Pengembangan Fungsi Random pada Kriptografi Visual untuk Tanda Tangan Digital

Abdurrahman Dihya Ramadhan/13509060
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
a.dihya@students.itb.ac.id

***Abstraksi*— Dewasa ini kebutuhan untuk menjaga keamanan dokumen sangatlah besar. Untuk menjaga keamana kirim-mengirim dokumen, digunakan tanda tangan digital. Dengan konsep ini, keaslian sebuah dokumen dapat dibuktikan. Seiring berkembangnya zaman pun, bukan hanya dokumen teks yang dapat dijaga keasliannya, berbagai macam media seperti video, foto, dan suara pun dapat dijaga keasliannya dengan tanda tangan digital.**

Tanda tangan digital tersimpan secara visual dalam wujud file gambar. Untuk menjaga keamanan file gambar, terdapat sebuah mekanisme yang dinamakan kriptografi visual. Kriptografi visual melakukan pemecahan satu gambar menjadi dua gambar atau lebih yang terlihat acak atau random dan baru dapat diketahui gambar aslinya jika disatukan. Untuk memecah suatu gambar menjadi dua gambar yang terlihat random, diperlukan fungsi pembangkit bilangan random. Terdapat beberapa fungsi pembangkit bilangan random yang dapat digunakan dengan berbagai tingkat keteracakan dan keamanan.

Makalah ini bertujuan untuk menggabungkan ketiga konsep dalam kriptografi yaitu pembangkit bilangan acak, kriptografi visual, dan tanda tangan digital untuk meningkatkan keamanan dan autentikasi dokumen yang dikirimkan melalui jaringan internet.

***Kata kunci*—Tanda tangan digital, kriptografi visual, fungsi hash, kunci pribadi, kunci publik**

I. PENDAHULUAN

Semakin berkembangnya teknologi pada berbagai bidang, khususnya bidang IT, membuat segala hal lebih mudah dilakukan. Fasilitas yang diberikan teknologi yang setiap hari bermunculan menjadi semakin lengkap. Proses pengiriman berkas dari satu *storage* ke *storage* yang lain melalui berbagai macam cara dapat lebih mudah dilakukan. Namun kemudahan tersebut mengakibatkan permasalahan baru bermunculan. Salah satunya adalah autentikasi file yang tersebar di dunia maya. Pembuktian suatu file apakah benar dimiliki oleh orang tertentu memunculkan konsep tanda tangan digital. Dengan tanda tangan digital suatu file dapat diautentikasi kepemilikannya.

Autentikasi adalah proses yang melalui pembuktian dan verifikasi dari informasi tertentu. Terkadang seseorang ingin memverifikasi keaslian dokumen, identitas dari pengirim, waktu dan tanggal pengiriman dokumen dan/atau perubahan dokumen, identitas dari komputer maupun *user*, dan masih banyak lagi. Tanda tangan digital merupakan suatu cabang dari kriptografi artinya tanda tangan digital melewati banyak proses verifikasi. Tanda tangan digital dari suatu dokumen adalah potongan informasi yang didasari pada kunci pribadi baik milik dokumen maupun milik orang yang menandai dokumen tersebut. Tanda tangan digital tersebut biasanya dibuat menggunakan fungsi hash dan fungsi penanda pribadi.

Tanda tangan digital biasanya digunakan untuk mengimplementasikan tanda tangan elektrik, sebuah istilah yang lebih luas yang menunjukkan data elektronik apapun yang membawa sifat-sifat tanda tangan, akan tetapi tidak semua tanda tangan elektronik menggunakan tanda tangan digital. Di beberapa negara, termasuk Amerika Serikat, India, dan anggota-anggota Persatuan Eropa, tanda tangan elektronik tidak selalu terlihat jelas sebagai tanda tangan digital yang memiliki sifat kriptografi, akan tetapi bisa juga terlepas dari definisi legal dari tanda tangan digital itu sendiri.

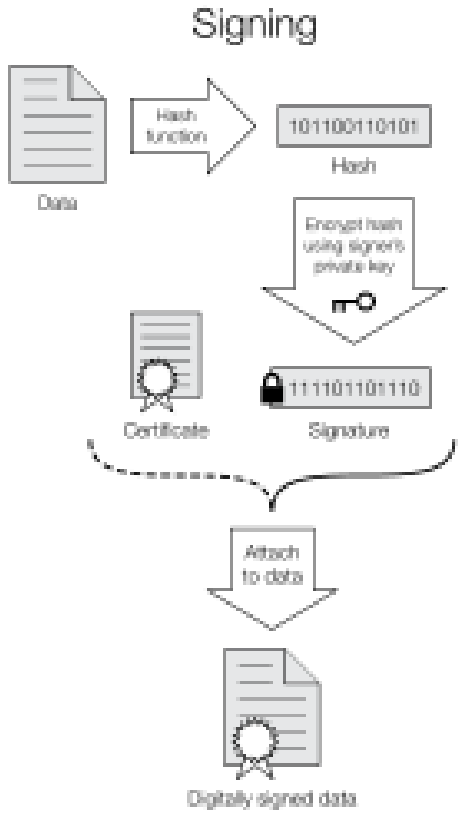
Tanda tangan digital menggunakan jenis kriptografi asimetris. Untuk pesan yang dikirimkan melewati kanal yang tidak aman, tanda tangan digital memberikan kepercayaan kepada penerima pesan bahwa pesan yang ia terima benar-benar berasal dari pengirim yang mengaku mengirimkan pesan. Tanda tangan digital setara dengan tanda tangan tradisional dengan tulisan tangan dalam banyak aspek; tanda tangan digital lebih sulit dipalsukan ketimbang tanda tangan asli.

Skema tanda tangan digital yang dibuat berdasarkan aturan-aturan kriptografi harus diimplementasikan secara benar supaya menjadi efektif. Tanda tangan digital juga dapat memberikan ketidaktertolakan yang artinya penanda tidak dapat sukses mengaku bahwa dia tidak menandai pesan, sambil mengaku juga bahwa kunci pribadi yang ia miliki tetap rahasia. Lebih jauh lagi, beberapa skema ketidaktertolakan menawarkan cap untuk tanda tangan

digital supaya meskipun kunci publik tersebar, tanda tangan tersebut tetap valid. Pesan yang ditandai secara digital bisa saja berupa segala hal yang mewakilinya, seperti bitstring, yang dicontohkan pada surat elektrik, kontak, atau pesan yang dikirimkan melalui protokol kriptografi.

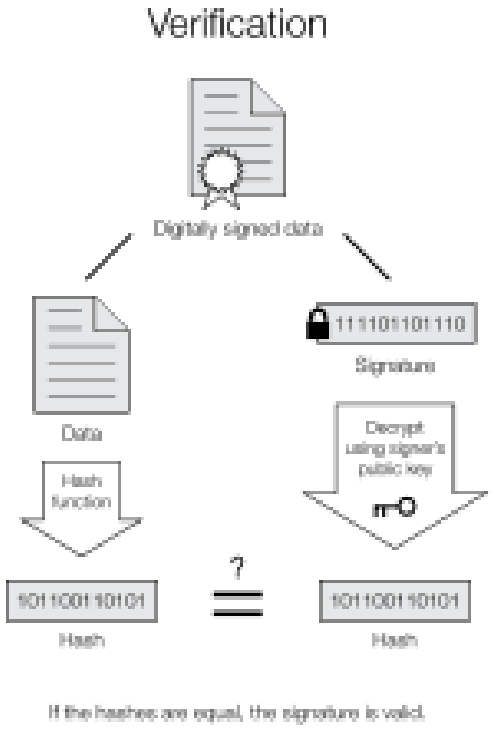
Tanda tangan digital terdiri dari tiga algoritma:

- Pembangkit kunci, yaitu algoritma yang menyeleksi kunci pribadi secara seragam dengan acak dari sekumpulan kunci pribadi yang mungkin. Output dari algoritma ini adalah kunci pribadi dan kunci publik yang sesuai.
- Algoritma penandaan yang memberikan pesan dan kunci prbadi dan memproduksi tanda tangan.
- Algoritmaverifikasi tanda tangan yang memberikan pesan, kunci publik dan tanda tangan, baik pada akhirnya menyetujui maupun tidak menyetujui pernyataan autentikasi pesan.



Gambar 01: Alur Proses Penandaan

Terdapat dua properti utama yang harus ada, yaitu yang pertama adalah tanda tangan yang dibangkitkan dari pesan tetap dan kunci pribadi tetap yang harus dapat memverifikasi keaslian dari pesan tersebut dengan menggunakan kunci publik yang sesuai. Syarat kedua adalah, tanda tangan digital harus benar-benar tidak dapat membangkitkan tanda tangan yang valid kepada pihak yang tidak memiliki kunci pribadi.



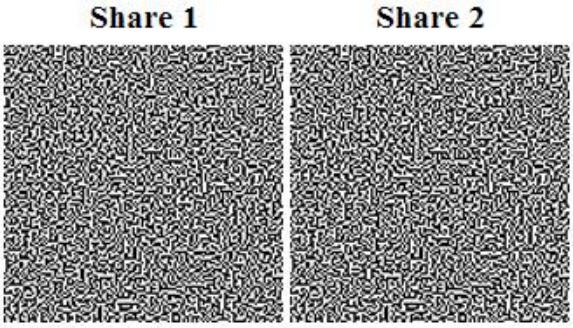
Gambar 02: Alur Proses Verifikasi

II. KRIPTOGRAFI VISUAL

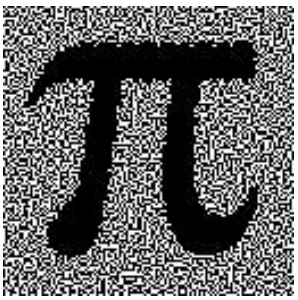
Kriptografi visual adalah sebuah teknik ekripsi yang dikhususkan untuk menyembunyikan informasi di dalam gambar dengan cara tertentu sehingga dapat didekripsikan dengan penglihatan manusia. Dengan pandangan saja, dapat dilihat apakah gambar sesuai atau tidak. Kriptografi visual menggunakan dua gambar transparan. Satu gambar mengandung piksel acak dan gambar lain mengandung informasi rahasia. Tidak mungkin mendapatkan informasi rahasia dari satu gambar. Akan tetapi, minimal terdapat dua buah gambar transparan atau dua buah layar untuk mendapatkan suatu informasi dari kriptografi visual.

Cara paling mudah untuk mengimplementasikan kriptografi visual adalah dengan cara mencetak kedua gambar menjadi dua lembar layar yang berbeda. Kemudian kedua gambar akan nampak seperti piksel acak. Ketika kedua gambar tersebut digeser menjadi bertumpuk satu sama lain tepat sejajar, maka dekripsi akan terjadi dan informasi berupa gambar akan terlihat. Gambaran dari kriptografi visual adalah sebagai berikut.

Gambar 03: Gambar Asli



Gambar 04: Dua gambar acak yang dibagikan secara terpisah

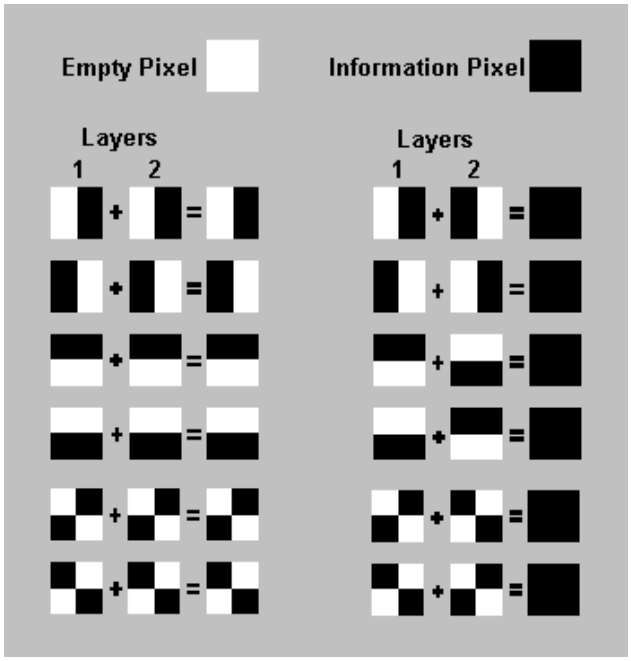


Gambar 05: Gambar 1 diletakkan sejajar dengan gambar 2

Dari gambar-gambar di atas terlihat bahwa ketika gambar 1 diletakkan di atas gambar 2 secara sejajar, akan terlihat gambar asli yang terbentuk dari susunan piksel 0 piksel random dari gambar 1 dan gambar 2. Metode ini sesuai untuk dipakai dalam menyembunyikan gambar namun juga tidak sulit untuk memecahkannya dan melihat gambar aslinya. Akan tetapi peletakkan dari kedua gambar harus benar-benar sejajar. Karena apabila bergeser satu piksel saja, maka gambar asli tidak akan jelas terlihat.

III. CARA KERJA KRIPTOGRAFI VISUAL

Untuk membuat kriptografi visual setiap piksel dari gambar dibagi menjadi blok yang lebih kecil. Blok putih diberi nomor, begitu pula blok hitam. Jika piksel dibagi menjadi dua bagian, ada satu blok hitam putih dan satu blok hitam. Jika piksel dibagi menjadi empat bagian yang sama, ada dua blok hitam putih dan dua. Contoh gambar di bawah ini menggunakan piksel yang terbagi dalam empat bagian.



Gambar 06: Cara membuat piksel informasi berupa blok hitam

Dalam tabel di sebelah kanan kita dapat melihat bahwa piksel, dibagi menjadi empat bagian, dapat memiliki enam status/kombinasi penyusun. Jika piksel yang berbeda pada layer 1 memiliki keadaan tertentu, piksel pada layer 2 dapat memiliki salah satu dari dua kondisi, yaitu identik atau terbalik dengan piksel dari layer 1. Jika piksel lapisan 2 adalah identik dengan layer 1, piksel yang tergabung akan setengah hitam dan setengah putih. Piksel yang tergabung tersebut disebut abu-abu atau kosong. Jika piksel dari lapisan 1 dan 2 adalah terbalik atau berlawanan, versi gambar gabungan akan hitam secara keseluruhan. Piksel ini disebut piksel informasi.

Setelah itu tinggal bagaimana caranya membuat dua lapisan. Dua lapisan ini terdiri dari satu gambar transparan, yaitu lapisan 1, yang memiliki piksel-piksel yang semuanya memiliki keadaan acak yang diambil dari salah satu dari enam kondisi yang mungkin. Layer 2 adalah identik dengan layer 1, kecuali untuk piksel yang harus hitam (berisi informasi) saat gambar digabungkan. Piksel ini memiliki keadaan yang berlawanan dengan piksel yang sama pada lapisan 1. Jika kedua gambar digabungkan, daerah dengan kondisi yang sama akan terlihat abu-abu, sedangkan daerah dengan kondisi piksel yang berlawanan akan menjadi hitam.

Sistem piksel dapat diterapkan dengan cara yang berbeda. Salah satunya adalah, setiap piksel dibagi menjadi empat blok. Akan tetapi bisa juga hanya dibagi menjadi dua blok persegi panjang, atau bahkan dibagi menjadi lingkaran. Selain itu, tidak masalah jika piksel dibagi secara horizontal atau vertikal. Ada banyak sistem piksel yang berbeda, di antaranya ada yang memiliki kontras yang lebih baik, resolusi yang lebih tinggi atau bahkan piksel warna yang bervariasi.

Jika status piksel lapisan 1 benar-benar acak, supaya menjaga keamanan kriptografi, piksel kosong sekaligus informasi dari layer 2 juga akan memiliki status yang benar-benar acak. Tidak ada yang dapat tahu apakah piksel pada lapisan 2 digunakan untuk membuat piksel abu-abu atau hitam, karena kita perlu keadaan piksel yang di layer 1 untuk mengetahui hasil pengabungan kedua gambar. Jika semua persyaratan untuk tingkat keacakan telah terpenuhi, maka visual kriptografi memberikan kerahasiaan mutlak sesuai dengan teori keamanan informasi.

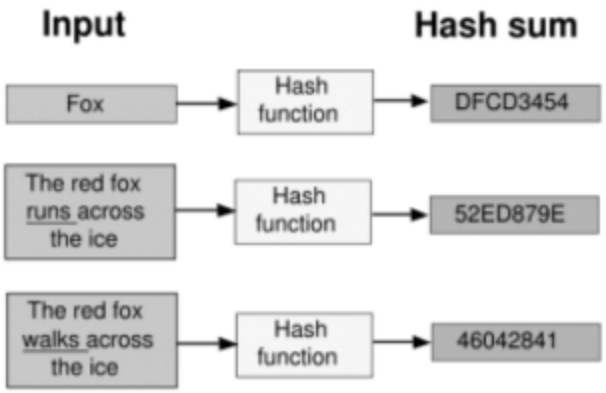
Jika visual kriptografi ingin digunakan untuk komunikasi yang aman, pengirim akan mendistribusikan satu atau lebih lapisan acak 1 di bagian yang terlihat untuk penerima. Jika pengirim memiliki pesan, ia dapat menciptakan lapisan 2 untuk lapisan 1 tertentu yang didistribusikan dan mengirimkannya ke penerima. Penerima menggabungkan secara sejajar dua lapisan dan kemudian informasi rahasia akan terungkap, hal ini tidak memerlukan perangkat enkripsi, perhitungan komputer, atau perhitungan dengan tangan. Sistem ini aman digunakan, asalkan kedua lapisan tidak jatuh di tangan yang salah. Ketika salah satu dari kedua lapisan dicegat tidak mungkin untuk mengambil informasi dari lapisan yang dienkripsi.

IV. FUNGSI HASH

Fungsi Hash merupakan perhitungan atau komputasi yang melibatkan sejumlah variable input m dan pengembalian sejumlah tetap string, yang disebut dengan nilai hash. Maka dapat kita tulis fungsi hash seperti rumus berikut.

$$h = H(m)$$

Input dan output fungsi hash adalah sebagai berikut.



Gambar 07: Input dan output fungsi hash

Karakteristik dasar dari fungsi hash dalam kriptografi adalah:

1. Input dapat sepanjang apa saja
2. Output memiliki panjang yang tetap
3. H(x) relative mudah dihitung untuk setiap x yang diberikan
4. H(x) bersifat satu arah
5. H(x) bersifat bebas kolisi

Fungsi hash H disebut satu arah jika sulit untuk diinversi. Sulit untuk diinversi artinya secara komputasi tidak mungkin mendapatkan beberapa input x sehingga H(x) = h.

Jika pesan x yang diberikan secara komputasi tidak mungkin menghasilkan pesan y tidak sama dengan x sehingga H(x) = H(y) kemudian H dinyatakan sebagai fungsi hash yang bebas kolisi secara lemah. Fungsi hash yang bebas kolisi secara kuat adalah yang secara komputasi tidak mungkin untuk menemukan dua pasan x dan y sehingga H(x) = H(y).

Nilai hash merepresentasikan pesan yang lebih panjang atau atau dokumen yang asal sebelum dia memasuki tahap komputasi. Intisasi dari pesan yang dihasilkan dapat dinyatakan sebagai tanda tangan digital dari dokumen yang lebih besar. Contoh yang terkenal dari fungsi hash adalah MD2, MD5 dan SHA.

Fungsi utama dari fungsi hash adalah membuktikan validitas dari tanda tangan digital. Fungsi hash secara umum lebih cepat dibanding algortima tanda tangan digital. Dengan begitu fungsi hash dapat mengkomputasikan tanda tangan digital menjadi beberapa dokumen dengan cara mengkomputasikan tanda tangan pada nilai hash dari dokumen yang dapat dibandingkan dengan dokumen itu sendiri. Selain itu, sebuah ringkasan dari dokumen dapat dibuat publik tanpa membocorkan konten dari dokumen aslinya. Hal ini sangat penting dalam pemberian stempel waktu pada dokumen di mana dengan fungsi hash seseorang dapat menerima dokumen yang

telah diberi stempel waktu tanpa membongkar konten dokumen tersebut kepada jasa pelayanan pemberian stempet waktu.

Ketiga konsep di atas, yaitu tanda tangan digital, kriptografi visual, dan fungsi hash adalah penyusun ide dari makalah ini. Dalam makalah ini dicoba digunakan ketiga konsep tersebut untuk lebih menguatkan keamanan dari tanda tangan digital.

V. TANDA TANGAN DIGITAL DARI GAMBAR

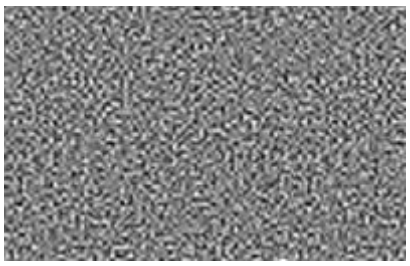
Tanda tangan digital yang diimplementasikan pada makalah ini adalah tanda tangan digital gambar. Dalam konsep asal tanda tangan digital pesan yang disimpan berupa string. Sedangkan pada makalah ini dicoba pesan berupa tanda tangan gambar yang biasa orang tulis ketika membuat tanda tangan dengan tulisan tangan. Dengan begitu diharapkan proses pembubuhan tanda tangan menjadi lebih natural dan mirip dengan proses tanda tangan sebenarnya pada dunia nyata.

VI. IMPLEMENTASI TANDA TANGAN DIGITAL

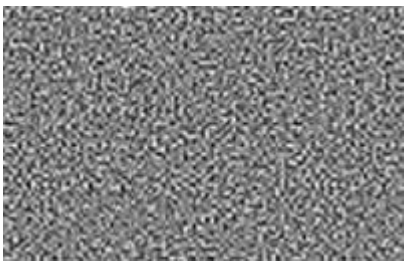
Tanda tangan digital yang diimplementasikan pada makalah ini seperti pada gambar berikut.

Gambar 08: Contoh tanda tangan asli yang ingin dienkripsi

Tanda tangan tersebut akan diacak pikselnya dengan fungsi hash untuk membuat gambar abstrak seperti kriptografi visual. Untuk mengacak piksel gambar tersebut dilakukan iterasi dari titik paling kiri atas gambar hingga titik paling kanan bawah kemudian mencari piksel mana yang bisa dijadikan hitam, dan piksel mana yang bisa dijadikan blok putih sesuai dengan konsep kriptografi visual di atas. Dalam makalah ini digunakan 4 piksel untuk satu informasi. Itulah cara untuk melakukan enkripsi tanda tangan pada makalah ini. Contoh keluaran dari enkripsi tanda tangan adalah dua gambar di bawah ini.



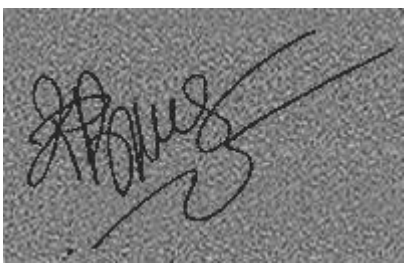
Gambar 09: Contoh gambar acak pertama hasil enkripsi tanda tangan



Gambar 10: Contoh gambar acak kedua hasil enkripsi tanda tangan

Kedua gambar di atas merupakan piksel – piksel yang telah diacak sehingga tidak dapat menampilkan informasi apa-apa kepada yang melihatnya. Jika ingin melihat informasi yang disimpan di dalam kedua gambar, maka kedua gambar harus digabungkan terlebih dahulu.

Penggabungan kedua gambar dalam program yang dibuat tidak dapat dilakukan langsung akan tetapi harus memecahkan fungsi hash yang digunakan untuk mengacak gambar hasil kriptografi visual. Fungsi hash yang digunakan adalah SHA. Sehingga yang harus dimiliki adalah kunci pribadi dan kunci publik untuk mengembalikan urutan gambar menjadi gambar acak sebenarnya. Setelah dilakukan pengembalian susunan gambar acak, maka kedua gambar harus digabungkan untuk melihat informasi yang tersimpan pada kedua gambar tersebut. Hasil penggabungan kedua gambar di atas adalah sebagai berikut.



Gambar 11: Contoh visualisasi tanda tangan hasil dekripsi

Dari gambar di atas dapat dilihat informasi sebenarnya yang terkandung dalam suatu gambar. Meskipun gambar sudah terpengaruh pengacakan piksel, akan tetapi infromasi yang terkandung di dalamnya masih dapat dilihat dengan jelas. Tanda tangan hasil enkripsi tadi disimpan dalam satu file dengan penyisipan pada bit paling tidak signifikan yang terletak pada bagian awal file untuk gambar pertama, dan bagian akhir file untuk gambar kedua. Proses ekstraksi informasi hanya akan menghasilkan bit - bit yang tidak ada gunanya kecuali pembaca sudah memiliki kunci enkripsi.

Setelah itu file-file berupa dokumen, video, gambar, dapat dibubuhi tanda tangan natural, seperti tanda tangan dengan tulisan tangan orang biasa namun dimasukkan sehingga tidak terlihat di dalam file. Penyisipan tanda tangan dalam file-file tersebut juga tidak akan merusak kualitas file. File gambar tidak akan mengalami perubahan yang dapat dilihat, file video maupun suara tidak akan berkurang kualitasnya, dan seterusnya.

VII. KESIMPULAN DAN SARAN

Tujuan dari kriptografi visual pada makalah kali ini adalah mengamankan pesan gambar yang terdapat pada suatu file supaya tidak sampai ke pihak yang tidak berhak. Tujuan lainnya adalah supaya tiap file dapat diverifikasi siapa pembuat file tersebut. Dengan begitu diharapkan upaya plagiarisme atau pengakuan seseorang terhadap dokumen yang bukan miliknya dapat dilacak dan dikurangi prakteknya.

REFERENCES

[1] Munir, Rinaldi. 2009. "Diktat Kuliah IF3058, Kriptografi." Bandung: Program Studi Teknik Informatika ITB.

[2] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology -EUROCRYPT'94, A. D. Santis., Ed., vol. 950. Springer-Verlag, 1995, pp. 1–12.

[3] Hassler, V;& Helmut, B.1999. Digital Signature Management, In ternet Research, Emerald journal 9 (4).

[4] Schneir, Bruce. (1996). Applied Crypthography. John Wiley.

[5] http://www.absoluteastronomy.com/topics/Digital_signature. Dikunjungi tanggal 20 Mei 2013, pukul 3:11.

[6] http://users.telenet.be/d.rijmenants/en/visualcrypto.htm. Diakses tanggal 20 Mei 2013 7:12.

[7] http://x5.net/faqs/crypto/q94.html. Diakses pada 20 Mei 2013 9:15.

[8] http://hari-cio-8a.blog.ugm.ac.id/2013/03/22/fungsi-hash-teknik-kriptografi/. Diakses pada 20 Mei 2013 14:20.

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, 20 Mei 2013

Abdurrahman Dihya Ramadhan
13509060