STUDI PENERAPAN *IMAGE WATERMARKING* PADA KEAMANAN *ePASSPORT*

Riani Rilanda – NIM : 13505051

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if11051@students.if.itb.ac.id

Abstrak

Watermarking digital adalah suatu teknik untuk menanamkan pesan khusus pada sebuah pesan yang menunjukkan pembuat pesan atau pengguna yang berhak akan pesan tersebut, biasanya pesan khusus yang ditambahkan adalah pesan yang merupakan ciri khas dari pembuat pesan. *Watermarking digital* memiliki beberapa varian, tergantung dari media pesan yang digunakan, diantaranya *image watermarking. Image watermarking* adalah *watermarking digital* yang diterapkan pada pesan dengan media gambar.

ePassport merupakan paspor yang mengandung *electronic chip,* dimana *electronic chip* tersebut mengandung informasi yang sama dengan yang tertera pada halaman paspor. Di dalam *chip* juga terdapat foto diri dari pemilik paspor.

Makalah ini menjelaskan dan membandingkan teknik penerapan *image watermarking* pada *ePassport* yang dapat digunakan sebagai otentifikasi dari *ePassport* tersebut. Metode yang akan diperbandingkan adalah *image watermarking* menggunakan *spread spectrum*, *quantization*, dan *amplitude modulation.*

***Kata kunci**: Image watermarking, ePassport.*

1. Pendahuluan

Paspor yang sudah ada sebelumnya berupa sebuah kertas kecil dengan kepala negara yang memberikan *subjects* dan *favoured foreigners*, dan memberikan hak akses bagi pemilik untuk melakukan perjalanan ke luar negaranya secara bebas. Kemudian kertas tersebut berkembang menjadi sebuah dokumen kecil seperti yang sudah diketahui sekarang ini. Di akhir 2006, paspor akan mengandung *computer chips* dan berkerja dengan perangkat lunak *facial mapping* untuk memverifikasi pemegang paspor tersebut.

Di awal 2007, *the Identity and Passport Service* (IPS) telah berhasil mengenalkan rangkaian prosedur dan sistem untuk mencegah pemalsuan identitas dan paspor. Paspor baru ini berjudul *biometric passport* atau *ePassport*. *Biometric passport memiliki* desain baru dan fitur keamanan yang telah dikembangkan dan tidak ada di dalam paspor yang sebelumnya. Halaman paspor yang baru memiliki desain yang rumit dan *chip* antena.

Banyak kelebihan paspor ini dibandingkan paspor yang terdahulu, namun tetap saja masih banyak serangan yang mengenai paspor ini. Oleh karena itu, pada makalah ini akan dibahas mengenai bagaimana mengamankan paspor, terutama untuk *digital signature,* sehingga dapat dipastikan bahwa paspor tersebut memang dikeluarkan oleh negara yang tertulis di halaman awal dan paspor tidak pernah diubah sebelumnya sehingga dapat dipastika informasi dari identitas pemilik benar. *Digital signature* tersebut dapat dilakukan dengan melakukan *image watermarking* pada halaman-halaman paspor.

Image watermarking dapat dilakukan dengan berbagai macam metode, namun pada makalah kali ini hanya akan dibahas tiga buah metode, *spread spectrum, quantization* dan *amplitude modulation*. Dari ketiga metode tersebut, akan dicari metode mana yang paling pas, dari segi *secure* dan *robust* menahan serangan serta kualitas citra hasil, untuk digunakan sebagai *digital signature* pada *ePassport*.

2. Metode *Image Watermarking*

Image watermarking yang handal harus memiliki sifat *robust* dan *hidden* yang tinggi. Adanya *trade-off* untuk mendapatkan *robust* dan *hidden watermarking* menyebabkan sulit mendapatkan teknik *watermarking* yang handal.

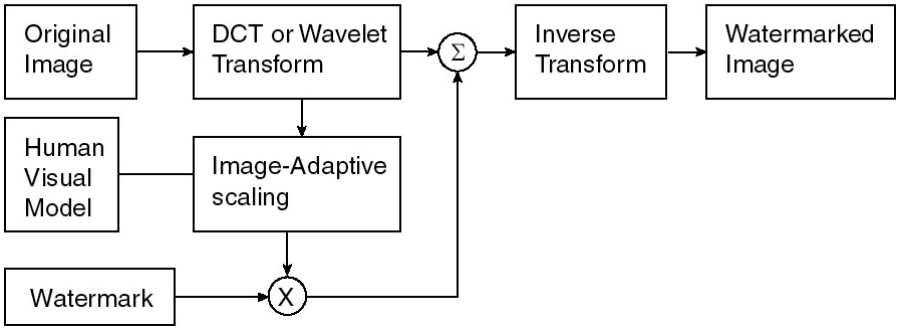
Oleh karena itu akan dilakukan studi terhadap ketiga metode untuk melakukan *image watermarking* yaitu dengan *spread spectrum, quantization* dan *amplitude modulation* sehingga didapatkan metode yang paling *robust* dan *hidden* untuk nantinya diterapkan kepada keamanan *ePassport*.

2.1 Metode *Spread Spectrum*

Metode *spread spectrum* digunakan untuk menyebarkan energi dari citra *watermark* ke seluruh frekuensi, sehingga energi pada sebuah frekuensi akan semakin kecil dan *undetecable,* dengan demikian akan menambah hidden citra *watermark*.

Spread spectrum menjamin keamanan dari citra *watermark* karena lokasi dari watermark yang sudah disebar tidak jelas. Selain itu, *spread spectrum* juga menjamin *robustness* dari citra *watermark* karena untuk mengeliminasi sebuah *watermark* serangan harus ditujukan kepada seluruh kemungkinan frekuensi sehingga akan sangat banyak kemungkinan serangan yang harus dilakukan.

Komunikasi *spread spectrum* menggunakan *narrow-band signal* yang ditransmisikan dengan *bandwidth* yang cukup besar sehingga energi sinyal yang ada pada sinyal frekuensi *undetecable.*



Gambar 1 *Spread Spectrum*

Cara kerja *spread spectrum* :

- Untuk menempatkan *watermark* berukuran n ke dalam citra NxN, NxN DCT dari citra akan dikomputasi dan *watermark* akan ditempatkan ke koefisien *magnitude* terbesar dari citra yang diubah sebanyak n.
- *Watermark* mengandung sekuens dari bilangan *real* $X = x_1, x_2, x_3, ..., x_n$, dimana setiap nilai dari x_i dipilih secara acak tergantung kepada N(0,1) : *normal distribution assumption*.
- *Watermark insertion :* saat memasukkan x ke dalam v akan menghasilkan v', dengan scaling parameter berupa α dimana α akan mendeterminasikan nilai tambahan untuk merubah nilai x ke dalam v.

(1) $v_i' = v_i + \alpha x_i$
(2) $v_i' = v_i (1 + \alpha x_i) = v_i + \alpha x_i v_i$
(3) $v_i' = v_i (e \alpha x_i)$ *or* $\log v_i' = \log v_i + \alpha x_i$

- Determinasi nilai α : nilai α yang tunggal mungkin tidak dapat diaplikasikan untuk mengubah semua menjadi v_i.

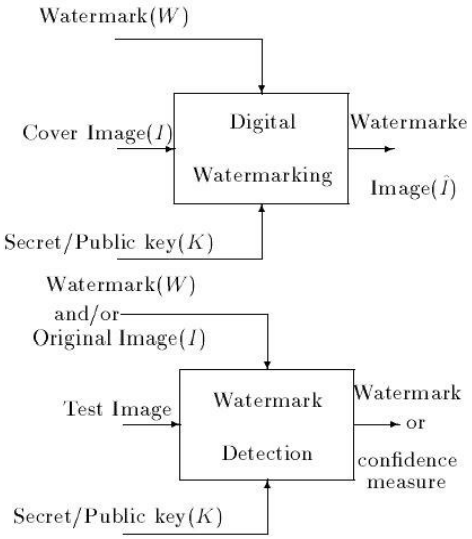
$v_i' = v_i (1 + \alpha_i x_i)$

dimana α_i dapat dilihat sebagai *relative measure* dari banyaknya perubahan v_i yang harus dirubah untuk mendapatkan kualitas terbaik.

- Pilihan n : pilihan dari n merupakan indikasi dari tingkat dimana watermark disebar pada komponen citra yang relevan. Pada umumnya, apabila nilai dari n semakin tinggi maka nilai perubahan yang harus dilakukan akan semakin kecil dan kemampuan untuk diserang semakin rendah.

2.2 Metode *Quantization*

Image watermarking dengan *vector quantization* adalah penambahan bit *watermark* ke dalam dimensi informasi dari variable dimensi blok rekonstruksi dari *cover* atau citra masukan. Ekstraksi *watermark* untuk *oblivious watermarking* akan diselesaikan dengan cara mengidentifikasi dimensi dari blok rekonstruksi.



Gambar 2 *Virtual Quantization*

Cara kerja *vector quantization* :

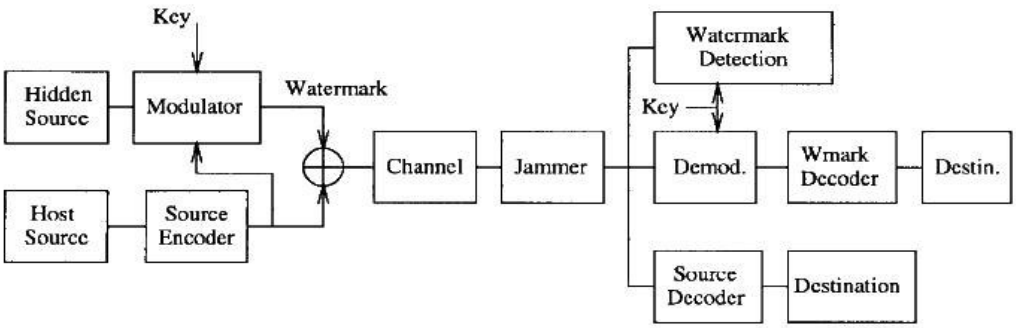
- Partisi *codebook* menjadi beberapa *cluster*, bersifat sebagai *codevectors* yang tertutup. Setiap pasang *codevectors* di dalam *cluster* memiliki nilai ambang bawah *Euclidean distance* yang pasti.
- Masukkan *codevectors* sebagai blok input pada beberapa cluster, dengan cluster index *i* dan misalkan ukuran cluster sebesar $2^{n(i)}$
- $^{n(i)}$ bit integer g, informasi *watermark* akan ditambahkan dengan mengtransmisikan sebuah indeks yang berkoresponden ke $(j+g)\ mod\ 2^{n(i)}$*-th codevectors* di dalam cluster yang sedang dilihat.

Skema yang diajukan di dalam *vector quantization* ini menghasilkan *watermark* yang tidak dapat dilihat secara langsung dengan visual. Identifikasi kerusakan yang terjadi pada citra juga dapat dideteksi dengan mudah, yaitu dengan mencocokan index yang diterima dengan *the best match* index, apabila tidak berada pada *cluster* yang sama berarti citra telah dirusak.

Skema ini aman, efisien dan *robust* karena ekstrasi dari skema ini membutuhkan citra *original* dari citra *watermark* selain itu partisi *codebook* akan menjadi *secret key.* Akan tetapi, biaya yang harus dikeluarkan untuk membuat, mendeteksi dan memverifikasi citra watermark dengan metode ini cukup besar.

2.3 Metode *Amplitude Modulation*

Amplitude modulation akan secara *multiple* memasukkan bit citra *watermark* ke dalam nilai *pixel* yang telah dimodifikasi di dalam *blue channel*. Modifikasi ini sebanding dengan antara *luminance* dan *additive* atau *subtractive*, tergantung pada nilai dari bit. Metode ini tahan terhadap serangan klasik, seperti *filtering* dan serangan *geometrical*. Lebih jauh lagi, *watermark* yang dihasilkan dari metode ini dapat diekstrasi tanpa citra aslinya.



Gambar 3 ***Amplitude Modulation***

Cara kerja *amplitude modulation* :

- *Single bit embedding :* anggap *s* sebagai single bit yang akan ditambahkan pada citra $I = \{R, G, B\}$ dengan $p = (i, j)$ sebagai posisi *pseudo-random* di dalam *I*. Posisi ini tergantung pada *secret key K,* yang digunakan sebagai tempat untuk generator nomor *pseudo-random*. *s* ditambahkan ke dalam *blue channel* B yang sudah dimodifikasi dengan posisi *p* dari fraksi luminance $L = 0{:}299R + 0{:}587G + 0{:}114B$ sebagai berikut :

  $B_i \leftarrow B_{ij} + (2s - 1)L_{ij}q$

  Dimana *q* adalah konstanta yang mendeterminasi kekuatan dari *watermark*.

- *Single bit retrieval :* dalam tujuan untuk mengekstraksi bit yang sudah ditambahkan, prediksi nilai awal dari *pixel* yang mengandung informasi dibutuhkan. Prediksi didasarkan pada kombinasi linear dari nilai *pixel* di sekitar nilai *p.*

  Fungsi *embedding* dengan fungsi *retrieval* tidak simetri, jadi fungsi *retrieval* bukan merupakan *inverse* dari fungsi *embedding*. Meskipun demikian, *retrieval* yang dihasilkan akan menjadi mirip namun tidak dijamin. Untuk mengurangi kesalahan dalam proses *retrieval*, bit ditambahkan secara *multiple* (beberapa kali).

- *Multiple embedding :* untuk meningkatkan performa dari *retrieval*, bit dapat ditambahkan *n* kali di lokasi yang berbeda. *n* posisi ini *p1, ..., pn* ditentukan oleh sekuen *pseudo-random*. Seperti sebelumnya, generator nomor *pseudo-random* diinisialisasi dengan nilai yang sama dengan *secret key k.*

  Dengan menggunakan *density* parameter ρ, redundansi kontrol bisa membuat ukuran dari citra bebas. *Density* ini memberikan probabilitas dari *pixel* tunggal manapun yang digunakan untuk penambahan. Nilainya berkisar antara 0 dan 1, dimana 0 berarti tidak ada informasi yang ditambahkan, dan 1 berarti informasi ditambahkan di setiap *pixel*. Jumlah dari *pixel* yang digunakkan sama dengan ρ kali ditambah dengan jumlah total *pixel* di dalam citra.

- *Extension to an m-bit signature :* penambahan pada *m*-bit *signature* $S = \{s_0, ..., s_{m-1}\}$ yang terus membuat $p_1, ..., p_n$ menjadi *n* posisi yang dapat dipilih untuk penambahan *multiple* dari bit tunggal. Untuk setiap posisi dari tanda bit dipilih secara acak dan lalu ditambahkan.

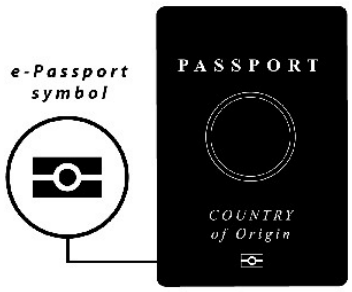
  Diberikan *m-2* bit *string* untuk ditambahkan, 2 bit sudah ditambahkan ke dalam *string* sebagai form untuk *m*-bit *signature.* Kedua bit ini selalu diset menjadi 0 atau 1.

3. *ePassport*

3.1 Penjelasan

ePassport merupakan paspor yang mengandung *electronic chip,* dimana *electronic chip* tersebut mengandung informasi yang sama dengan yang tertera pada halaman paspor. Di dalam *chip* juga terdapat foto diri dari pemilik paspor. *ePassport* dapat dikatakan sangat aman karena didalamnya terdapat berbagai layer dari keamanan

yang mencegah dari duplikasi dokumen serta pembuatan dokumen palsu.

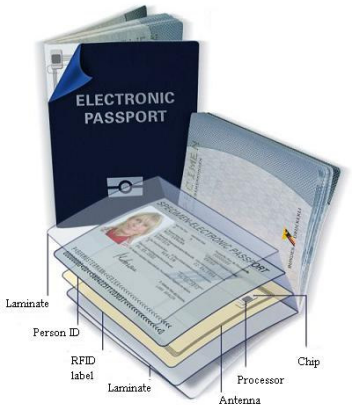


Gambar 4 *ePassport*

Keuntungan dari penggunaan *ePassport* diantaranya adalah dapat mengidentifikasi wisatawan/turis secara aman, menyediakan proteksi dari pencurian identitas, proteksi privasi dari wisatawan/turis dan menyulitkan bagi perubahan data dari dokumen guna menambah keuntungan.

3.2 Keamanan dari *ePassport*

Keamanan *ePassport* digunakan untuk menunjukkan apakah paspor yang dibawa adalah asli beserta data-data didalamnya atau telah dirusak/dipalsukan. Selain itu, keamanan dari *ePassport* juga ditujukan untuk mengetahui apakah pemegang dari paspor tersebut adalah pemilik asli dari paspor tersebut. Keamanan dari ePassport dilakukan pada dua aspek, pertama, *originality protection* yang didapat dari *paper feature* dan yang kedua, *data protection* yang didapat dari *biometric feature*.



Gambar 5 Detil keamanan *ePassport*

Secara umum, keamanan *ePassport* menggunakan dua lapis keamanan. Hal ini berguna dalam pencegahan pemalsuan dan penggelapan paspor. Kedua lapisan keamanan tersebut adalah :

a. Proteksi dari pembacaan data paspor yang tidak semestinya.
b. Penguncian data menggunakan *public key infrastructure* yang menyediakan proteksi terhadapa perubahan data. Proteksi ini merupakan enkripsi digital yang membantu memvalidasi keaslian dari data.

Selain dari ketiga lapisan keamanan yang secara umum sudah digunakan, masing-masing negara yang mengeluarkan *ePassport* memiliki metode keamanan berbeda. Berikut akan diberikan metode keamanan apa saja yang digunakan oleh USA dan Malaysia dalam mengamankan *ePassport*.

3.2.1 *United States of America ePassport*

Electonic chip dari *ePassport United States of America* menyimpan gambar dari foto pemilik paspor, data dari paspor, dan personal data dari pemilik paspor selain itu *chip* masih memiliki kapasitas untuk menyimpan data tambahan apabila suatu saat dibutuhkan seperti *identifier biometric*, *fingerprints* atau *retina scans*.

Data yang terdapat didalam *chip* dapat di-*scan* oleh manusia dengan tujuan mempercepat proses dari imigrasi. Jadi paspor tidak butuh untuk dimasukkan ke dalam mesin pembaca untuk pembacaan data yang terdapat di dalamnya.

Gambar 6 USA *ePassport*

3.2.2 *Malaysian ePassport*

Malaysia adalah negara pertama yang mengangkat persoalan mengenai *ePassport* pada tahun 1998 karena sebelumnya sudah terdapat teknologi yang serupa pada kartu identitas di Malaysia, yaitu MyKad.

Data *biometric* yang terdapat pada *ePassport* Malaysia adalah digital foto yang merupakan foto wajah dari pemilik paspor tersebut selain itu terdapat gambar dari kedua sidik ibu jari pemilik. Untuk tambahan pada data *biometric* dan informasi personal yang terdapat pada halaman informasi, *electronic chip* juga mencatat *track* dari perjalanan pemilik paspor dari sepuluh perjalanan yang terakhir dilakukan dan penyimpanan ini terdapat pada *border control points* Malaysia.

Pembacaan data yang terdapat pada *chip* harus dilakukan menggunakan mesin pembaca yang terdapat pada kantor imigrasi Malaysia dan negara-negara lain seperti USA dan UK.

4. Penerapan *Image Watermarking* pada *ePassport*

Pada pembahasan sebelumnya telah disebutkan ketiga metode *image watermarking* yang akan diperbandingkan mana yang lebih baik untuk diterapkan pada *ePassport* sebagai *digital signature* yang dapat memastikan bahwa benar paspor tersebut dikeluarkan oleh negara yang tertulis.

Untuk metode yang pertama, *spread spectrum* memiliki kemudahan di dalam pengimplementasiannya, selain itu keamanan dan *robustness*-nya juga dapat terjamin. Serangan yang dilakukan terhadap metode ini harus dilakukan secara *brute force*, karena proses penyebaran dilakukan secara *random*. serangan *brute force* ini akan sulit dilakukan mengingat besarnya kemungkinan yang harus dilakukan, sehingga metode ini dapat dikatakan cukup aman. Citra keluaran dari metode ini tidak mengalami penurunan kualitas dari citra aslinya.

Untuk metode yang kedua, *vector quantization* memiliki keunggulan di bidang pengecekan citra keluaran, citra keluaran dapat dilihat secara langsung oleh manusia, hal ini berkaitan dengan kualitas citra keluaran yang tentunya berbeda dengan citra aslinya. Selain itu, metode ini memudahkan dalam identifikasi kerusakan, dapat dengan mudah mengetahui apakah citra keluaran tersebut telah dirusak atau belum. Metode ini aman dan *robust* karena untuk mengekstraksi metode ini dibutuhkan citra asli sebelum mengalami *watermarking*, sehingga akan sulit dilakukan serangan untuk mengembalikan citra yang telah dirusak ataupun mengembalikan ke citra aslinya. Kekurangan dari metode ini adalah biaya untuk implementasi, deteksi dan ekstraksi yang tinggi.

Untuk metode yang ketiga, *amplitude modulation* merupakan metode yang aman dikarenakan bit yang diolah akan diolah berulang, selain itu ekstraksi dengan pengulangan pengolahan bit tersebut juga dipermudah. Selain itu, metode ini juga *robust* terhadap serangan klasik seperti *filtering* dan serangan *geometric* seperti *rotate*.

Digital signature dari sebuah *ePassport* membutuhkan metode yang tidak terlalu sulit diimplementasikan sehingga watermarking tersebut dapat dikerjakan oleh semua negara, tidak hanya negara dengan teknologi tinggi. Tidak mudah diserang atau diubah, hal ini jelas karena apabila *ePassport* diserang maka informasi didalamnya akan menjadi *stale* dan tidak dapat digunakan. Pengubahan yang terjadi dapat diketahui, untuk memastikan apakah informasi yang ada benar atau tidak, selain itu dibutuhkan metode yang menghasilkan citra keluaran yang tidak terlalu berbeda dari citra asli , citra *watermark* tidak dapat dibaca secara langsung tanpa mesin pembaca, hal ini agar *ePassport* tidak dapat dibajak dengan peniruan citra dari *digital signature* tersebut. Oleh karena itu, apabila dilihat dari kelebihan dan kekurangan masing-masing metode, *spread spectrum* merupakan metode yang paling cocok untuk digunakan untuk melakukan *image watermarking* sebagai *digital signature* dari sebuah *ePassport*.

5. Kesimpulan

Image watermarking sebagai salah satu teknologi proteksi terhadap konten digital dalam kajiannya dapat digunakan untuk proses verifikasi kebenaran paspor yang

dipegang oleh pemilik. Selain itu, *image watermarking* ini juga dapat memberi tahu ketika sebuah paspor telah dirusak, dimana kerusakan tersebut dapat meragukan keabsahan dari informasi yang terdapat di dalam paspor tersebut.

Metode dari *image watermarking* yang paling sesuai dengan kebutuhan sebuah ePassport adalah *spread spectrum* dimana keamanan, kemudahan dan *robustness*nya sesuai dengan kebutuhan.

Dalam kaitannya dengan verifikasi tersebut, *image watermarking* tidak hanya pada aplikasi *ePassport* namun juga dapat dikembangkan pada aplikasi-aplikasi lainnya.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. 2006. Diktat Kuliah IF3058 Kriptografi.

[2] Home Office. 2008. *Identity and Passport Service*. *http://www.ips.gov.uk/passport* . Tanggal akses 12 Maret 2009.

[3] Homeland Security. 2008. *ePassport.* *http://www.dhs.gov/* . Tanggal akses 12 Maret 2009.

[4] *Digital watermarking*. http://www.cosy.sbg.ac.at. Tanggal akses : 31 Maret 2009.

[5] *Passport*. http://www.dfat.gov.au/dept. Tanggal akses : 31 Maret 2009.

[6] http://www.computerworld.com. Tanggal akses : 31 Maret 2009.

[7] Sirait, Rummi. Teknologi *Watermarking* pada Citra Digital. http://jurnal.bl.ac.id/wp-content/uploads/2007/01/TELTRON-v3-n1-artikel4-april2006.pdf. Tanggal akses : 1 April 2009.

[8] Martin, Kutter and friends. *Digital Watermarking of Color Images Using Amplitude Modulation*. http://adsabs.harvard.edu/abs/1998JEI....7..326K. Tanggal akses : 1 April 2009.

[9] Martin, Kutter. *Digital Signature of Color Image Using Amplitude Modulation.* https://eprints.kfupm.edu.sa/35019/1/35019.pdf. Tanggal akses : 1 April 2009.