WATERMARKING DENGAN QRCODE DIGUNAKAN UNTUK VERIFIKASI PADA WEBSITE

Hepi Nuryadi
Raldy08@gmail.com

Abstrak

With the development of digital technology and the internet today more and more works Digital image is duplicated. However this will be detrimental to the original owner or owner of the digital image.
Therefore, a means of providing copyright protection or ownership of the digital image works is required. One way is done by watermarking technique, which is a method to insert a watermark into a digital image. And for verification of the Watermark the insertion on the watermak uses QR Code (Quick Response Code) in order to prove the ownership of a digital image.

Keywords- Steganography, Watermarking, QR Code (Quick Response Code)

1. PENDAHULUAN

Perkembangan teknologi digital dan internet saat ini memberikan kemudahan kepada orang untuk menggandakan, memodifikasi, dan menyebarkan karya multimedia digital. Salah satu karya multimedia digital adalah citra digital. Namun hal ini akan merugikan bagi pembuat atau pemilik asli citra digital tersebut bila penggandaan, pemodifikasian, atau penyebaran dilakukan oleh orang lain tanpa memperhatikan hak cipta (I*ntellectual Property Right*).

Untuk itu diperlukan suatu cara untuk memberikan perlindungan hak cipta atau kepemilikan terhadap karya citra digital. Salah satu cara yang dilakukan adalah dengan teknik watermarking, yaitu suatu metode untuk menyisipkan sebuah watermark kedalam citra digital. Watermark tesebut dapat diekttraksi dikemudian hari sebagai bukti kepemilikan suatu citra digital. Dalam tulisan ini watermark yang digunakan adalah QR Code untuk verifikasi kepemilikan dari Citra Digital tersebut.

1.1 Steganografi

Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Sebaliknya, kriptografi menyamarkan arti dari suatu pesan, tapi tidak menyembunyikan bahwa ada suatu pesan. Kata "steganografi" berasal dari bahasa Yunani *steganos*, yang artinya “tersembunyi atau terselubung”, dan *graphein*, “menulis”.

Kini, istilah steganografi termasuk penyembunyian data digital dalam berkas-berkas (*file*) komputer. Contohnya, si pengirim mulai dengan berkas gambar biasa, lalu mengatur warna setiap pixel ke-100 untuk menyesuaikan suatu huruf dalam alphabet (perubahannya begitu halus sehingga tidak ada seorangpun yang menyadarinya jika ia tidak benar-benar memperhatikannya).

Pada umumnya, pesan steganografi muncul dengan rupa lain seperti gambar, artikel, daftar belanjaan, atau pesan-pesan lainnya. Pesan yang tertulis ini merupakan tulisan yang menyelubungi atau menutupi. Contohnya, suatu pesan bisa disembunyikan dengan menggunakan tinta yang tidak terlihat di antara garis-garis yang kelihatan.

Teknik steganografi meliputi banyak sekali metode komunikasi untuk menyembunyikan pesan rahasia (teks atau gambar) di dalam berkas-berkas lain yang mengandung teks, *image*, bahkan audio tanpa menunjukkan ciri-ciri perubahan yang nyata atau terlihat dalam kualitas dan struktur dari berkas semula. Metode ini termasuk tinta yang tidak tampak, *microdots*, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar.

Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan di antaranya:

- Format *image* : bitmap (bmp), gif, pcx, jpeg, dll.
- Format audio : wav, voc, mp3, dll.
- Format lain : teks file, html, pdf, dll.

Kelebihan steganografi jika dibandingkan dengan kriptografi adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.

Sebuah pesan steganografi (*plaintext*), biasanya pertama-tama dienkripsikan dengan beberapa arti tradisional, yang menghasilkan *ciphertext*. Kemudian, *covertext* dimodifikasi dalam beberapa cara sehingga berisi *ciphertext*, yang menghasilkan *stegotext*. Contohnya, ukuran huruf, ukuran spasi, jenis huruf, atau karakteristik *covertext* lainnya dapat dimanipulasi untuk membawa pesan tersembunyi; hanya penerima (yang harus mengetahui teknik yang digunakan) dapat membuka pesan dan mendekripsikannya.

Dialam steganografi terdapat beberapa metode didalam menyembunyikan pesan dianataranya adalah :

- Least Significatn Bit Insertion (LSB)
- Algoritms and Tranformation
- Redundant Pattern Encoding
- Spread Spectrum Method
- Steganalisis dan Stegosystem

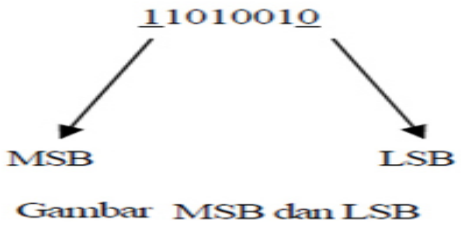
1.2 Metode Steganografi

Kebanyakan algoritma steganografi menggunakan sebuah kombinasi dari bidang jenis teknik untuk melakukan sebuah tugas dalam penyelubungan pesan rahasia dalam sebuah selubung berkas. Sebuah program steganografi dibutuhkan untuk melakukan hal-hal berikut (baik implisit melalui suatu perkiraan maupun eksplisit melalui sebuah perhitungan), menemukan kelebihan bits dalam selubung file yang dapat digunakan untuk menyelubungi pesan rahasia didalamnya, memilih beberapa diantaranya untuk digunakan dalam menyelubungi data dan penyelubungan data dalam bits dipilih sebelumnya.

1.2.1 Least Significant Bit Insertion (LSB)

Metoda yang digunakan untuk menyembunyikan pesan pada media digital tersebut berbeda-beda. Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap pixel berkas bitmap 24 bit kita dapat menyisipkan 3 bit data.

Teknik Steganografi Modifikasi LSB dilakukan dengan memodifikasi bit-bit yang termasuk bit LSB pada setiap byte warna pada sebuah pixel. Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan bit bit informasi lain yang ingin disembunyikan. Setelah semua bit informasi lain menggantikan bit LSB di dalam file tersebut, maka informasi telah berhasil disembunyikan. Ketika informasi rahasia tersebut ingin kembali dibuka, maka bit-bit LSB yang sekarang ada, diambil satu per satu kemudian disatukan kembali menjadi sebuah informasi yang utuh seperti semula. Penentuan bit-bit LSB dilakukan secara berurutan, mulai dari byte awal sampai byte terakhir sesuai panjang dari data rahasia yang akan disembunyikan.Mengubah bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya tidak berpengaruh terhadap persepsi visual/auditori.



Gbr. 1 Contoh gambar metode LSB dan MSB

Metode LSB
contoh penggunaan metode LSB
Misal pesan yang akan disisipkan 5 bit
= 11010, maka jumlah byte yang digunakan = 5 byte
10010110 11001001 11111001 10001000 10100011 (byte yang digunakan untuk penyisipan pesan)
Proses penyisipan
pesan **11010**
hasil penyisipan menjadi
10010111 11001001 11111000 10001001 10100010
jadi metode LSB ini hanya menggantikan bit pertama.

2 Watermarking

Salah satu karya intelektual yang dilindungi adalah barang dalam bentuk digital, seperti *software* dan produk multimedia seperti teks, musik (dalam format MP3 atau WAV), gambar/citra (*image*), dan video digital (VCD). Selama ini penggandaan atas produk digital tersebut dilakukan secara bebas dan

leluasa. Pemegang hak cipta atas produk digital tersebut tentu dirugikan karena ia tidak mendapat royalti dari usaha penggandaan tersebut.

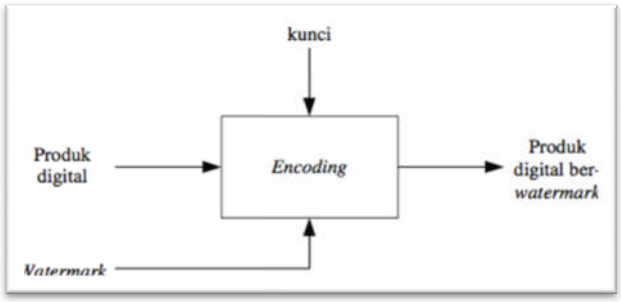
Salah satu cara untuk melindungi hak cipta multimedia (gambar/foto, suara, teks, video) adalah dengan menyisipkan informasi ke dalam data multimedia tersebut dengan teknik *watermarking*. Informasi yang disisipkan ke dalam data multimedia disebut *watermark*, dan *watermark* dapat dianggap sebagai sidik digital (*digital signature*) atau stempel digital dari pemilik yang sah atas produk multimedia tersebut.

Pemberian *signature* dengan teknik *watermarking* ini dilakukan sedemikian sehingga informasi yang disisipkan tidak merusak data digital yang dilindungi. Sehingga, seseorang yang membuka produk multimedia yang sudah disisipi *watermark* tidak menyadari kalau di dalam data multimedia tersebut terkandung label kepemilikan pembuatnya.
Jika ada orang lain yang mengklaim bahwa produk multimedia yang didapatkannya adalah miliknya, maka pemegang hak cipta atas karya multimedia tersebut dapat membantahnya dengan mengekstraksi *watermark* dari dalam data multimedia yang disengketakan. *Watermark* yang diekstraksi dibandingkan dengan *watermark* pemegang hak cipta. Jika sama, berarti memang dialah pemegang hak cipta produk multimedia tersebut.

Pada dasarnya, teknik *watermarking* adalah proses menambahkan kode identifikasi secara permanen ke dalam data digital. Kode identifikasi tersebut dapat berupa teks, gambar, suara, atau video. Selain tidak merusak data digital produk yang akan dilindungi, kode yang disisipkan seharusnya memiliki ketahanan (*robustness*) dari berbagai pemrosesan lanjutan seperti pengubahan, transformasi geometri, kompresi, enkripsi, dan sebagainya. Sifat *robustness* berarti data *watermark* tidak terhapus akibat pemrosesan lanjutan tersebut.

Tujuan dibuatnya Watermarking
* Memberikan perlindungan copyright terhadap pemilik dari dokumen digital.
* Dapat memberikan otentifikasi terhadap pemilik dari dokumen digital.
* Menyediakan cara untuk validasi data tersebut.

Menyisipkan informasi dengan tidak merusak data digital yang dilindungi.

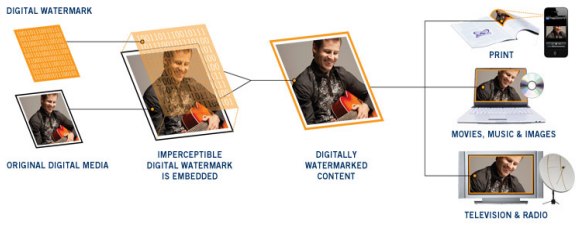


Gbr. 2 Contoh gambar watermark

2.1 Digital Watermarking

Pengertian Digital Watermak [1] Sebuah digital watermark adalah jenis penanda yang tertanam dalam sinyal suara-toleran seperti audio atau data gambar. Hal ini biasanya digunakan untuk mengidentifikasi kepemilikan hak cipta dari sinyal tersebut. "Watermarking" adalah proses menyembunyikan informasi digital dalam sinyal pembawa, informasi yang tersembunyi [2] tetapi tidak perlu mengandung kaitannya dengan sinyal pembawa.

Sebuah watermark digital disebut rapuh jika gagal menjadi terdeteksi setelah sedikit modifikasi. Watermark rapuh seperti ini biasanya digunakan untuk pendeteksian (integritas bukti). Modifikasi karya asli yang jelas dan terlihat, biasanya tidak disebut sebagai watermark, tetapi sebagai barcode secara umum.



Cth Gambar ilustrasi digital watermark
http://www.digimarc.com/technology/about-digital-watermarking

2.2 Perbedaan Watermark dengan Steganografi

Berdasarkan uraian diatas didapatkan perbedaan antara steganografi dan watermarking seperti tabel dibawah ini.

Tabel 1 Perbedaan Steganogafi dan Watermarking

	Steganografi	Watermarking
Tujuan	Mengirimkan pesan rahasia apapun tanpa menimbulkan kecurigaan	Perlindungan *copyright*, pembuktian kepemilikan, *finger print*

Persyaratan	Aman, sulit dideteksi, sebanyak mungkin menampung pesan	Robustness, sulit dihapus
Komunikasi	Point to point	One to many
Komentar lain	Media penampung tidak punya arti apa-apa	Media penampung yang justru diproteksi, watermark tidak rahasia, tidak mementingkan kapasitas watermark

3 QR Code (Quick Response Code)

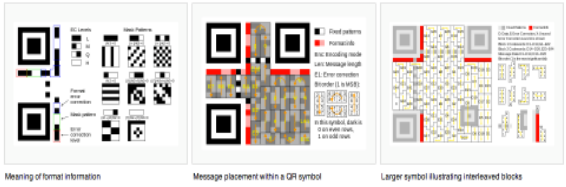
3.1 Definisi

Qr Code adalah suatu jenis kode matriks atau kode batang dua dimensi yang dikembangkan oleh Denso Wave, sebuah divisi Denso Corporation yang merupakan sebuah perusahaan Jepang dan di-publikasikan pada tahun 1994 dengan fungsionalitas utama yaitu dapat dengan mudah dibaca oleh pemindai. QR merupakan singkatan dari *quick response* atau respons cepat, yang sesuai dengan tujuannya adalah untuk menyampaikan informasi dengan cepat dan mendapatkan respons yang cepat pula. Berbeda dengan *Bar Code*, yang hanya menyimpan informasi secara horizontal, QR Code mampu menyimpan informasi secara horizontal dan vertikal, oleh karena itu secara otomatis Kode QR dapat menampung informasi yang lebih banyak daripada Bar Code.

QR code (disingkat dari Quick Response Code) adalah merek dagang untuk jenis matriks barcode (atau bar code dua dimensi) pertama kali dirancang untuk industri otomotif di Jepang. Kode bar label dapat dibaca mesin optik melekat pada item yang mencatat informasi yang berhubungan dengan item. Itu awalnya dipatenkan, namun, pemegang paten memilih untuk tidak mengakses hak-haknya [3]. Baru-baru ini, sistem Kode QR telah menjadi populer di luar industri otomotif karena pembacaan yang cepat dan kapasitas penyimpanan yang lebih besar dibandingkan dengan standar UPC barcode.. Kode ini terdiri dari modul hitam (titik persegi) diatur dalam kotak persegi pada latar belakang putih. Informasi yang dikodekan dapat terdiri dari empat jenis standar ("mode") data (numerik, alfanumerik, byte / biner, Kanji) atau, melalui ekstensi didukung, hampir semua jenis data [4].

3.2 Versi QR Code

Versi simbol QR-Code berkisar dari Versi 1 ke Versi 40. Setiap versi memiliki konfigurasi modul yang berbeda atau jumlah modul (Modul ini mengacu pada titik-titik hitam dan putih yang membentuk QR-Code). "Konfigurasi Modul" mengacu pada jumlah modul yang terkandung dalam simbol, dimulai dengan Versi 1 (21 x 21 modul) sampai ke Versi 40 (177 x 177 modul).



3.3 Koreksi Kesalahan pada QR Code

QR Code memiliki kemampuan mengoreksi kesalahan untuk mengembalikan data jika kode kotor atau rusak. Empat tingkat kesalahan koreksi yang tersedia bagi pengguna, tingkatan ini mampu mengoreksi kesalahan pada QR-Code.

Koreksi Kesalahan Pada QR Code	
Level L	Dapat mengoreksi kesalahan sampai 7%
Level M	Dapat mengoreksi kesalahan sampai 15%
Level Q	Dapat mengoreksi kesalahan sampai 25%
Level H	Dapat mengoreksi kesalahan sampai 30%

3.4 Data Encoding pada QR Code

Kapasitas QR Code yang diberikan tergantung pada versi dan tingkat koreksi kesalahan, serta pada jenis data yang diencode. Ada empat mode data yang kode QR dapat mengkodekan: numerik, alfanumerik, biner, atau Kanji. Daftar Denso-Wave situs web versi QR mencakup informasi tentang berapa banyak bit data yang dapat mengkodekan di tiap versi.

Adapun tahapan-tahapan dalam encoding text menjadi QR code adalah sebagai berikut:

3.4.1 Data analisys.

Sebuah kode QR mengkodekan string teks. QR standar memiliki empat mode untuk encoding teks: numerik, alfanumerik, byte, dan Kanji. Setiap mode mengkodekan teks sebagai string bit (1 dan 0), tetapi masing-masing modus menggunakan metode yang berbeda untuk mengubah teks menjadi bit, dan setiap

metode pengkodean dioptimalkan untuk mengkodekan data dengan sesingkat mungkin string bit. Oleh karena itu, langkah pertama Anda harus melakukan analisis data untuk menentukan apakah teks Anda dapat dikodekan dalam numerik, alfanumerik, byte, atau Kanji modus, lalu pilih modus yang paling optimal untuk tex Anda

Alphanumeric character codes

Code	Character	Code	Character	Code	Character	Code	Character	Code	Character
00	0	09	9	18	I	27	R	36	SP
01	1	10	A	19	J	28	S	37	$
02	2	11	B	20	K	29	T	38	%
03	3	12	C	21	L	30	U	39	*
04	4	13	D	22	M	31	V	40	+
05	5	14	E	23	N	32	W	41	–
06	6	15	F	24	O	33	X	42	.
07	7	16	G	25	P	34	Y	43	/
08	8	17	H	26	Q	35	Z	44	:

Tabel kode aphanumerik pada QR Code

3.4.2 Data Encoding

Setelah memilih modus pengkodean yang sesuai untuk teks, langkah berikutnya adalah untuk me-nyandikan teks. Bagian data encoding menjelaskan proses ini. Hasil dari langkah ini adalah string bit yang dibagi menjadi codeword data yang masing-masing panjang 8 bit.

3.4.3 Error Corection coding.

Yaitu proses generate dari bit-bid data yang merepresaentasikan teks yang akan dijadikan kode QR menggunakan Reed-Solomon Error Correction.

3.4.4 Structure Final Message.

Data dan koreksi kesalahan codeword yang dihasilkan pada langkah sebelumnya sekarang harus diatur dalam urutan yang tepat. Untuk kode QR yang besar, data dan koreksi kesalahan codeword yang dihasilkan dalam blok, dan blok ini harus disisipkan sesuai dengan spesifikasi kode QR.

3.4.5 Module Placment In Matrix

Setelah menghasilkan codeword data dan codeword koreksi kesalahan dan mengaturnya dalam urutan yang benar, Anda harus menempatkan bit dalam kode matriks QR. Codeword-codeword disusun dalam matriks dengan cara tertentu. Selama langkah ini, juga akan menempatkan pola yang umum untuk semua kode QR, seperti kotak pada tiga sudut.

3.4.6 Data Masking.

Pola-pola tertentu dalam kode matriks QR dapat membuat sulit untuk scanner QR code dengan benar membaca kode. Untuk mengatasi ini, spesifikasi QR code mendefinisikan delapan pola masker, masing-masing yang mengubah kode QR menurut pola tertentu. Anda harus menentukan pola hasil tmasking ini di kode QR dengan sifat yang tidak diinginkan paling sedikit. Hal ini dilakukan dengan mengevaluasi setiap matriks bertopeng berdasarkan empat aturan penalti. QR code akhir Anda harus menggunakan pola masker yang diperoleh skor penalti terendah.

3.4.7 Format dan Versi Informasi

Langkah terakhir adalah menambahkan Format dan (jika perlu) informasi versi ke kode QR dengan menambahkan piksel di daerah tertentu dari kode yang dibiarkan kosong di langkah sebelumnya. Format piksel mengidentifikasi tingkat koreksi kesalahan dan pola topeng yang digunakan dalam kode QR. Versi piksel menyandikan ukuran matriks QR dan hanya digunakan dalam kode QR yang lebih besar

4 Tahapan digital Pada Watermark.

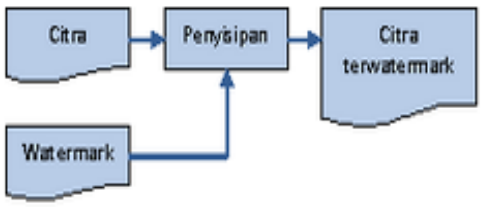
Pada tahapan digital watermarking terdapat 2 (dua) tahapan yaitu tahapan penyisipan gambar watermark dan verifikasi untuk keabsahan dari watermark tersebut.

4.1 Tahapan Penyisipan

Pada tahap penyisipan, langkah yang dilakukan adalah sebagai berikut:

a. Memilih citra yang akan digunakan sebagai citra pembawa watermark. Citra yang dipilih adalah citra grayscale dengan dua dimensi.
b. Memilih citra yang akan dijadikan watermark. Citra watermark dipilih citra biner dengan ukuran yang lebih kecil dari citra pembawa.
c. Menentukan algoritma yang digunakan untuk penyisipan.

Membuat matriks penampung citra dan melakukan penyesuaian untuk citra watermark karena besarnya tidak sama dengan citra pembawa. Tahapan Penyisipan diatas dapat digambarkan sebagai berikut:

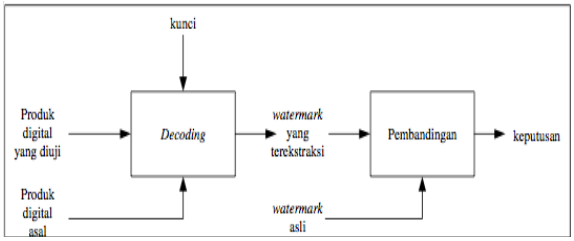


Gambar Alur Penyisipan Watermark

4.2 Tahapan Verifikasi

Pada tahap verifikasi, langkah yang dilakukan adalah sebagai berikut:

a. Memilih citra digital yang telah terwatermark.
b. Menggunakan alat untuk membaca QR code untuk memverifikasi text yang telah di input didalam Qr Code.
c. Membandingkan Qrcode yang ada dengan keterangan yang ada.
d. Membuat keputusan mengenai citra digital tersebut.



Gambar Alur Verifikasi Watermark.

5 Pembahasan

Pada bagian pembahasan ini akan dibahas tentang beberapa hal yaitu, studi kasus dan Analisa Program, Rancangan Program, dan Hasil Program berdasarkan dari studi kasus tersebut

5.1 Studi Kasus

Kasus yang ada pada saat ini adalah banyaknya website tempat kita mengupload dan juga mendownload gambar (citra digital), sehingga diperlukan suatu cara untuk memverifikasi data tersebut.

a) Masalah yang ada :
i. Banyaknya website yang menyimpan hasil foto dari fotographer seperti photographer.net Flickr dll.
ii. Semakin banyaknya social media dimana kita dapat menguppload citra digital yang kita punya ke website.
iii. Semakin berkurangnya kesadaran pengguna internet untuk hasil karya orang lain.
iv. Semakin banyakanya citra digital yang dipergunakan secara tidak bertanggung jawab.

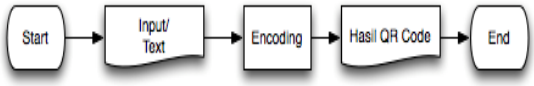
b. Keinginan dari para penggunan website tersebut atau secara garis besar pengunjung dan pengguna website tersebut adalah :
i. Mempunyai digital signature yang dapat mencegah pemakaian yang disalah gunakan.
ii. Mempunyai digital signature yang dapat diverifikasi bahwa hasil tersebut adalah miliknya.

5.2 Analisa Program

Secara garis besar program ini dibagi menjadi tiga bagian. Yang pertama adalah encode teks menjadi QR Code, kedua yaitu menyisipkan kode QR kedalam image, dan yang ketiga adalah memverifikasi QR code dengan QR Code Reader.

5.2.1 Memasukan text dan merubahnya menjadi QR Code dalam bentuk image (citra digital).

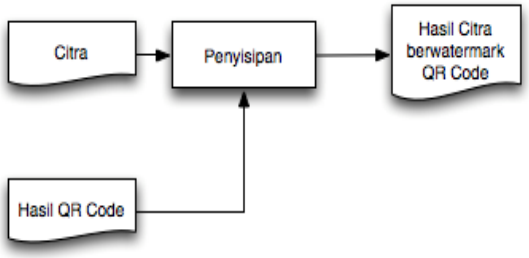
Pada proses ini dilakukan dengan menggunakan GD library dari php yang merubah text kedalam bit dan merubahnya dalam bentuk image.



Gambar Proses Generate QR code.

5.2.2 Menyisipkan Qr Code yang sudah berbentuk image tersebut kedalam image (cover image)

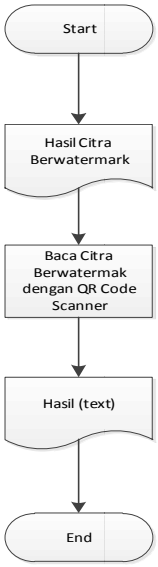
Pada proses ini dilakukan penyisipan gambar yang sudah dalam bentuk QR code kedalam cover image dengan menggunakan metode LSB. Dengan metode tersebut maka data yang dimasukan ukuranya lebih kecil dari cover image



Gambar Proses Penyisipan QR Code.

5.2.3 Proses Verifikasi QR Code dengan alat pembaca QR Code.

Pada proses ini image yang telarh terwatermark dengan QR code dapat di print, atau langsung discan di media untuk memverifikasi keaslian dari image tersebut. Sehingga bagi pengguna atau pemakai dari hasil citra terwatermark tersebut dapat membandingkan keaslian dari citra digital tersebut dan melakukan atau membuat keputusan.

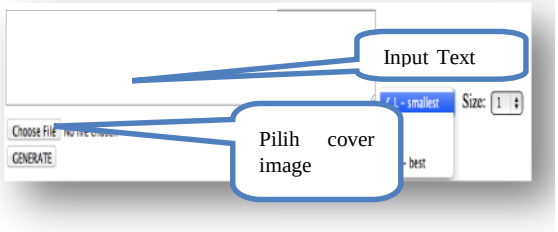


Gambar Proses Pembacaan QR Code pada Citra berwatermark.

5.3 Rancangan Program.

Program yang akan dibuat penulis adalah menggunakan bahasa pemrograman PHP. Php adalah : ***Hypertext Preprocessor [5]*** adalah bahasa skrip yang dapat ditanamkan atau disisipkan ke dalam HTML. PHP banyak dipakai untuk memrogram situs web dinamis.

Dengan menggunakan php maka dibuatlah rancangan sederhana dari interfacenya sebagai berikut:



5.4 Hasil Program

Dari rancangan yang ada, penulis melakukan konversi atau encoding text yang ada dirubah langsung menjadi QRcode dalam bentuk image (.png)

Dan langsung menempelkan/menyisipkan image tersebut dalam proses watermarking kedalam file yang akan dipilih oleh pengguna (cover Image). Contoh hasil dari proses ini adalah sebagai berikut

* Text : Universitas Budi Luhur
* Nama : Hepi Nuryadi
* Nim : 1211600125

Gambar hasil dari QR Code

Gambar Cover Image

Gambar hasil image dengan watermark

6 Kesimpulan

Kekurangan dari LSB Invertion: Dapat diambil kesimpulan dari contoh 8 bit pixel, menggunakan LSB Insertion dapat secara drastis mengubah unsur pokok warna dari pixel. Ini dapat menunjukkan perbedaan yang nyata dari *cover image* menjadi *stego image*, sehingga tanda tersebut menunjukkan keadaan dari steganografi. Variasi warna kurang jelas dengan 24 bit image, bagaimanapun file tersebut sangatlah besar. Antara 8 bit dan 24 bit *image* mudah diserang dalam pemrosesan image, seperti *cropping* (kegagalan) dan *compression* (pemampatan).

Keuntungan dari LSB Insertion : Keuntungan yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki *software* steganografi yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi *pallete* (lukisan).

Kesimpulan dari studi kasus dan pustaka yang telah dipelajari penulis adalah :

a) Dengan adanya QR Code maka dapat diverifikasi keabsahan dari citra digital tersebut.
b) QR Code dapat menyimpan lebih banyak informasi dibandingkan dengan barcode.
c) Pengguna dapat lebih leluasa untuk mengupload hasil karya mereka.
d) Program yang dibuat masih berbentuk dummy (contoh).
e) Citra digital yang dipakai masih bentuk gambar (jpeg,jpg,png)
f) Tidak menutup kemungkinan untuk menggunakan program ini untuk mencetak surat keterangan ataupun surat konfirmasi, dalam bentuk file .pdf

7 Penutup

Demikian paparan mengenai watermarking dengan steganografi yang terletak pada QR Code, dimana dengan menggunakan QR code, data yang terseimpan relative lebih banyak. Dan dapat dibaca oleh berbagai macam alat scanner untuk membaca QR Code sebagai alat untuk memverifikasi data tersebut.

Terima kasih kami panjatkan atas kehadiran Allah SWT, dan berkat rezeki Nya lah kami diberikan kesehatan untuk dapat terus menimba Ilmu. Dan semoga ilmu yang kami dapat dapat bermanfaat. Amin.

REFERENSI

[1] http://en.wikipedia.org/wiki/Digital_watermarking#cite_note-Cox-1
[2] ^ a b Ingemar J. Cox: Digital watermarking and steganography. Morgan Kaufmann, Burlington, MA, USA, 2008
[3] ^ "QR Code Essentials". Denso ADC. Retrieved 12 March 2013
[4] ^ "QR Code features". Denso-Wave. Archived from the original on 2012-09-15. Retrieved 3 October 2011
[5] http://id.wikipedia.org/wiki/PHP.