

**PROTOTYPE *DIGITAL SIGNATURE* DENGAN
TEKNIK STEGANOGRAFI DAN QR CODE**

TESIS



PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)

PROGRAM PASCASARJANA

UNIVERSITAS BUDI LUHUR

JAKARTA

2014

**PROTOTYPE *DIGITAL SIGNATURE* DENGAN
TEKNIK STEGANOGRAFI DAN QR CODE**

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (MKOM)



Oleh:

FIKI HAFANA

1211600083

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

JAKARTA

2014



PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDILUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama Mahasiswa : Fiki Hafana
Nomor Induk Mahasiswa : 1211600083
Program Studi : Magister Ilmu Komputer
Konsentrasi : Rekayasa Komputer Terapan
Fakultas/Program : Pascasarjana Universitas Budi Luhur

Menyatakan bahwa Tesis yang berjudul :

Prototipe Digital Signature Dengan Teknik Steganografi Dan QR Code

1. Merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. Saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengannormahukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta , 15Agustus 2014



(Fiki Hafana)



PROGRAM STUDI : MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDILUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Fiki Hafana
Nomor Induk Mahasiswa : 1211600083
Konsentrasi : Rekayasa Komputer Terapan
Judul : Prototype Digital Signature Dengan Teknik
Steganografi dan QR Code

Jakarta, 15 Agustus 2014

Tim Penguji :

Ketua,

(Dr.Moedjiono, M.Sc)

Anggota,

(Ir. Wendi Usino M.Sc, MM, Ph.D)

Pembimbing Utama,

(Dr.Ir.Nazori Az, M.T)

Tanda Tangan :

Ketua Program Studi

(Dr.Ir.Nazori Az, M.T)

ABSTRAK

Tanda tangan merupakan sebuah simbol yang biasa kita gunakan untuk menyatakan keabsahan suatu tindakan atau dokumen. Didalam dunia digital juga diperlukan sebuah metode untuk menyatakan sebuah keabsahan sebuah dokumen digital atau tindakan yang dilakukan, tanda tangan digital ini harus bersifat unik untuk setiap pengguna yang berarti dapat merepresentasikan penggunanya, selain itu tanda tangan dalam bentuk digital juga harus memiliki tingkat keamanan dan validasi yang baik. Dengan begitu penggunaan tanda digital dapat mempercepat proses administrasi data secara online, serta dapat menyatakan sebuah dokumen valid dan dapat dipertanggung jawabkan oleh pengguna jika dokumen tersebut terdapat tanda tangan digital milik penggunanya. Hal ini tentu saja dapat dimanfaatkan untuk membantu kemajuan dalam transaksi data secara online dan dapat melindungi hak cipta seseorang di dalam dunia digital. Melalui sebuah konsep tanda tangan digital yang umum, dalam tulisan ini penulis mencoba untuk membuat tanda tangan digital dalam bentuk visual yang terenkripsi yang menggunakan beberapa konsep dasar seperti kriptografi, steganografi dan QR Code. QR Code biasa digunakan untuk menyimpan data berupa teks, baik itu numerik, alfanumerik, maupun kode biner. QR Code banyak digunakan untuk keperluan komersil, khususnya di Jepang, biasanya berisi *link* url ke alamat tertentu atau sekedar teks berisi iklan, promosi, dan lain-lain. Pada tulisan ini dilakukan implementasi pengembangan prototipe dan studi mengenai penyisipan data terenkripsi di dalam sebuah *image* menggunakan metode *low significant bit*, kemudian dari gambar yang berisi pesan rahasia tersebut akan di-enkripsi kedua kalinya dan akan dibentuk QR Code yang nantinya akan digunakan sebagai digital signature. Oleh karena itu dilakukan analisis untuk menyisipkan pesan kedalam gambar dan kemudian mengubahnya menjadi QR Code, dengan tidak melebihi kapasitas maksimal QR Code. Solusi yang mungkin untuk diimplementasikan adalah dengan memberikan input gambar dengan ukuran pixel tertentu, kemudian dari gambar tersebut diubah ke *byte stream* dan dilakukan *enkoding* ke base64. Berdasarkan hasil pengujian data dan *image* yang kami lakukan, output berupa gambar QR Code yang berisi steganografi terenkripsi dapat digunakan sebagai alternatif tanda tangan digital yang memiliki tingkat keamanan data yang cukup baik.

Kata kunci: Low Significant Bit, QR Code, Steganografi, Digital Signature, Visual Kriptografi

ABSTRACT

Signature is a symbol that we use to assert the validity of an act or documents. In the digital world also needed a method to proof a validity of a digital document or the action taken, the digital signature must be unique for each user which means it can represent users, in addition to the signature in digital form also must have a good security and better validation. Thus using a digital sign can speed up the administrative data process, and can state a valid document and may be subject to the user if the document contained a digital signature belongs to its users. Of course it can be used to help advance the online data transactions and can protect copyright in the digital world. Through a concept of a common digital signature, in this paper the author tries to create a digital signature in a visual form that is encrypted using some basic concepts such as cryptography, Steganografi and QR Code. QR Code commonly used to store data in the form of text, be it numeric, alphanumeric, or binary code. QR Code is widely used for commercial purposes, especially in Japan, usually contains a link url to a specific address or simply text containing advertising, promotion, and others. In this paper the development of a prototipe implementation and conducted a study on the insertion of encrypted data in an image using a low significant bit, then from the image that contains the secret message will be encrypted for a second time and then QR Code will be established that will be used as a digital signature. Therefore the analysis to insert messages into images and then convert it into a QR Code, with a maximum capacity not exceeding QR Code. A possible solution to implement is to provide the input image with a certain pixel size, then from the image is converted into a byte stream and carried to the base64 enencoding. Based on the results of the testing data and images that we do, the output of the QR Code images containing encrypted Steganografi can be used as an alternative to digital signatures that have high levels of data security is quite good.

Keyword: Low Significant Bit, QR Code, Steganografi, Digital Signature, Visual Cryptography

KATA PENGANTAR

Alhamdulillahirabbil'aalamin puji dan syukur penulis panjatkan kehadiran Allah SWT atas rahmat, karunia, dan berbagai kemudahan yang diberikan kepada penulis. Selama menempuh pendidikan Magister, penulis juga memperoleh dukungan dan bantuan dari banyak pihak. Oleh karena itu, penulis ingin mengucapkan banyak terima kasih kepada:

1. Kedua orang tua, yang selalu mendukung dan mendoakan saya.
2. Dr. Moedjiono, M.Sc, Direktur Program Pascasarjana Universitas Budi Luhur.
3. Dr. Ir. Nazori AZ, MT, Ketua Program Studi Magister Ilmu Komputer Universitas Budi Luhur.
4. Dr. Ir. Nazori AZ, MT selaku Dosen Pembimbing tesis pada Program Studi Pascasarjana Magister Ilmu Komputer Universitas Budi Luhur.
5. Seluruh Dosen, Staff Karyawan dan Karyawanati Universitas Budi Luhur.
6. Keluarga tercinta yang selalu memberikan dukungan segenap hati.
7. Teman-teman seangkatan yang telah sama-sama berjuang.

Telah banyak pengalaman, ilmu, dan pengetahuan yang penulis dapatkan selama menyelesaikan studi di Universitas Budi Luhur. Memiliki kesempatan untuk menempuh pendidikan di Universitas Budi Luhur merupakan sebuah kehormatan yang besar bagi penulis.

Penulis juga menyadari bahwa tesis ini masih jauh dari sempurna. Karenanya, komentar, masukan maupun kritik untuk perbaikan di masa mendatang sangat diharapkan oleh penulis.

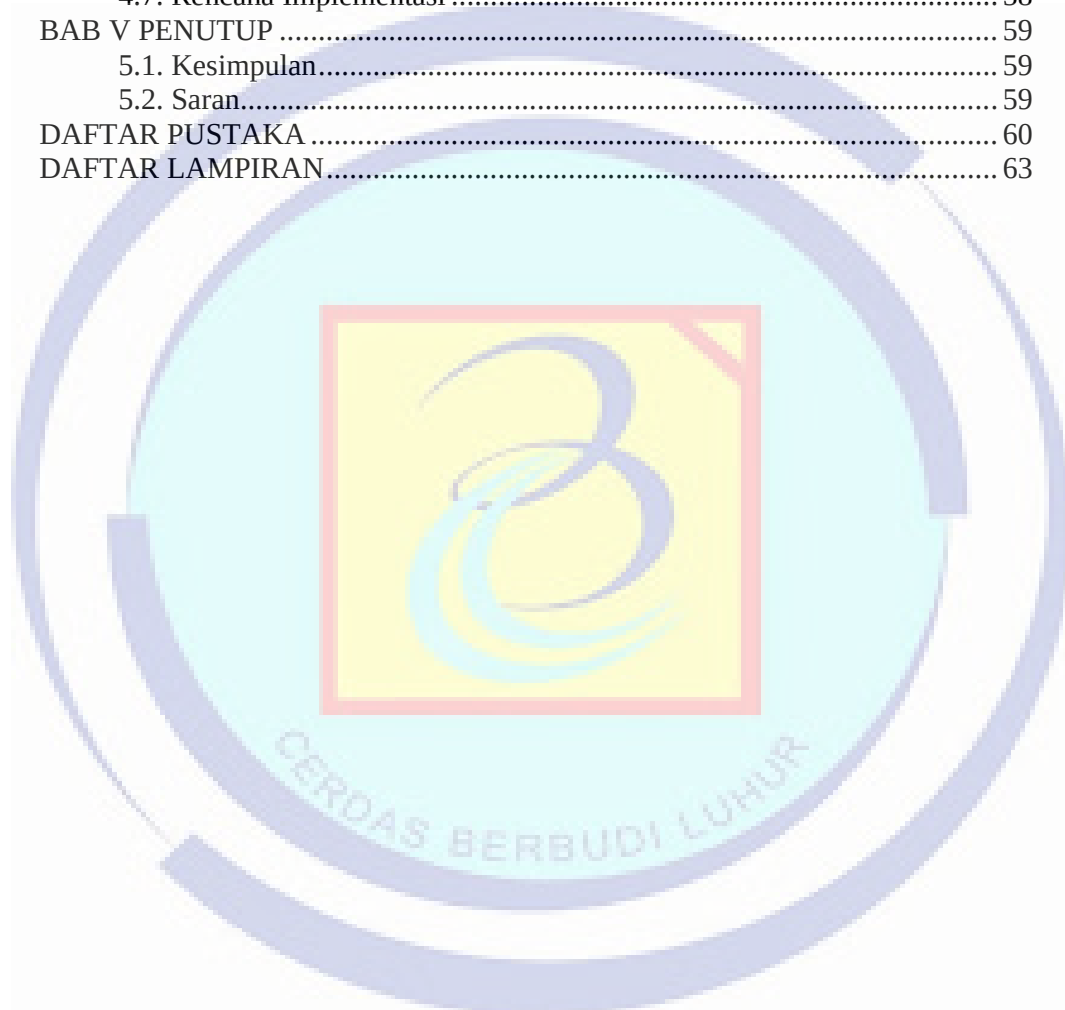
Jakarta, 14 September 2014

Penulis

DAFTAR ISI

LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN.....	ii
ABSTRAK	iii
ABSTRACT	iv
KATA PENGANTAR	v
DAFTAR ISI	VI
DAFTAR GAMBAR.....	viii
DAFTAR TABEL	ix
BAB I PENDAHULUAN	1
1.1.Latar Belakang.....	1
1.2.Masalah Penelitian.....	3
1.2.1.Identifikasi Masalah	3
1.2.2.Pembatasan Masalah.....	3
1.2.3.Rumusan Masalah	4
1.3.Tujuan dan Manfaat Penelitian.....	4
1.3.1.Tujuan Penelitian.....	4
1.3.2.Manfaat Penelitian.....	4
1.4.Sistematika Penulisan	5
1.5.Daftar Pengertian Istilah	6
BAB II LANDASAN TEORI	8
2.1.Tinjauan Pustaka.....	8
2.1.1.Konsep dasar QR Code.....	8
2.1.2.Steganografi	10
2.1.3.Kriptografi.....	14
2.1.4.Tanda Tangan Digital	15
2.1.5.Extreme Programming.....	17
2.2.Tinjauan Studi.....	23
2.3.Tinjauan Objek Penelitian.....	24
2.3.1. Objek Penelitian	24
2.4.Hardware dan Software yang Akan Digunakan	26
2.5.Kerangka Konsep.....	27
2.6.Hipotesis.....	28
BAB III METODOLOGI DAN RANCANGAN PENELITIAN.....	29
3.1. Metode Penelitian	29
3.2.Teknik Perancangan.....	30
3.3.Teknik Konstruksi.....	30
3.4.Langkah Penelitian	30
3.5.Jadwal Penelitian	33
BAB IV ANALISIS, INTERPRETASI DAN IMPLIKASI PENELITIAN.....	34
4.1. Analisis dan Implementasi Sistem	34
4.1.1. Pengumpulan Data.....	35
4.1.2. Prototipe GUI Digital Signature QR Code	38

4.2. Pengujian Sistem.....	40
4.3. Hasil Pengujian Proses Dekoding Dari QR Code <i>Signature</i> Menjadi Teks.....	49
4.4. Hasil Pengujian Kualitas Keamanan Pada <i>Digital Signature</i> QR Code Menggunakan <i>Brute Force</i>	50
4.5. Interpretasi.....	56
4.6. Implikasi Penelitian	57
4.6.1. Implikasi Aspek Sistem	57
4.6.2. Implikasi Aspek Penelitian Lanjut	58
4.7. Rencana Implementasi	58
BAB V PENUTUP	59
5.1. Kesimpulan.....	59
5.2. Saran.....	59
DAFTAR PUSTAKA	60
DAFTAR LAMPIRAN.....	63



DAFTAR GAMBAR

Gambar II.1	Struktur QR Code.....	9
Gambar II.2	Ilustrasi Steganografi.....	10
Gambar II.3	Alur Proses Enkripsi dan Dekripsi.....	14
Gambar II.4	Sistem Kripto Simetrik.....	15
Gambar II.5	Sistem Kripto Asimetrik.....	15
Gambar II.6	Aspek Dasar Extreme Programming.....	18
Gambar II.7	Form Tanda Tangan <i>Request Budget</i>	25
Gambar II.8	Kerangka Konsep Penelitian.....	27
Gambar III.1	Langkah Penelitian.....	31
Gambar IV.1	Kerangka Pengembangan Model	34
Gambar IV.2	Tampilan Menu Input File dan Cover <i>Image</i>	38
Gambar IV.3	Tampilan Menu Otentikasi <i>Digital Signature QR Code</i>	39
Gambar IV.4	Kesalahan Pada Saat Serangan Bruto Force.....	51
Gambar IV.5	Kesalahan Pada Otentikasi Data	52



DAFTAR TABEL

Tabel II.1	Kapasitas Data QR Code	9
Tabel II.2	Tinjauan Studi.....	23
Tabel II.3	Spesifikasi Komputer Untuk Penelitian	26
Tabel III.1	Jadwal Penelitian	33
Tabel IV.1	Contoh Form Digital dan Nilai Hash	36
Tabel IV.2	Sampel Gambar Sebagai Cover <i>Image</i>	36
Tabel IV.3	Struktur Pesan Yang Disisipkan	37
Tabel IV.4	Pengujian Sistem Pada Gambar Hitam Putih	40
Tabel IV.5	Hasil Pengujian Dengan Cover <i>Image</i> Hitam Putih.....	41
Tabel IV.6	Hasil pengujian Steganografi Dengan Cover <i>Image</i> Berwarna...	44
Tabel IV.7	Hasil Pengujian Gambar Stego Setelah Berhasil Di Encode ke QR Code	46
Tabel IV.8	Hasil Uji Coba Enkoding Digital Signature QR Code.....	48
Tabel IV.9	Hasil Uji Coba Dekoding Digital Signature QR Code.....	49
Tabel IV.10	Hasil Pengujian Menggunakan Serangan <i>Brute Force</i>	53
Tabel IV.11	Hasil Pengujian Qr Code Robustness	53
Tabel IV.12	Hasil Pengujian <i>Stego Image</i> Robustness	54
Tabel IV.13	Proses Ekstraksi Data Setelah Mengalami Serangan	55
Tabel IV.14	Kebutuhan Software.....	57
Tabel IV.15	Kebutuhan Hardware	58

DAFTAR PUSTAKA

- [1], Akshay Choche and Hamid R. Arabnia, "A Methodology to Conceal QR Codes for Security Applications." Proceedings of the International Conference on Information and Knowledge Engineering (IKE'11): July. 2011.
- [2], R. Barker, Elain, etc., NIST SP 800-21: *Guideline for Implementing Cryptography In the Federal Government*, New York: NIST, 2005.
- [3], Beck. Kent, "Extreme Programming Explained: Embrace Change", Addison-Wesley. 1999.
- [4], Denso Wave, "QR Code Structure", 2010, www.QR Code.com (diakses 20 Mei 2014)
- [5], Omprasad Deshmukh dan Shefali Sonavane, "Multi-Share Crypt-Stego Authentication System", International Journal of Computer Science and Mobile Computing Vol.2 Issue. 2, pg. 80-90, February-2013.
- [6], Sugiyono, Metode Penelitian Kuantitatif, Kualitatif dan R&D, Jakarta: Alfabeta, 2009.
- [7], Scheiner. Bruce, "Applied Cryptography", 2nd ed., John Wiley & Sons, Inc
- [8], Tukenov and Tlueov, "Steganography Process", 2003, www.myshared.ru (diakses 25 Mei 2014)
- [9], Vikram, "Steganography", 2004, www.myshared.ru (diakses 25 Mei 2014)