ANALISIS ALGORITMA SHA-512 DAN WATERMARKING DENGAN METODE LEAST SIGNIFICANT BIT PADA DATA CITRA

Jakaria Sembiring
Manajemen Informatika, Politeknik Unggul LP3M
Jl. Iskandar Muda No. 3EF, Medan, 20155
Telp : +62 61 - 4156355
E-mail : jakarias@yahoo.com

Abstrak

Pesan ataupun informasi yang memiliki nilai kerahasiaan perlu mendapatkan perhatian khusus karena nilai pesan ataupun informasi tersebut sangat penting misalnya informasi tanda kepemilikan, informasi intelejen, militer, dan informasi penting dan rahasia lainnya. Maka perlu adanya teknik atau metode mengamankan data ataupun informasi tersebut yaitu menggunakan kriptografi dan atau watermark. Penelitian ini untuk menganalisa implementasi algoritma SHA-512 dan watermark metode least significant bit pada data citra, untuk mengetahui bagaimana kualitas dan perbedaan citra sebelum dan sesudah disisipkan teks, untuk mengetahui performa kriptografi SHA-512 dan watermark dengan metode least significant bit terhadap data citra.Percobaan dilakukan dengan meng-hashing pesan teks rahasia dengan panjang pesan maksimal 250 karakter, karakter yang telah di-hashing dikonversi menjadi bit, setiap bit karakter tersebut disisipkan ke data citra dengan menggunakan metode least significant bit sehingga menghasilkan watermark yang tersembunyi didalam citra tersebut, hasil yang diharapkan adalah data citra tidak berubah namun pesan teks telah disisipkan.

Kata kunci*:kriptografi, wartermark, hashing, SHA, LSB*

Abstract

Messageorinformationthathas valueconfidentialityneeds special attentiondue tothe value ofthe messageorinformation is veryimportantasa sign of ownershipinformation, intelligence, military, andotherimportant and confidentialinformation. Hence need fortechniquesormethods ofsecuringdata orinformation, theuse ofcryptographyandwatermark. This research istoanalyzethe implementation ofthe SHA-512 algorithmandwatermarkmethod ofleast significantbits oftheimage data, to determinehow theimagequalityandthe differencebeforeand after insertedtext, andto determine theperformance ofSHA-512 cryptographyandwatermarkwith themethod ofleast significantbits oftheimage data. Experimentsdoneby clickinghashinga text messagewith thesecretmessage lengthof 250characters, characters that have beenin-hashing converted intobits, each bit ofthecharacteris insertedintothe image datausing theleast significantbits givingthe hiddenwatermarkintheimages,the expected resultis theimage datais notchanged but thetexthas beeninserted.

Keyword*: cryptography, watermark, hashing, SHA, LSB*

1. PENDAHULUAN

Zaman sekarang ini banyak orang menyimpan pesan pada media digital misalnya disimpan pada media gambar namun pesan tersebut merupakan pesan rahasia sehingga pemilik menginginkan agar beberapa orang saja yang dapat mengetahui isi pesan tersebut. Pesan ataupun informasi yang memiliki nilai kerahasiaan perlu mendapatkan perhatian khusus karena nilai pesan ataupun informasi tersebut sangat penting misalnya informasi tanda kepemilikan, informasi intelejen, militer, dan informasi penting dan rahasia lainnya. Oleh karena itu perlu adanya teknik atau metode untuk mengamankan data ataupun informasi tersebut.

Berbagai jenis metode pengamanan pesan dan pengamanan hak ciptadata digital telah tersedia. Salah satu metode yang digunakan untuk mengatasi masalah tersebut adalah digital *Watermarking*. *Watermarking* merupakan suatu bentuk dari *Steganography* (teknik untukmenyembunyikan suatu informasi pada suatu media tanpa perubahan yang berartipada media tersebut). Teknik *Watermarking* akan menyisipkan informasi digital yang disebut *watermark*ke dalam suatu data digital yang disebut *carrier*. *Watermark* yang disisipkan dapat berupa teks biasa, audio,citra maupun video tergantung dari kemampuan media yang ditumpanginya.

Penambahan *watermark* ke dalam citra digital tanpa mempengaruhi kualitas data citra dapat digunakan sebagai bukti otentik kepemilikan suatu data.Untuk pengamanan informasi rahasia maka salah satu caranya adalah informasi tersebut dienkripsi terlebih dahulu sebelum disisipkan ke dalam media digital dan kemudian diekstrak dan didekripsi kembali dari mediadigital tersebut.

2. TINJAUAN PUSTAKA

Pada naskah publikasi Tugas Akhir yang berjudul "Implementasi Algoritma Kriptografi DES dan Watermark dengan Metode LSB Pada Data Citra" menyatakan bahwa hasil watermark menggunakan metode LSB pada data citra memiliki performa yang cukup bagus dengan waktu relatif cepat dengan menggunakan 100 karakter. Untuk enkripsi dan dekripsi membutuhkan waktu 0.3 dt. Untuk penyisipan teks ke dalam gambar pada file GIF=0.8 dt, JPEG= 1.0 dt, dan PNG=0.7 dt. Sedangkan pengekstrakan pada file GIF=0.5 dt, JPEG=0.6 dt , dan file PNG=0,4 dt. Kualitas citra yang disisipi teks sebanyak 100 karakter atau sekitar 100 byte masih belum bisa dilihat secara visual dan walaupun tidak bisa dilihat secara visual, perbedaan citra bisa dilihat dengan histogram.[1]

Perbedaan penelitian ini dengan penelitian sebelumnya terdapat pada algoritma kritografi yang digunakan, format data citra, dan panjang karakter yang digunakan. Maka penulis mencoba melakukan penelitian menggunakan algoritma SHA-512 dan watermark dengan metode LSB pada data citra dengan format *.BMP dan *.JPEG, dimana panjang karakter yang disisipkan adalah 250 karakter.

2.1 Fungsi Hash

Fungsi hash adalah fungsi yang menerima masukan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (*fixed*). Jika string menyatakan pesan (*message*), maka sembarang pesan M berukuran sembarang dikompresi oleh fungsi *hash* H melalui persamaan h = H(M).
Keluaran fungsi *hash* disebut nilai *hash* atau pesan ringkas. Pada persamaan h = H(M), h adalah nilai *hash* atau *message digest* dari fungsi H untuk pesan M. Fungsi *hash* satu arah adalah fungsi *hash* yang bekerja dalam satu arah, pesan yang sudah diubah menjadi pesan ringkas tidak dapat dikembalikan lagi menjadi pesan semula. Contoh fungsi has yang satu arah adalah MD5 dan SHA. MD5 menghasilkan pesan ringkas berukuran 128 bit sedangkan SHA menghasilkan pesan ringkas yang berukuran 160 bit.[2]

2.2 Secure Hash Algorithm (SHA)

SHA adalah fungsi *hash* satu arah yang didesain oleh *National Security Agency* (NSA) dan dipublikasi oleh *National Institute of Standards and Technology* (NIST) sebagai *Federal Information Processing Standard* (FIPS) pada tahun 1993 dan disebut sebagai SHA-0, dua tahun kemudian dipublikasikan SHA-1 generasi selanjutnya yang merupakan perbaikan dari algoritma SHA-0. Pada tahun 2002 dipublikasikan empat variasi lainnya, yaitu SHA-224, SHA-256, SHA-384, dan SHA-512, keempatnya disebut sebagai SHA-2. SHA dinyatakan aman karena secara komputasi tidak dapat ditemukan isi pesan dari message digest yang dihasilkan, dan tidak dapat dihasilkan dua pesan yang berbeda menghasilkan message digest yang sama. Setiap perubahan yang terjadi pada pesan akan menghasilkan message digest yang berbeda. SHA-512 menggunakan 80 konstanta 64 bit yang sama, yang ditampung pada variable $K_0^{\{512\}}$, $K_1^{\{512\}}$,…$K_{79}^{\{512\}}$. Konstanta dihasilkan dari proses *fractional parts* dari *cube roots* pada 80 bilangan prima pertama.[3]

2.3 Watermark

*Watermarking*merupakan teknik penyisipan data ke dalam elemenmultimediaseperticitra, audio atauvideo[4]. *Watermarking*merupakan suatu proses yang berakar pada konsep ilmu*steganography*.Steganographysendiri sudah dikenal sejak jaman Mesir kuno. MenurutCachin dalam [5]*steganography*diartikan sebagai suatu seni dan ilmu untukmenyembunyikan pesan yang sebenarnya sehingga orang awam tidak dapat mendeteksinya

2.4 Least Significant Bit (LSB)

Menurut [6], metodeLSB (*Least Significant Bit*)merupakan salah satu metode*watermarking*yang bekerja dalam mode warnaRGB (*Red, Green, Blue*). Metode inibekerja dengan cara menyisipkan informasi pada bit-bit paling kanan dari setiapelemenRGB. Perubahan bit paling kanan hanya menimbulkan perubahan nilaiRGBsebesar 1 dari 256 warna yang ada. Perubahan tersebut tidak dapat dideteksi denganmata telanjang. Namun dengan komputer, misalnya menggunakan metode*Enhanced*LSB, dapat dideteksi dengan mudah apakah gambar mengandungwatermarkatautidak. MetodeLSBmudah untuk dideteksi karena penyisipan informasi dilakukansecara langsung dalam *bit-bit* dokumen tanpa melalui proses pengacakan.

3. ANALISA DAN PEMBAHASAN

3.1 Fungsi *Hash* SHA-512

Fungsi *hash* SHA-512 merupakan fungsi yang menghasilkan *message digest* ukuran 512 *bit* dan panjang blok 1024 *bit*. Terdapat 80 putaran dalam fungsi ini. Untuk melakukan *padding bit* dilakukan dengan cara yang sama dengan SHA-1, namun ukuran blok menjadi 1024 bit, bukan 512 bit. Daftar konstanta setiap putaran adalah sebagai berikut [3] (dari kiri ke kanan) :

```
428a2f98d728ae22     7137449123ef65cd     b5c0fbcfec4d3b2f     e9b5dba58189dbbc
3956c25bf348b538     59f111f1b605d019     923f82a4af194f9b     ab1c5ed5da6d8118
d807aa98a3030242     12835b0145706fbe     243185be4ee4b28c     550c7dc3d5ffb4e2
72be5d74f27b896f     80deb1fe3b1696b1     9bdc06a725c71235     c19bf174cf692694
e49b69c19ef14ad2     efbe4786384f25e3     0fc19dc68b8cd5b5     240ca1cc77ac9c65
2de92c6f592b0275     4a7484aa6ea6e483     5cb0a9dcbd41fbd4     76f988da831153b5
983e5152ee66dfab     a831c66d2db43210     b00327c898fb213f     bf597fc7beef0ee4
c6e00bf33da88fc2     d5a79147930aa725     06ca6351e003826f     142929670a0e6e70
27b70a8546d22ffc     2e1b21385c26c926     4d2c6dfc5ac42aed     53380d139d95b3df
650a73548baf63de     766a0abb3c77b2a8     81c2c92e47edaee6     92722c851482353b
a2bfe8a14cf10364     a81a664bbc423001     c24b8b70d0f89791     c76c51a30654be30
d192e819d6ef5218     d69906245565a910     f40e35855771202a     106aa07032bbd1b8
19a4c116b8d2d0c8     1e376c085141ab53     2748774cdf8eeb99     34b0bcb5e19b48a8
391c0cb3c5c95a63     4ed8aa4ae3418acb     5b9cca4f7763e373     682e6ff3d6b2b8a3
748f82ee5defb2fc     78a5636f43172f60     84c87814a1f0ab72     8cc702081a6439ec
90befffa23631e28     a4506cebde82bde9     bef9a3f7b2c67915     c67178f2e372532b
ca273eceea26619c     d186b8c721c0c207     eada7dd6cde0eb1e     f57d4f7fee6ed178
06f067aa72176fba     0a637dc5a2c898a6     113f9804bef90dae     1b710b35131c471b
28db77f523047d84     32caab7b40c72493     3c9ebe0a15c9bebc     431d67c49c100d4c
4cc5d4becb3e42b6    597f299cfc657e2a 5fcb6fab3ad6faec    6c44198c4a475817
```

Berikut adalah fungsi yang digunakan pada setiap putaran adalah:

1. Penjadwalan pesan

$$W_t = \begin{cases} M_t^{(i)} & 0 \le t \le 15 \\ \sigma_1^{\{512\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{512\}}(W_{t-15}) + W_{t-16} & 16 \le t \le 79 \end{cases}$$

2. Inisialisasi

$a = H_0^{(i-1)}\ b = H_1^{(i-1)}\ c = H_2^{(i-1)}\ d = H_3^{(i-1)}\ e = H_4^{(i-1)}\ f = H_5^{(i-1)}\ g = H_6^{(i-1)}\ h = H_7^{(i-1)}$

3. Fungsi untuk setiap putaran

$T_1 = h + \sum_1^{\{512\}}(e) + Ch(e,f,g) + K_t^{\{512\}} + W_t$

$T_2 = \sum_0^{\{512\}}(a) + Maj(a,b,c)$

$h = g$

$g = f$

$f = e$

$e = d + T_1$

$d = c$

$c = b$

$b = a$

$a = T_1 + T_2$

$Ch(x,yz) = (x^y) \oplus (\neg x^z)$

$Maj(x,yz) = (x\text{^}y) \oplus (x\text{^}z) \oplus (y\text{^}z)$

$\sum_0^{\{512\}}(x) = ROTR^{28}(x) \oplus ROTR^{34}(x) \oplus ROTR^{39}(x)$

$\sum_1^{\{512\}}(x) = ROTR^{14}(x) \oplus ROTR^{18}(x) \oplus ROTR^{41}(x)$

$\sigma_0^{\{512\}} = ROTR^{1}(x) \oplus ROTR^{18}(x) \oplus SHR^{7}(x)$

$\sigma_1^{\{512\}} = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^{6}(x)$

4. Hitung nilai hash

$H_0^{(i)} = a + H_0^{(i-1)}$
$H_1^{(i)} = b + H_1^{(i-1)}$
$H_2^{(i)} = c + H_2^{(i-1)}$
$H_3^{(i)} = d + H_3^{(i-1)}$
$H_4^{(i)} = e + H_4^{(i-1)}$
$H_5^{(i)} = f + H_5^{(i-1)}$
$H_6^{(i)} = g + H_6^{(i-1)}$
$H_7^{(i)} = h + H_7^{(i-1)}$

5. Nilai hash akhir
   $H_0^{(N)} \| H_1^{(N)} \| H_2^{(N)} \| H_{03}^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)}$

Keluaran akhir dari algoritma SHA adalah hasil penyambungan *bit-bit* di A, B, C, D, E, F, G dan H.

Misalnya hendak melakukan *hashing* terhadap pesan berikut ini :

universitas putra indonesia

Maka hasil hashing SHA-512 adalah :

359297FB866D63C2E6059F317ED28F992552131C4834597E25A4909B77A2E93B2AC9028F56CC12BF6CF
8260EEE4E40EDA24AC437FB0DD3FA49A5CC9B466C88A2

Hasil tersebut dikonversi menjadi bilangan biner, bilangan biner tersebut disisipkan di bit terakhir pada masing-masing warna baik R, G dan B.

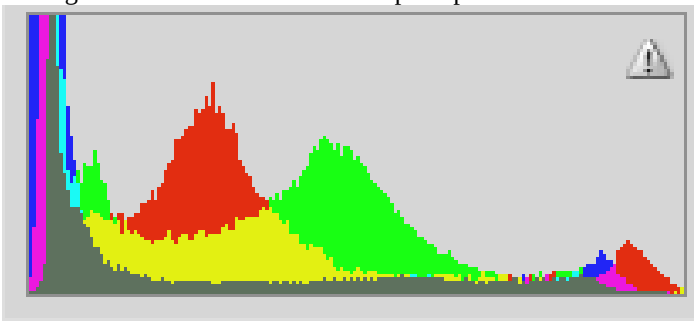
3.2 Metode Penyisipan *Least Signifcant Bit*

Hasil perhitungan fungsi hashing dikonversi menjadi bilangan biner, maka masing-masing hasil konversi tersebut disisipkan ke dalam data citra. Metode yang digunakan untuk penyisipan pesan adalah dengan metode *least significant bit* pada data citra yang menyusun file gambar BMP 24 bit. Gambar BMP 24 bit setiap pixel pada gambar terdiri dari susunan tiga warna yaitu merah, hijau, biru dikenal dengan warna RGB. Masing warna disusun oleh bilangan 8 bit dengan format biner 00000000 sampai 11111111.

Warna biru berada pada bit pertama sampai bit delapan, dan warna hijau berada pada bit sembilan sampai dengan bit 16, sedangkan warna merah berada pada bit 17 sampai dengan bit 24. Metode penyisipan LSB (*least significant bit*) merupakan penyisipan pesan dengan cara mengganti bit ke 8, 16 dan 24 pada representasi biner file gambar dengan representasi biner pesan rahasia yang akan disembunyikan. Dengan demikian pada setiap *pixel* file gambar BMP 24 bit dapat disisipkan 3 bit pesan. Pada bit ke-8, 16 dan 24 diganti dengan representasi biner huruf, dan hanya tiga bit rendah yang berubah, untuk penglihatan mata manusia, sulit untuk membedakan warna pada file gambar yang telah diisi pesan bila dibandingkan dengan data citra asli sebelum disisipi dengan pesan. Sebelum melakukan penggantian bit LSB, semua data citra yang bukan tipe 24-bit diubah menjadi format 24-bit. Jadi, setiap dua *pixel* sudah mengandung komponen RGB. Setiap byte di dalam data bitmap diganti satu bit LSB dengan bit data yang disembunyikan. Jika byte tersebut merupakan komponen hijau (G), maka penggantian 1 bit LSB hanya mengubah sedikit kadar warna hijau, dan perubahan ini tidak terdeteksi oleh mata manusia. Data citra 24 bit sudah tersusun atas komponen RGB, maka tidak perlu dilakukan perubahan format. Setiap *byte* di dalam data bitmap diganti satu bit LSB dengan bit data yang akan disisipkan.

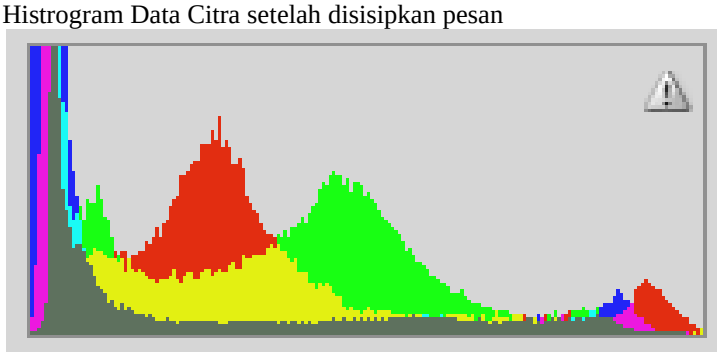
Berikut adalah hasil perbandingan performa data citra sebelum dan sesudah disisipkan pesan :

Tabel 1 Performa Data Citra sebelum disisipkan pesan

Data Citra	Histrogram Data Citra sebelum disisipkan pesan
 Ukuran Citra 800 x 600 Format Citra BMP	

Dari Tabel 1 dapat dilihat bahwa data citra dengan ukuran 800 x 600 pixel merupakan data citra yang belum disisipkan pesan teks, dan pada kolom kedua merupakan histogram yang berguna untuk melihat apakah data citra ada perbahan warna atau tidak.

Tabel 2 Performa Data Cita setelah disisipkan pesan

Data Citra	Histrogram Data Citra setelah disisipkan pesan
 Ukuran Citra 800 x 600 Format Citra BMP	

Berdasarkan Tabel 2 dapat dilihat bahwa data citra dengan ukuran 800 x 600 pixel merupakan data citra yang telah disisipkan pesan teks, dan pada kolom kedua adalah histogram yang berguna untuk melihat perbedaan warna citra setelah disisipkan pesan teks. Baik tabel 1 dan tabel 2 tidak tampak perbedaan yang signifikan akibat dari penyisipan pesan teks.

4. SIMPULAN DAN SARAN

4.1 Simpulan

Data citra yang telah disisipkan pesan teks memiliki performa yang baik. Kualitas citra yang disisipi pesan teks tidak bisa dilihat secara visual. Walaupun tidak bisa dilihat secara visual, perbedaan citra bisa dilihat dengan histogram. Oleh karena itu citra yang telah disisipkan pesan teks tidak mempengaruhi kualitas citra secara signifikan. Penggunaan kriptografi SHA-512 dalam penyisipkan pesan teks ke dalam data citra dapat dijadikan metode pengamanan pesan rahasia agar tidak dapat diketahui oleh orang-orang yang tidak bertanggungjawab.

4.2 Saran

Berikut ini saran yang dapat dijadikan bahan pertimbangan dalam pengembangan aplikasi watermarking agar dapat dikembangkan menjadi lebih baik lagi, yaitu: format gambar yang digunakan untuk menyimpan pesan rahasia hanya format *.bmp dan *.jpegsehingga saran penulis dapat dikembangkan format gambar yang lain.

5. DAFTAR RUJUKAN

[1] Fitri, Sulidar, 2010, Implementasi Algoritma Kriptografi DES dan Watermark dengan Metode LSB Pada Data Citra, AMIKOM Yogyakarta.
[2] Burrows, James, 2005, *Securer Hash Standard*, USA: US National Institute and Technology.
[3] FIPS 180-3, 2008, *Secure Hash Standard* (SHS), USA: Information Technology Laboratory, USA: National Institute of Standards and Technology.
[4] Cahyana; T. Basarudin dan Danang Jaya. 2007. Teknik Watermarking Citra berbasis SVD.National Conference on Computer Science & Information Technology 2007. Januari 29-30,2007.
[5] C. Cachin, *An Information-Theoretic Model for Steganography*, Proceedings of 2nd Workshop on Information Hiding, MIT Laboratory for Computer Science, May 1998
[6] Evan. 2009. Studi Digital Watermarking Citra Bitmap dalam Mode Warna Hue Saturation Lightness, Institut Teknologi Bandung, Bandung.