciphertext dalam bentuk rangkaian bit, demikian sebaliknya. Salah satu contohnya adalah AES, RSA, 3DES, DES, dan algoritma lainnya. Kriptografi modern masih menggunakan prinsip-prinsip dari kriptografi klasik yang digabungkan, hanya saja kriptografi modern sering beroperasi dalam bentuk bit dan operasi yang paling banyak digunakannya adalah operasi XOR. Membangun kriptografi modern yang baik tergolong sulit karena studi untuk memecahkan suatu algoritma kriptografi sudah cukup banyak berkembang.

Kriptografi memiliki beberapa aspek keamanan antara lain :^[4]

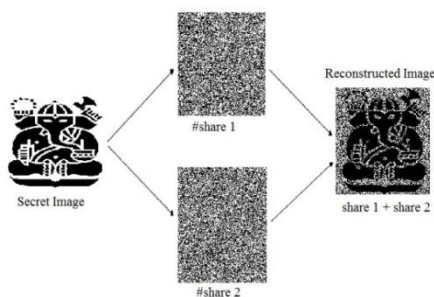
- 1) Kerahasiaan (*confidentiality*), yang berarti bahwa data-data tersebut hanya bisa diakses oleh pihak-pihak tertentu saja. Kerahasiaan bertujuan untuk melindungi

suatu informasi dari semua pihak yang tidak berhak atas informasi tersebut.

- 2) Otentikasi (*authentication*), yang berarti identifikasi yang dilakukan oleh masing – masing pihak yang saling berkomunikasi, maksudnya beberapa pihak yang berkomunikasi harus mengidentifikasi satu sama lainnya. Informasi yang didapat oleh suatu pihak dari pihak lain harus diidentifikasi untuk memastikan keaslian dari informasi yang diterima.
- 3) Integritas (*integrity*), yang berarti menjamin setiap pesan yang dikirim pasti sampai pada penerimanya tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, dirusak, diubah urutannya, dan ditambahkan. Integritas data bertujuan untuk mencegah terjadinya perubahan informasi oleh pihak-pihak yang tidak berhak atas informasi tersebut. Untuk menjamin integritas data ini pengguna harus mempunyai kemampuan untuk mendeteksi terjadinya manipulasi data oleh pihak-pihak yang tidak berkepentingan. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, maupun penggantian data.
- 4) Nirpenyangkalan (*Non-repudiation*), yang berarti mencegah pengirim maupun penerima mengingkari bahwa mereka telah mengirimkan atau menerima suatu pesan. Jika sebuah pesan dikirim, penerima dapat membuktikan bahwa pesan tersebut memang dikirim oleh pengirim yang tertera. Sebaliknya, jika sebuah pesan diterima, pengirim dapat membuktikan bahwa pesannya telah diterima oleh pihak yang ditujunya.

2.2. Kriptografi Visual

Kriptografi visual adalah teknik kriptografi yang mengenkripsi informasi visual dengan suatu cara sehingga dekripsi cukup dilakukan dengan mempersepsi informasi menggunakan indra penglihatan (mata) yang diperkenalkan oleh Moni Naor dan Adi Shamir dalam makalah berjudul "*Visual Cryptography*" di dalam jurnal Eurocrypt'94.^[5] Kriptografi visual tidak membutuhkan komputasi kriptografi yang rumit untuk proses dekripsinya. Ide awal dari kriptografi visual ini adalah dengan membagi sebuah gambar menjadi dua bagian, sehingga satu gambar menjadi *cipherteks* dan gambar lainnya menjadi kunci. Kedua gambar ini lalu dapat dikirim secara terpisah kepada tujuan. Kemudian, dilakukan dekripsi dengan cara mencetak kedua gambar tersebut pada lembar transparan. Kedua lembar tersebut lalu dibentuk menjadi sebuah tumpukan sehingga gambar asli dapat terlihat dengan mata. Dengan demikian proses mendapatkan *plainteks* dapat dilakukan oleh siapa saja yang memiliki *cipherteks* dan kunci secara bersamaan.



Gambar 2.1. Contoh Kriptografi Visual

Sumber : <https://catatankriptografi.wordpress.com/category/kriptografi-visual/>

Cara kerja kriptografi visual adalah sebagai berikut.^[5]

- 1) Setiap *pixel* dibagi 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 4 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.

Model yang paling sederhana dari kriptografi visual adalah dengan menggunakan gambar yang hanya terdiri dari *pixel* berwarna hitam atau putih saja yang dimana setiap *pixel* ditangani secara terpisah. Lalu, setiap *pixel* akan muncul pada objek hasil enkripsi (*share*). Tiap *share* adalah subset dari objek asli. Pemodelan sederhana ini dapat ditampilkan dalam representasi matriks *boolean* yang berukuran $m \times n$ di mana m adalah lebar dan n adalah tinggi yang diukur dalam satuan *pixel*. Jika suatu *pixel* berwarna hitam pada gambar aslinya, maka pada matriks digambarkan dengan nilai 1 atau *true*, dan sebaliknya jika *pixel* berwarna putih maka digambarkan dengan nilai 0 atau *false*.^[6]

2.3. QR Code

QR Code (*Quick Response Code*) adalah jenis *barcode* matriks atau *barcode* dua dimensi yang dimana isi kode dapat diuraikan dengan cepat dan tepat. QR Code pertama kali dikembangkan oleh Denso Wave, sebuah perusahaan Jepang pada tahun 1994 untuk industri otomotif di Jepang. QR Code sering kali berisi data untuk pencari lokasi, pengenalan, atau pelacak yang mengarah ke situs web atau aplikasi. QR Code menggunakan empat mode pengkodean standar (numerik, alfanumerik, *byte* / biner, dan kanji) untuk menyimpan data secara efisien; ekstensi juga dapat digunakan.

QR Code terdiri dari kotak hitam yang disusun dalam kotak persegi dengan latar belakang putih, yang dapat dibaca oleh perangkat pencitraan seperti kamera, dan diproses menggunakan koreksi kesalahan Reed – Solomon hingga

gambar dapat diinterpretasikan dengan tepat. Data yang diperlukan kemudian diekstraksi dari pola yang ada di komponen horizontal dan vertikal gambar.



Gambar 2.2. Contoh QR Code

Sumber : <https://www.kaspersky.com/resource-center/definitions/what-is-a-qr-code-how-to-scan>

Pola dalam QR Code mewakili kode biner yang dapat diartikan untuk mengungkapkan data yang disimpan oleh kode tersebut. Pembaca QR dapat mengidentifikasi QR Code standar berdasarkan tiga kotak besar di luar QR Code. Setelah mengidentifikasi ketiga bentuk ini, pembaca tahu bahwa semua yang ada di dalam kotak itu adalah QR Code. Pembaca QR kemudian menganalisis QR Code dengan memecah semuanya menjadi kisi dengan melihat kotak grid individu dan memberikan masing-masing nilai berdasarkan apakah itu hitam atau putih. Kemudian mengelompokkan kotak-kotak grid untuk membuat pola yang lebih besar.

Terdapat dua jenis QR Code, antara lain sebagai berikut.

- 1) *Static QR Code* adalah QR Code yang berisi tautan ke halaman web yang tetap. Penggunaan *Static QR Code* menyebabkan konten QR Code tidak dapat diubah.
- 2) *Dynamic QR Code* adalah QR Code berisi sebuah URL singkat yang kemudian dialihkan ke halaman web yang lain. Penggunaan *Dynamic QR Code* menyebabkan QR Code dapat diubah dan digunakan ulang terus menerus.

QR Code memiliki kelebihan sebagai berikut.

- 1) Berisi lebih banyak informasi daripada *barcode*. *Barcode* hanya dapat berisi satu string informasi berupa kode numerik. Sedangkan QR Code, dapat berisi lebih banyak informasi dan dalam berbagai jenis (seperti kata dan karakter).
- 2) Lebih sedikit *error*. Kapasitas penyimpanan informasi yang lebih tinggi dari QR Code memberi ruang untuk brankas-gagal untuk dibangun.
- 3) Mudah dibaca. QR Code dapat dibaca dan dipahami oleh *smartphone* dan kamera digital. Ini membuatnya jauh lebih berguna untuk hal-hal seperti kampanye pemasaran yang dihadapi konsumen.
- 4) Mudah dicetak. QR Code hanya membutuhkan pencetakan hitam dan

putih (meskipun warna apa pun atau bahkan beberapa warna dapat digunakan).

- 5) Lebih aman
Dimungkinkan untuk mengenkripsi informasi dalam QR Code menawarkan tingkat perlindungan ekstra.

III. IMPLEMENTASI QR CODE DENGAN KRIPTOGRAFI VISUAL PADA PRODUK ORIGINAL DI MARKETPLACE

Untuk menyembunyikan informasi QR Code, penulis menggunakan teknologi enkripsi visual yang ditingkatkan berdasarkan teknologi enkripsi visual yang ada untuk mewujudkan penyembunyian pola QR Code. Melalui metode enkripsi ini, informasi yang disembunyikan dalam QR Code lebih sulit diakses oleh pemalsu. Sehingga untuk mencapai tujuan informasi tersembunyi lebih aman.

QR Code dengan informasi tersembunyi adalah *image* rahasia yang asli, menggunakan metode enkripsi khusus yang matriks pseudo-random kombinasikan dengan algoritma kriptografi visual untuk menghasilkan dua *shared image*. Langkah-langkahnya untuk mengimplementasikan QR Code dengan kriptografi visual tersebut adalah sebagai berikut.

- 1) Dua koleksi matriks boolean pengkodean M_0 dan M_1 , masing-masing mewakili *pixel* putih dan *pixel* hitam dari *image* rahasia yang asli.
- 2) Membuat matriks *pseudo-random* dengan ukuran yang sama dengan *image* rahasia yang asli, yang berada dalam kisaran 0 sampai 3, masing-masing nilai sesuai dengan matriks dasar M_0 dan M_1 . Matriks dasar di M_1 dilakukan XOR oleh matriks dasar di M_0 dan matriks yang menyatu.
- 3) Matriks *pixel* dari *shared image* adalah matriks dasar yang dipilih dari M_0 atau M_1 , tetapi aturan yang dipilih ditentukan oleh partisipasi matriks *pseudo-random*.
 - a) Saat membuat *share image* A, aturannya sebagai berikut: posisi *pixel* (termasuk *pixel* putih dan *pixel* hitam) pada *image* rahasia dipetakan ke posisi yang sesuai dalam matriks *pseudo-random*, kemudian dipilih matriks dasar yang sesuai dari M_0 sesuai dengan nilai dalam matriks *pseudo-random*.
 - b) Saat membuat *share image* B, aturannya sedikit berbeda ketika *pixel* putih dan *pixel* hitam dipetakan ke matriks *pseudo-random*. Jika kasus *pixel* putih, aturannya adalah sebagai berikut: posisi *pixel* putih pada *image* rahasia dipetakan ke posisi yang sesuai dalam matriks *pseudo-random*, kemudian matriks dasar yang sesuai dipilih dari M_0 sesuai dengan nilai dalam matriks *pseudo-random*. Dalam kasus *pixel* hitam, aturannya adalah sebagai berikut. Posisi *pixel* hitam pada *image* rahasia dipetakan ke posisi yang sesuai dalam matriks *pseudo-random*, dan matriks dasar yang sesuai dipilih dari M_1 sesuai dengan nilai dalam matriks *pseudo-random*.
- 4) Dalam *image* rahasia yang direkonstruksi, *pixel* putih atau hitam pada *image* rahasia yang asli diwakili oleh

satu sub-*pixel*. Matriks dasar dari kumpulan matriks pengkodean M_0 dan M_1 adalah sebagai berikut:

$$M_0 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$M_1 = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Prinsip superposisi *pixel* berdasarkan AND dalam skema ini ditunjukkan pada Tabel 3.1 dan Tabel 3.2 berikut.

Tabel 3.1. Konstruksi Skema Two-Out-Of-Two (Pixel Putih)

Pixel	Putih			
Peluang	25%	25%	25%	25%
share A				
share B				
Stack share A&B				

Tabel 3.2. Konstruksi Skema Two-Out-Of-Two (Pixel Hitam)

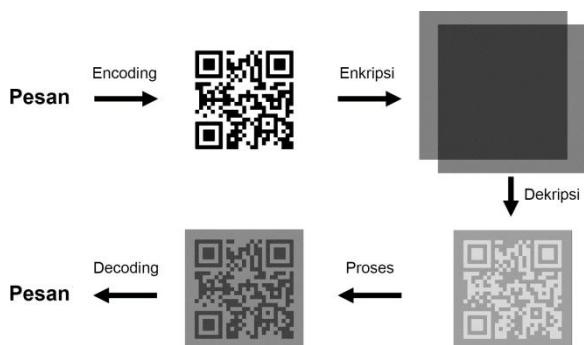
Pixel	Hitam			
Peluang	25%	25%	25%	25%
share A				
share B				
Stack share A&B				

Dalam skema di atas, *share image* rahasia A dan B dihasilkan dengan menggunakan skema kriptografi visual berdasarkan operasi AND. Dari prinsip dasar cipher visual dan sifat operasi, dua *share image* A dan B dapat digunakan untuk memulihkan *image* rahasia.

Share image yang dihasilkan dalam skema ini terkait dengan matriks *pseudo-random*. *Pixel* pada *share image* A dipilih secara acak dari matriks dasar, dan *pixel* pada *share image* B juga dihasilkan dari matriks dasar seperti dijelaskan di atas. Bahkan jika matriks dasar diperoleh oleh mereka, penyerang atau pemalsu tidak dapat memecahkan enkripsi atau memperoleh informasi rahasia. Namun, *image* rahasia yang ditumpuk memiliki kehilangan kontras dibandingkan dengan

image rahasia aslinya. Matriks dasar menggantikan pixel pada *image* asli yang menyebabkan fenomena ini. Ini normal, dan ini diharapkan menjadi hasil eksperimen. Ukuran gambar yang dibagikan dan *image* rahasia yang ditumpuk diperluas menjadi empat kali lipat dibandingkan dengan gambar aslinya. Ini juga terkait dengan penggantian pixel. Karena pixel gambar asli diganti dengan matriks dasar 4x4, maka gambar yang dibagikan dan gambar QR setelah pemulihan *overlay* akan menjadi empat kali lebih banyak dari *image* rahasia yang asli.

Semua fungsi dalam Implementasi kriptografi visual untuk encoding/decoding QR Code, dan enkripsi/dekripsi kriptografi visual dapat digunakan secara individual atau sebagai *pipeline*. Berdasarkan QR code, sistem dapat mengenkripsi/mendekripsi pesan jenis string apa pun, serta dapat menggunakan fitur kriptografi visual hanya untuk mengenkripsi/mendekripsi *image*.



Gambar 3.1. Alur Penggunaan QR Code dengan Kriptografi Visual
Sumber : Dokumen Penulis

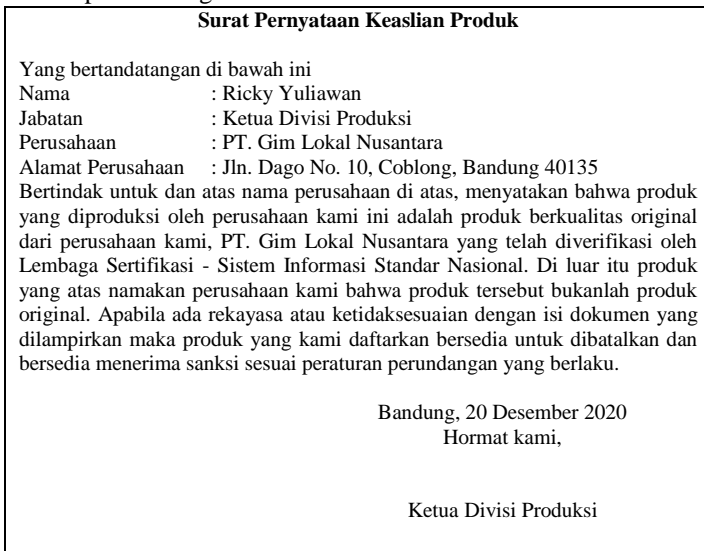
QR Code digunakan untuk mengimplementasikan enkripsi string dengan kriptografi visual. Dengan kapasitas QR Code dan karakteristik anti-noise diperlukan untuk meningkatkan kinerja kriptografi visual. *Image* yang setelah didekripsi dilakukan proses untuk lebih meningkatkan kualitas gambar.

Pesan atau file yang akan dienkripsi dalam QR Code berisi pesan atau file yang menyatakan bahwa produk yang dikasih QR Code tersebut berkualitas original resmi dari pembuat produk tersebut. Melalui metode enkripsi ini, informasi yang disembunyikan dalam QR Code lebih sulit diakses oleh pemalsu untuk meminimalisir adanya pemalsuan oleh produk-produk berkualitas non-original untuk mengaku produk tersebut berkualitas original. Dengan demikian implementasikan QR Code yang aman dengan kriptografi visual ini dapat membedakan antara produk berkualitas original dan non-original (tiruan) pada produk-produk di *marketplace* karena sulitnya untuk ditiru dan diakses oleh pemalsu.

IV. EKSPERIMEN DAN HASIL ANALISIS

Berdasarkan proses yang dijelaskan di atas, penulis membangun skema eksperimental kriptografi visual menggunakan skema Two-Out-Of-Two. Eksperimen ini menggunakan bahasa pemrograman Python untuk melakukan enkripsi dan dekripsi QR Code dengan kriptografi visualnya.

Berkas yang penulis coba untuk masukkan ke QR Code adalah berisi pesan sebagai berikut.

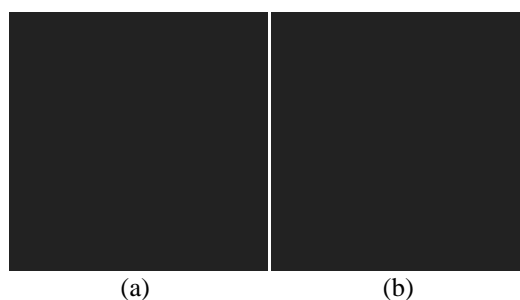


Kemudian, setelah dilakukan encode, didapatkanlah QR Code dari berkas tersebut. Berikut adalah QR Code dari hasil encode tersebut.



Gambar 4.1. QR Code Hasil Encode
Sumber : Dokumen Penulis

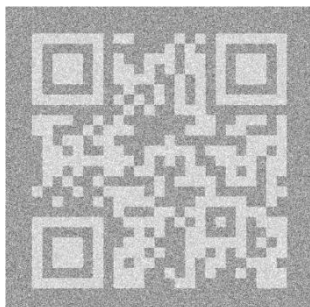
Setelah itu, dilakukan enkripsi pada QR Code yang telah diencode tadi. *Share image* yang digunakan dalam proses enkripsi dengan kriptografi visual adalah sebagai berikut.



Gambar 4.2. (a) share image A (b) share image B
Sumber : Dokumen Penulis

Kedua share image yang dihasilkan dari proses enkripsi jika digabungkan akan menghasilkan image hasil dekripsi sebagai

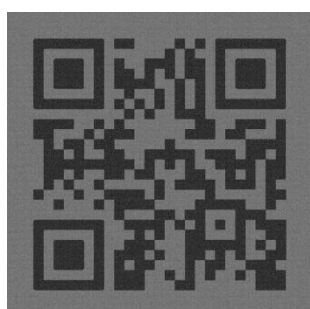
berikut.



Gambar 4.3. QR Code Hasil Dekripsi

Sumber : Dokumen Penulis

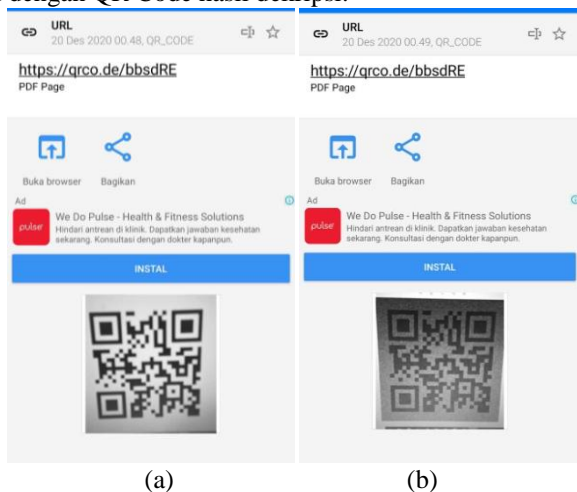
QR Code di atas masih tidak bisa dibaca oleh pemindai QR Code. Maka, *image* QR Code hasil dekripsi tersebut diproses dengan melakukan invers pada warnanya untuk lebih meningkatkan kualitas gambar sehingga mendekati QR Code awalnya. Berikut adalah hasil dari proses tersebut.



Gambar 4.4. Hasil Dekripsi setelah diproses

Sumber : Dokumen Penulis

Hasil dekripsi tersebut kemudian penulis coba pindai dengan menggunakan aplikasi pemindai yang tersedia dari gawai penulis. Hasil dari pindai tersebut menelusuri berkas yang disimpan dalam QR Code tersebut. Berikut adalah tangkapan layar dari penulis yang membandingkan hasil pindai QR Code awal dengan QR Code hasil dekripsi.



Gambar 4.5. (a) Hasil scan QR Code awal (b) Hasil scan QR Code hasil dekripsi

Sumber : Dokumen Penulis

Berdasarkan hasil eksperimen di atas, skema ini merealisasikan pemulihan lengkap image rahasia dengan perluasan pixel, yang hanya membutuhkan dua partisipan untuk membawa *share image*.

Dari hasil percobaan, enkripsi keamanan dari skema QR Code tersebut cukup layak. Namun skema ini masih bisa ditingkatkan agar lebih sesuai untuk penggunaannya lebih lanjut pada *marketplace*.

V. KESIMPULAN

Dalam membedakan dan memverifikasikan produk berkualitas original pada *marketplace*, implementasi QR Code dengan kriptografi visual dapat digunakan. Dengan menerapkan matriks *pseudo-random* dalam kriptografi visual dalam skema ini, dan melakukan eksperimennya, dapat disimpulkan bahwa skema tersebut cukup efisien untuk keamanannya. Namun, untuk hasil dekripsinya masih memiliki cukup banyak *noise* sehingga untuk proses memindai QR Code tersebut terkadang masih mengalami error atau tidak bisa dipindai. Sehingga skema ini masih perlu ditingkatkan agar lebih sesuai untuk penggunaannya lebih lanjut pada *marketplace*.

VI. UCAPAN TERIMA KASIH

Pertama-tama, penulis mengucapkan puji syukur kepada Allah swt. atas segala nikmat yang telah diberikan-Nya, sehingga penulis bisa menyelesaikan makalah ini tepat pada waktunya. Penulis juga ingin mengucapkan terima kasih kepada dosen mata kuliah IF4020 Kriptografi yang pernah mengajari penulis, khususnya kepada Bapak Dr. Ir. Rinaldi Munir, M.T. yang telah mengajar selama satu semester ini dan memberikan ilmu kepada penulis. Penulis juga ingin mengucapkan terima kasih kepada keluarga dan teman-teman penulis yang telah memberikan motivasi dan mengirimkan doa kepada penulis.

REFERENSI

- [1] Mubarok, Ilham. 2019. *Apa Itu Marketplace? Pengertian, Jenis, dan Contohnya*. <https://www.niagahoster.co.id/blog/marketplace-adalah/> (diakses tanggal 9 Desember 2020)
- [2] Oky. 2018. *Perbedaan Barang Ori, OEM, KW Super*. <https://www.winnetnews.com/post/perbedaan-barang-ori-oem-kw-super/> (diakses tanggal 9 Desember 2020)
- [3] Bellare, Mihir; Rogaway, Phillip (21 September 2005). "Introduction". *Introduction to Modern Cryptography*. hlm. 10.
- [4] Andika, Dwiky. 2018. *Pengertian dan Sejarah Kriptografi*. <https://www.it-jurnal.com/pengertian-dan-sejarah-kriptografi/> (diakses tanggal 9 Desember 2020)
- [5] Munir, Rinaldi. 2020. *Kriptografi Visual, Teori dan Aplikasinya* (Bag. 1). <http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Visual-Bagian1.pdf> (diakses tanggal 9 Desember 2020)
- [6] N.Naor and A. Shamir, *Visual Cryptography, Advances in Cryptology: Eurocrypt '94*, Springer - Verlag, Berlin, hlm 1-129 (1995).

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, 11 Desember 2020

A handwritten signature in black ink, appearing to read 'Ricky', with a horizontal line underneath.

Ricky Yuliawan 13517025