BAB II
LANDASAN TEORI

2.1 Watermarking

Salah satu cara untuk melindungi hak cipta multimedia adalah dengan menyisipkan informasi ke dalam data multimedia tersebut dengan teknik *watermarking*, Informasi yang disisipkan dalam data disebut *Watermark*, dan *Watermark* dapat dianggap sebagai sidik digital (digital signature) dari pemilik yang sah atas produk multimedia tersebut. Dengan kata lain, *watermark* yang disisipkan menjadi label hak cipta dari pemiliknya. Pemberian *signature* dengan teknik *watermarking ini dilakukan sedemikian rupa sehingga informasi yang disisipkan tidak merusak data digital yang dilindungi.Sehingga, seseorang* yang membuka produk multimedia yang sudah disisipi *watermark* tidak menyadari kalau yang didalam 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 mengektraksi *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 permanent kedalam data digital.Kode Identifikasi tersebut dapat berupa teks, gambar, suara, atau video.Selain tidak merusak data digital produk yang

akan dilindungi, kode disisipkan seharusnya memiliki ketahanan (*robustness*) dari berbagai pemrosesan lanjutan seperti pengubahan,transfomasi geometri, kompresi, enkripsi, dan sebagainya.Sifat *robustness* berarti data *watermark* tidak terhapus akibat pemrosesan lanjutan tersebut.

2.2 Sejarah *Watermarking*

Watermarking sudah ada sejak 700 tahun yang lalu.Pada abad 13, pabrik kertas di fabriano, Italia, membuat kertas yang diberi watermark atau tanda air dengan cara menekan bentuk cetakan gambar atau tulisan pada kertas yang baru setangah jadi. Ketika kertas dikeringkan terbentuklah suatu kertas yang ber-*watermark.* Kertas ini biasanya digunkan oleh seniman atau sastrawan untuk menulis karya mereka. Kertas yang sudah dibubuhi tanda-air tersebutsekaligus dijadikan identifikasi bahwa karya seni yang diatasnya adalah milik mereka. Kertas yang sudah dibubuhi tanda-air tersebut sekaligus dijadikan identifikasi bahwa karya seni diatasnya adlah milik mereka [HEN03].

Ide *watermarking* pada data digital (sehingga disebut data digital watermarking) dikembangkan dijepang tahun1990 dan swiss tahun1993. Digital *watermarking* semakin berkembang seiring dengan semakin meluasnya pengguna internet, objek digital seperti video, citra, dan suara yang dapat dengan mudah digandakan dan disebarluaskan.

2.3 Sejarah Steganografi

Steganografi berasal dari bahasa Yunani yaitu Steganós yang berarti menyembunyikan dan Graptos yang artinya tulisan sehingga secara keseluruhan artinya adalah tulisan yang disebunyikan. Secara umum steganografi merupakan seni atau ilmu yang digunakan untuk menyembunyikan pesan rahasia dengan segala cara sehingga

selain orang yang dituju, orang lain tidak akan menyadari keberadaan dari pesan rahasia tersebut.

Steganografi sudah digunakan sejak dahulu kala sekitar 2500 tahun yang lalu untuk kepentingan politik, militer, diplomatik, serta untuk kpntingan pribadi sebagai alat. Beberapa contoh penggunaan steganografi pada masa lampau:

1) Pada tahun 480 sebelum masehi, seseorang berkebangsaan Yunani yaitu Demaratus mengirimkan pesan kepada polis Sparta yang berisi peringatan mengenai penyerangan Xerxes yang ditunda. Teknik yang digunakan adalah dengan menggunakan meja yang telah diukir kemudian diberi lapisan lilin untuk menutupi pesan tersebut, dengan begitu pesan dalam meja dapat disampaikan tanpa menimbulakn kecurigaan oleh para penjaga.
2) Pada abad ke 5 sebelum masehi, Histaiacus mengirimkan pesan kepada Aristagoras Miletus untuk memberontak terhadap raja Persia. Pesan disampaikan dengan cara mencukur kepala pembawa pesan dan mentato kepalanya dengan pesan tersebut. Kemudian saat rambutnya tumbuh kembali, pembawa pesan dikirimkan dan pada tempat tujuan rambutnya kembali digunduli dan pesan akan terbaca.
3) Penggunaan tinta yang tidak terlihat pada pesan lainnya.

2.4 Perbedaan *Watermarking* dan Steganografi

Watermarking merupakan aplikasi dari Steganografi, namun ada perbedaan antara keduanya. Jika pada Steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apa , maka pada *watermarking* justru

media digital tersebut yang akan dilindungi kepemilikannya dengan memberi label hak cipta (*watermark*).

Meskipun steganografi dan *watermarking* tidak sama, namun secara prinsip proses penyisipan informasi ke dalam data digital tidk jauh berbeda. Beberapa metode yang sudah ditemukanuntuk penyisipan *watermark* adalah metode *LSB,* metode *adaptif*, metode *spread,* metode *spectrum* dan lain sebagainya.

Data *watermark* yang lazim disisipkan ke dalam data digital adalah teks, citra, atau suara.Watermark berupa teks mengandung kelemahan karena kesalahan dalam satu bit akan menghasilkan hasil teks yang berbeda pada waktu verifikasi (Ektraksi).Watermark dalam bentuk suara atau citra lebih disukai karena kesalahan pada beberapa bit watermark tidak menghasilkan perubahan berarti pada waktu verifikasi.Hasil ektraksi *watermark* yang mengandung kesalahan tersebut masih dapat dipersepsi secara visual (atau secara pendengaran jika watermark-nya berupa suara).citra yang sering digunakan sebagai watermark biasanya logo atau lambing.

2.5 Steganografi

Steganografi adalah teknik yang digunakan untuk menyembunyikan informasi dengan cara menyamarkan informasi, sehingga orang-orang tidak menyadari adanya pesan rahasia yang tersimpan. Steganografi merupakan salah satu teknik dari information hiding,teknik lainnya adalah digital watermarking. Teknik steganografi dengan metode LSB (Least Significant Bit).

LSB(Least Significant Bit) adalah teknik yang paling sering digunakan. Informasi yang akan disembunyikan akan diambil nilai binernya kemudian disisipkan pada LSB sederetan byte. Kelemahan dari metode LSB adalah besar pesan sangat tergantung dari

mediayangdipergunakan.Semisalkan ada sebuah media berupa gambar yang akan disisipkan informasi rahasia. Media gambar yang mempunyai kedalaman 24 bit setiap pixel-nya terdiri atas susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 byte dari 0 sampai 255 dalam format biner dari 00000000 sampai 1111111.Dengan menggunakan metode LSB, sebuah huruf dapat disisipkan dengan menggunakan tiga pixel gambar.

Contoh, akan disisipkan huruf A kedalam data

(10010101 11000101 00101010) –> piksel pertama(R,G,B)

(00011100 10000110 01100110) –>pikselkedua(R,G,B)

(10000111 10010100 00100010) –> piksel ketiga (R, G ,B)

Huruf A mempunyai representasi biner 01000001, sehingga bila disisipkan, data diatas akan berubah menjadi data

(1001010**0** 1100010**1** 0010101**0**) –> piksel pertama (R, G ,B)

(0001110**0** 1000011**0** 0110011**0**) –> piksel kedua (R, G ,B)

(1000011**0** 1001010**0** 0010001**1**) –> piksel ketiga (R, G ,B)

Perubahan data tersebut tentu saja akan merubah warna pixel, tetapi karena perubahannya sangat sedikit, tidak akan disadari oleh mata manusia, sehingga seakan2 gambar yang disisipkan pesan tadi sama sekali tidak berubah.

2.5.1 Bit Depth

Bit Depth Menentukan jumlah bit yang digunakan untuk mempersentasikan tiap piksel pada sebuah Image.kedalaman bit dinyatakan dalam bit/pixel. Semakin banyak jumlah bit yang digunakan untuk mempersentasikan sebuah piksel, yang berarti semakin tinggi kedalaman pikselnya, maka semakin baik pula

kualitasnya, dengan konsekuensi jumlah *bit* yang diperlukan menjadi lebih tinggi. Dengan 1 *Byte* (8 bit)untuk tiap piksel, diperoleh 2^8 atau 256 level intensitas. Dengan level intensitas sebanyak itu,umumnya mata manusia sudah dapat dipuaskan. Kedalaman piksel paling rendah terdapat pada *binary value image* yang hanya menggunakan 1 *bit/piksel*, sehingga hanya dua kemungkinan bagi tiap piksel, yaitu o untuk hitam dan 1 untuk putih. Pada kenyataanya semakin sedikit jumlah *bit* yang digunakan untuk tiap piksel, maka kualitas gambar akan semakin menurun.

2.6 Digital Watermarking

Steganografi pada saat ini banyak diterapkan dengan menggunakan *file-file* digital. Pada steganografi tulisan beberapa cara yang biasa digunakan untuk menyembunyikan pesan adalah menggunakan ruang kosong, baik ruang kosong antara baris maupun ruang kosong antara kata. Dengan menggunakan bebearapa *software* khusus pesan rahasia dapat disispkan pada ruang-ruang kosong tersebut.

Steganografi juga mulai menggunakan *file-file* multimedia sebagai kedok untuk menyembunyikan pesan rahasia, baik itu berupa gambar, suara, atau video yang biasa disebut *digital watermarking*. Sebelum lebih lanjut dengan pembahasan steganografi, perlu diketahui beberapa istilah yang sering igunakan. Berikut adalah beberapa istilah yang sering digunakan dalam teknik steganografi:

1) Carrier file : *file* yang berisi pesan rahasia tersebut
2) Steganalysis : proses untuk mendeteksi keberadaanpesan rahasia dalam suatu *file*
3) Stego-medium : media yang digunakan untuk membawa pesan rahasia

4) Redundant bits : sebagian informasi yang terdapat di dalam *file* yang jika dihilangkan tidak akan menimbulakn kerusakan yang signifiakan (setidaknya bagi indera manusia)
5) Payload : informasi yang akan disembunyikan

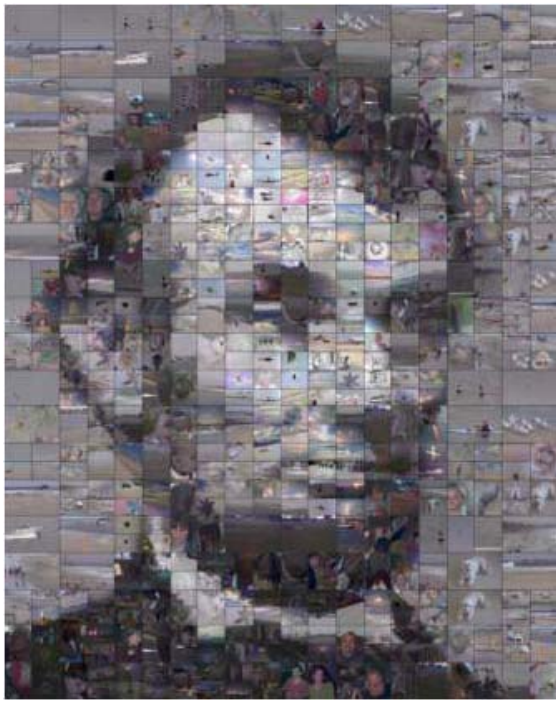
Teknik yang digunakan pada *digital watermarking* beragam tetapi secara umum teknik ini menggunakan *redundant bits* sebagai tempat menyembunyikan pesan pada saat dilakukan kompresi data, dan kemudian menggunakan kelemahan indera manusia yang tidak sensitive sehingga pesan tersebut tidak ada perbedaan yang terlihat atau yang terdengar. Cara yang paling sering digunakan adalah dengan mengganti LSB (Least Significant Byte) dengan pesan rahasia, dengan asumsi tidak semua data dibutuhkan. Kelemahan dari teknik adalah dengan mengganti LSB, maka besar pesan yang dapat disembunyikan menjadi tergantung dengan besar dari *carrier file*. Selain itu terdapat teknik lain yang dapat digunakan yaitu *Injection*. Teknik ini dengan langsung menyelipkan pesan rahasia pada *carrier file*. Namun dengan cara ini maka ukuran *carrier file* akan bertambah besar sesuai dengan besar pesan tersebut.

Cara yang harus dilakukan saat menggunakan *digital watermarking* adalah menghapus *file* asli dari *carrier file*. Karena jika tidak bila dilakukan perbandingan dengan berbagai cara, perbedaan antara keduanya dapat diketahui sehingga pesan dapat diketahui oleh orang lain. Walaupun sekarang tanpa *file* asli beberapa jenis steganografi dapat diketahui, cara ini merupakan cara yang harus dilakukan untuk setidaknya mengurangi kemungkinan untuk dilakukannya perbandingan.

Steganografi pada gambar biasanya menggunakan teknik penggantian LSB. Bagi computer gambar adalah *file* yang berisi kumpulan warna dan itntensitas cahaya pada daerah yang berbeda. Dengan menggunakan pnggantian LSB, maka untuk mendapatkan

hasil terbaik sebaiknya digunakan 24 bit Bitmap, dikarenakan ukurannya yang besar dan memiliki resolusi tinggi. Dengan ukuran yang besar maka pesan yang dapat dibawa semakin besar dan dengan resolusi tinggi tidak akan terlihat perubahan yang signifikan. Namun pada kenyataannya bnyak yang menggunakan 8bit Bitmap atau dengan menggunakan format lainnya seperti GIFF, JPEG, atau PNG untuk menghindari kecurigaan. Kelemahan dalam steganografi menggunakan gambar adalah bila dikonversiakan menjadi format yang lain, maka secara otomatis pesan yang disembunyikan akan hilang.

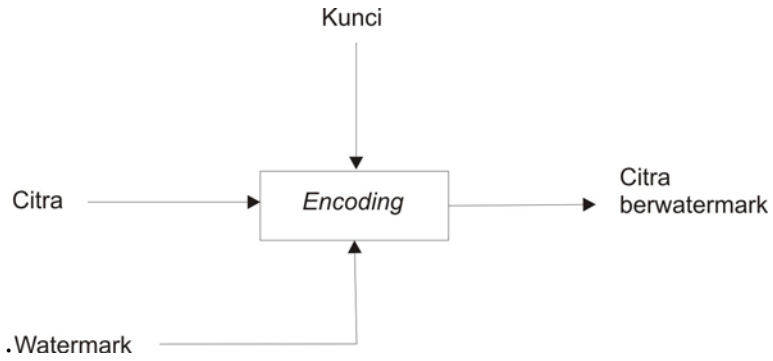
Walaupun bukan termasuk dalam steganografi, teknik penyusunan gambar dapat digunakan untuk menyembunyikan informasi dalam bentuk foto. Berikut adalah gambar contoh dari presiden Amerika Serikat Abraham Lincoln yang sebenarnya terdiri dari gabungan beberapa gambar:



Gambar 2.1 teknik penyusunan gambar yang membentuk gambar lain

2.7 Penyisipan Watermark

Disini kita hanya meninjau *watermarking* pada citra digital.Proses penyisipan pada *watermark* ke dalam citra di sebuti *encoding* dan ditunjikan gambar 2.1.3.*Encoding* dapat disertai dengan pemasukan kunci atau tidak memerlukan kunci. Kunci diperlukan agar *watermark* hanya dapat diekstraksi oleh pihak yang sah.Kunci juga dimaksudkan untuk mencegah *watermark* dihapus oleh pihak yang tidak berhak



Gambar 2.2 Proses penyisipan watermark pada citra digital

2.7. 1 Proses watermarking

Pada gambar proses watermarking di atas terdapat komponen kunci. Kunci ini berguna untuk mencegah penghapusan watermarking oleh pihak yang tidak berhak dengan menggunakan metode enkripsi tertentu. Ketahanan watermarking terhadap proses-proses lanjutan tergantung pada metode watermarking yang digunakan. Masing-masing metode mempunyai kelebihan dan kekurangan. Masing-masing metode biasanya mempunyai fokus yang berbeda pada hal-hal yang dianggap penting.

Terdapat tiga bagian yang menyusun sistem watermarking yaitu :

a) Label watermark.
b) Proses penyisipan watermark.
c) Proses mendapatkan kembali watermark dari data terwatermark

(ekstraksi).

Label watermark adalah data yang akan kita masukkan ke dalam data dgital yang ingin diwatermark. Ada dua jenis label yang bisa digunakan :

1) Text biasa

Label text biasanya berupa representasi ASCII dariteks tersebut kemudian dikonversi ke bentuk bit. Kelemahannya adalah apabila terjadi kesalahan satu bit saja, akan merubah watermark tersebut menjadi berbeda dengan text semula.

2) Non-text

Label non-text meliputi gambar atau suara. Berbeda dengan label text, kesalahan beberapa bit masih memberikan interpretasi yang sama dengan label asalnya menurut indera manusia. Kelemahannya adalah ukuran watermark menjadi lebih besar. Proses watermarking diakhiri dengan verifikasi. Proses verifikasi meliputi ekstraksi watermark dan pembandingan watermark asli dengan termark hasil ekstraksi. Proses ekstraksi bisa memerlukan data asli (non-blind watermarking) maupun tidak (blind watermarking).

2.7.2 **Watermarking pada Citra dengan Format Kompresi JPEG**

JPEG (Joint Photographic Expert Group) adalah salah satu format kompresi citra digital yang saat ini banyak dipakai. Format kompresi ini berbasis Discrete Cosine Transform, sama dengan format kompresi MPEG (Motion Picture Expert Group) pada video digital. Selama proses penyandian (encoding) dengan DCT, sebuah gambar dipecah-pecah menjadi blok-blok yang kecil-kecil yang tiap bloknya memuat 8 x 8 pixel (titik titik elemen gambar), yang bertidak sebagai masukan bagi suatu DCT. Operasi matematik yang rumit dikenakan pada setiap blok tersebut untuk memperoleh nilai-nilai

yang menyatakan karakter penting dari setiap bloknya seperti bagian sisi-sisi atau konturnya yang nantinya harus dapat direpresentasikan. Proses ini disebut discrete cosine transform. DCT kemudian mengkuantisasi dengan menggunakan fungsi-fungsi weighting (pembobotan) yang dioptimalkan sehingga mendekati sistem visual manusia. Kuantisasi dimaksudkan untuk menyederhanakan bobot angka-angka, yakni senilai 256 yang menunjukkan keseluruhan palet warna dari putih murni sampai hitam murni. Kuantisasi yang dilakukan ini membulatkan bobot angka dari kemungkinan 256 perbedaan tersebut menjadi kemungkinan warna katakanlah 16 saja dengan cara membulatkan ke dalam aproksimasi yang terdekat. Pada akhirnya angka-angka yang telah dikuantisasi tersebut di-entropy coded yang maksudnya nilai-nilai atau bobot angka yang paling banyak prevalensinya diberi nilai atau ditandai dengan angka-angka dengan bobot yang paling kecil. Untuk mendekompresi citra, prosesnya ditangani dengan cara kebalikannya.Banyak cara untuk menyembunyikan informasi di dalam gambar. Untuk menyembunyikan informasi, penyisipan pesan yang langsung dapat meng-enkode setiap bit dari informasi dalam gambar atau menempelkan pesan secara selektif dalam area noisy, menggambarkan area yang kurang diperhatikan, dimana ada banyak variasi warna natural. Pesan dapat juga terserak secara acak sepanjang gambar. Pola redundansi encoding “wallpapers” menutup gambar dengan pesan. Sejumlah cara yang ada untuk menyembunyikan informasi dalam gambar digital dengan pendekatan yang umum termasuk :

- penyisipan least significant bit
- masking dan filtering, dan
- algoritma dan transformasi.

Setiap teknik-teknik itu dapat diaplikasikan dengan derajat kesuksesan yang bervariasi pada file gambar yang berbeda.

1) Penyisipan Least Significant Bit (LSB)

Penyisipan *Least Significant Bit* (LSB) adalah umum, pendekatan yang sederhana untuk menempelkan informasi di dalam suatu file cover. Sayangnya, hal itu sangat peka untuk kejadian yang melalaikan manipulasi gambar. Meng-konvert suatu gambar dari format GIF atau BMP, yang merekonstruksi pesan yang sama dengan aslinya (*lossless compression*) ke JPEG yang *lossy compression*, dan ketika dilakukan kembali akan menghancurkan informasi yang tersembunyi dalam LSB.

Modifikasi LSB dilakukan dengan memodifikasi bit terakhir dalam satu byte data. Bit yang diganti adalah LSB karena perubahan pada LSB hanya menyebabkan perubahan nilai byte satu lebih tinggi atau satu lebih rendah. Misalkan data yang diubah adalah warna hijau, maka perubahan pada LSB hanya menyababkan sedikit perubahan yang tidak dapat dideteksi oleh mata manusia. Tenik penyisipan LSB adalah teknik paling sederhana, namun memiliki robustness yang rendah. Penyisipan LSB tidak tahan terhadap proses yang merubah data citra terutama kompresi JPEG.

2) Masking dan Filtering

Teknik masking dan filtering, hanya terbatas ke gambar 24-bit dan gray-scale, informasi disembunyikan dengan menandai suatu gambar dengan cara seperti paper watermark. Teknik watermarking dapat di aplikasikan dengan resiko rusaknya gambar dalam kaitannya dengan lossy compression, sebab mereka lebih menyatu ke dalam gambar. Penyembunyian watermark dilakukan dengan merubah luminance dengan prosentase lebih kecil sehingga watermark dalam mask tidak terdeteksi oleh mata manusia. Masking lebih robust dari pada penyisipan LSB dengan hasil

kompresi, cropping, dan beberapa pemrosesan gambar. Teknik masking menempelkan informasi dalam area significant sehingga pesan yang tersembunyi itu lebih bersatu dengan gambar cover dari pada penyembunyian dalam level “noise”.

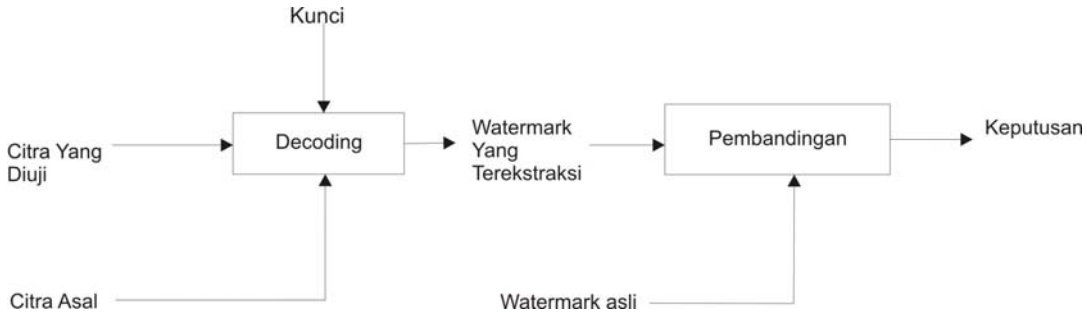
3) Algoritma dan Transformasi

Manipulasi LSB adalah suatu cara yang cepat dan mudah untuk menyembunyikan informasi tetapi sangat peka untuk perubahan hasil yang kecil dari pemerosesan gambar atau lossy compression. Seperti kompresi yang merupakan kunci keuntungan dari gambar JPEG yang mempunyai kelebihan dari format yang lain. Gambar dengan kualitas warna yang tinggi dapat disimpan dalam file yang relative kecil menggunakan metoda kompresi JPEG; sehingga gambar JPEG menjadi lebih berlimpah pada Internet. Ada berbagai algoritma berbasis transformasi yang bisa digunakan dalam teknik watermarking. Contohnya adalah metoda Cox dan Randomly Sequenced Pulse Potition Modulated Code (RSPPMC) yang diusulkan oleh Zhao & Koch. Kedua algoritma tersebut bekerja dengan basis Discrete Cosine Transform seperti yang digunakan pada sistem kompresi JPEG.Sehingga watermark yang dihasilkan lebih tahan terhadap kompresi JPEG.

2.8 Verifikasi Watermarking

Verifikasi *watermark* dilakukan untuk membuktikan status kepemilikan citra digital yang disengketakan. Verifikasi *watermark* terdiri atas dua sub-proses,yaitu ekstraksi *watermark* dan pembandingan. Sub-proses ekstraksi *watermark* disebut juga *Decoding,* bertujuan mengungkap *watermark* dari dalam citra. *Decoding* data mengikutsertakan citra asal (Yang belum di *watermark*)atau tidak sama sekali, karena beberapa skema *watermarking* memang menggunakan citra asal dalam proses *decoding* untuk meningkatkan unjuk kerja yang baik[HEN03]. Sub–proses pembandingan

bertujuan membandingkan *watermark* yang diungkap dengan *watermark* asli dan memberi keputusan tentang *watermark* tersebut. Proses verifikasi ditunjukan pada gambar berikut.



Gambar 2.3 Proses verifikasi watermark pada citra digital

2.9 Pengertian Enkripsi

Salah satu hal yang penting dalam komunikasi menggunakan komputer untuk menjamin kerahasian data adalah enkripsi. Enkripsi yang berasal dari bahasa Yunani, *kryptos* yang artinya 'rahasia' atau 'tersembunyi', adalah sebuah proses yang mengubah suatu data menjadi kode yang tidak bisa dimengerti (tidak terbaca).

Ilmu yang mempelajari seluk-beluk enkripsi dan dekripsi (lawan enkripsi) disebut *Cryptography*. Sementara itu, orang yang berusaha memecahkan kode enkripsi tanpa kuncinya disebut *cryptoanalyst* (*hacker*).

Dalam dunia kriptografi, pesan yang akan dirahasiakan disebut *plaintext*. Pesan yang sudah diacak disebut *ciphertekt*. Proses untuk mengkonversi *plaintext* menjadi *ciphertext* disebut enkripsi. Proses untuk mengembalikan *plainteks* dari *cipherteks* disebut deskripsi. Algoritma kriptografi (*ciphers*) adalah fungsi-fungsi matematika yang digunakan untuk melakukan enkripsi dan deskripsi. Pengertian dasar enkripsi yaitu Enkripsi (*encryption*) merupakan proses yang dilakukan untuk menyandikan *plaintext*

sehingga menjadi *ciphertext*. Selain enkripsi ada juga dekripsi. Dekripsi (*decryption*) merupakan proses yang dilakukan untuk memperoleh kembali *plaintext* dari *ciphertext*

Dua macam tipe kunci enkripsi yaitu: kunci simetrik dan kunci asimetrik. *Algoritma simetrik* menggunakan kunci yang sama untuk mengenkrip dan mendekrip. *Algoritma asimetrik* menggunakan dua kunci, kunci publik untuk enkripsi dan kunci pribadi untuk melakukan deskripsi.

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak. Dengan enkripsi, data Anda disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (*decrypt*) data tersebut, digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (*privat key*) atau dengan kunci yang berbeda (*public key*). Enkripsi menggunakan semacam algoritma untuk mengubah data atau pesan asli yang disebut dengan *plaintext* menjadi *chipertext*, atau bentuk yang terenkripsi. Proses sebaliknya untuk mengubah *chipertext* menjadi *plaintext* disebut dekripsi.

Model enkripsi yang digunakan secara luas adalah model yang didasarkan pada data *encrytion standard* (DES), yang diambil oleh Biro standart nasional US pada tahun 1977. Untuk DES data di enkripsi dalam 64 *bit block* dengan menggunakan 56 *bit kunci*. Dengan menggunakan kunci ini, 64 data *input* diubah dengan suatu urutan dari metode menjadi 64 *bit output*. Proses yang sama dengan kunci yang sama digunakan untuk mengubah kembali enkripsi.

Selain DES, juga ada PGP dan RSA *System*. RSA yang merupakan kepanjangan dari *Rivest, Shamir, Adleman* adalah algoritma enkripsi yang menggunakan dua kunci. Sistem ini dikembangkan tahun 1977. PGP juga menggunakan dua kunci seperti RSA.

PGP ditemukan oleh Philip Zimmerman dan merupakan salah satu sistem enkripsi yang banyak digunakan di internet karena efektif, gratis, dan mudah digunakan.

Pada sistem dua kunci atau disebut juga *public key system*, satu kunci mengenkripsi pesan, lalu kunci lain yang terhubung secara matematis digunakan untuk mendekripsi pesan. *Secure Sockets Layer* (SSL) juga merupakan sistem enkripsi yang digunakan oleh *Netscape* untuk mengirim dokumen atau pesan melalui internet.

Kelompok enkripsi terdiri dari 3 kelompok yaitu :

1. Enkripsi Simetrik (*Symmetric encryption*)

Menggunakan kunci (*key*) yang sama untuk proses enkripsi dan dekripsi, masalah yang muncul adalah kesulitan dalam manajemen *key*. Misalnya dilakukan pengirim data yang telah di enkripsi ke seorang penerima melalui e-mail, orang yang diberi data ini hanya dapat merubah data ke dalam bentuk aslinya dengan menggunakan *key* yang sama. Jadi pengirim harus memberitahukan ke penerima data *key* yang digunakan, disini masalahnya bagaimana mengirim *key* ke penerima tersebut. Algoritma enkripsi yang menggunakan metode ini adalah Data Encryption Standard (DES), AES, IDEA, RC-4, RC-5.

2. Enkripsi Asimetrik (*Asymmetric encryption*)

Menggunakan kunci (*key*) yang berbeda untuk proses enkripsi dan dekripsi. Pada sistem asimetrik dikenal adanya *private key* dan *public key*. Jika melakukan pengiriman data yang di enkripsi ke penerima, pengrim melakukan enkripsi dengan menggunakan *public key* dari penerima dan data hanya dapat dirubah kembali dalam bentuk *plaintext* dengan menggunakan *private key* yang dimiliki penerima. Algoritma enkripsi yang menggunakan metode ini adalah RSA, Dife-Hillman.

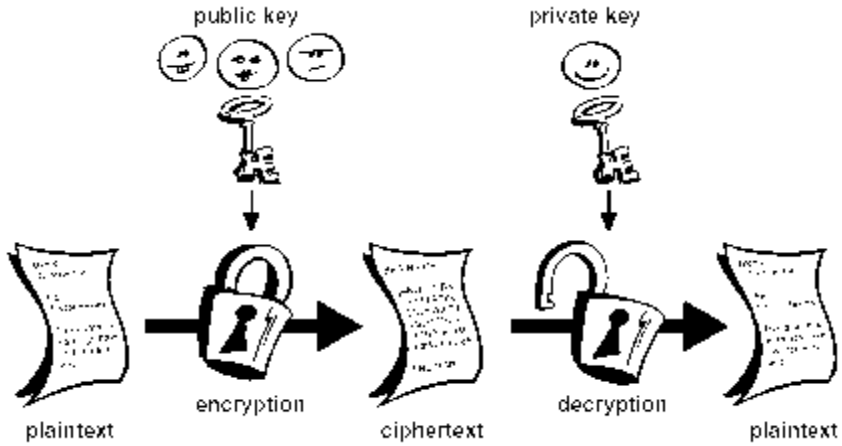
3. Enkripsi Hibrid (*Hybrid encryption*)

Metode ini menggabungkan konsep simetrik dan asimetrik, dengan menggunakan *key random* data dienkripsi dengan metode simetrik. Tahap berikutnya *key random* yang dipakai untuk proses enkripsi data juga dienkripsi, tetapi menggunakan metode asimetrik dengan menggunakan *public key* dari penerima. *Ciphertext* yang dihasilkan masing-masing metode digabungkan dan dikirimkan ke penerima. Penerima akan membuka *Ciphertext* untuk *key word* dengan menggunakan *private key* yang dimilikinya.

2.10 Kriptografi Public Key

Permasalahan dari key distribution dipecahkan oleh *public key cryptography*, konsep yang telah diperkenalkan Bywhitfield Diffie dan Burung martin Hellman di tahun 1975. (Sekarang ada bukti bahwa the British Secret Service lebih dulu dari Diffie dan Hellman dalam menemukannya, tetapi hal tersebut dirahasiakan oleh pemerintahan inggris.)

Public key cryptography adalah suatu skema *asymmetric* yang menggunakan sepasang kunci untuk enkripsi: suatu kunci publik, yang mengenkrip data, dan suatu kunci privat yang bersesuaian untuk deskripsi. Anda mempublis kunci publik Anda kepada dunia sementra kunci pribadi disimpan oleh anda sendiri. Setiap orang dengan suatu salinan kunci publik Anda kemudian bisa mengenkripsi informasi yang hanya Anda dapat membaca melalui kunci privat.



Gambar 2.4 Enkripsi Public Key

Keuntungan utama dari *public key cryptography* adalah mengizinkan orang yang belum memiliki kesepakatan keamanan sebelumnya untuk melakukan pertukaran pesan secara aman. Kebutuhan para pengirim dan penerima untuk berbagi kunci rahasia melalui suatu jalur rahasia telah dihilangkan. Seluruh komunikasi melibatkan hanya kunci publik dan tidak ada kunci privat yang ditransmisikan atau dishare.

2.11 ALGORITMA RSA

2.11.1Pengertian RSA

RSA adalah sebuah algoritma berdasarkan skema public-key cryptography. Diberi nama RSA sebagai inisial para penemunya: Ron Rivest, Adi Shamir, dan Leonard Adleman. RSA dibuat di MIT pada tahun 1977 dan dipatenkan oleh MIT pada tahun 1983. Setelah bulan September tahun 2000, paten tersebut berakhir, sehingga saat ini semua orang dapat menggunakannya dengan bebas. Lebih jauh, RSA adalah algoritma yang mudah untuk diimplementasikan dan dimengerti. Algoritma RSA adalah sebuah

aplikasi dari sekian banyak teori seperti extended euclid algorithm, euler's function sampai fermat theorem.

RSA merupakan contoh yang powerful dan cukup aman dari Public-Key Cryptography. RSA menggunakan perhitungan berdasarkan perhitungan matematika, proses yang digunakan berdasarkan fungsi-fungsi trap-door satu arah. Sehingga melakukan encryption dengan menggunakan public key sangat mudah bagi semua orang, namun proses decryption menjadi sangat sulit.

Proses decryption sengaja dibuat sulit agar seseorang, walaupun menggunakan *Cray supercomputers* dan ribuan tahun, tidak dapat men-decrypt pesan tanpa mempunyai private key. Perlu diingat juga bahwa pemilihan p*q = M haruslah sebuah bilangan yang sangat besar sehingga sulit dicari eksponen decoding-nya karena sulit melakukan pemfaktoran bilangan prima.

2.11.2 Notasi Matematika

Untuk memahami algoritma RSA, seseorang harus memahami beberapa notasi matematika dasar, teori dan formula. Hal tersebut dibutuhkan untuk mendukung semua kalkulasi yang dilakukan dalam algoritma RSA.

1. Modulo (didenotasikan dengan 'x mod m' atau 'x % m' dalam beberapa
   bahasa komputer)
   - x % m = x mod m = pembagian x dengan m dan mengambil sisanya.
   Contoh: 25 mod 5 = 0 karena 5 habis membagi 25
   25 mod 4 = 1 karena 25 / (4 * 6) menyisakan 1
   x mod m = x jika dan hanya jika x < m
2. Z/mZ
   - Z/7Z : { 0,1,2,3,4,5,6 } dimana [7]=[0], [8]=[1], [9]=[2] dan seterusnya.

- Operasi yang didukung dalam Z/mZ adalah penjumlahan, pengurangan, pembagian dan perkalian.
- Inverse: Sebuah elemen dalam Z/mZ seperti A, memiliki sebuah inverse B jika dan hanya jika [A]x[B] = [1]
- Units: Setiap elemen dalam Z/mZ yang memiliki inverse adalah sebuah unit.

Contoh:

Penjumlahan: [2]+[3] = [5] ; [5]+[5] = [10] ... [10-7] = [3]

Pengurangan: [2]-[3] = [-1] = [6] ; [6]-[4] = [2]

Pembagian : [6]/[2] = [3] ; [6]/[4] = [5] ([4]x[5] = [20] = [6])

Perkalian : [2]x[6] = [12] = [5] ;

Soal: [6]/[4]

Penyelesaian :

a. Tempatkan dalam formula [6] = [X][4]

b. Cari inverse dari [4], yaitu [2] ... [4]x[2] = [8] = [1]

c. Kali inverse dengan [6] ... [2]x[6] = [12] = [5]

d. Sehingga [4]x[5] = [20] = [13] = [6]

3. GCD(A,B)

GCD = greatest common divisor.

GCD(A,B) = D

GCD(78,32) = 2, karena tidak ada bilangan yang lebih besar dari dua yang membagi 78 dan 32.

GCD(A,B) dapat ditemukan dengan menggunakan algoritma extended euclid.

Jika GCD(A,B) = 1 maka A and B dalah coprime satu sama lainnya (dengan kata lain, A dan B adalah relatively prime).

4. Memecahkan 8x mod 13 = 1, dimana x adalah bilangan yang belum diketahui.

- Cari gcd(8,13) yang berarti 1 ... yang berarti persamaan dapat diselesaikan.
- Membuat sebuah matriks dan menggunakan operasi gaussian dalam matriks.

```
 8 | 1 0   r2=r2-r1    8 |  1 0  r1=r1-r2
13 | 0 1   ---------->  5  | -1 1  ---------->

 3 |  2 -1  r2=r2-r1    3 | 2 -1
 5 | -1  1  ---------->  2  |-3
```

lakukan sampai kita mendapatkan format : 1 | s t

0 | s' t'

s, t, s', t' dapat berupa bilangan apa saja.

Jika hasil akhir yang di dapat sbb: 0 | s' t' , maka kita harus

1 | s t

rotasi atas-bawah hasil nya menjadi format: 1 | s t

0 | s' t'

sehingga sekarang kita mendapatkan d = 1, s = 5, t = -3, sehingga x = s = 5.

5. Euler's phi function

Euler's phi function adalah sebuah total bilangan unit dalam Z/mZ

Teorinya :

Jika p adalah sebuah bilangan prima, maka phi(p) = p – 1

p dan phi(p) adalah (contoh: gcd(p,phi(p)) = 1)

ii): phi(m*n) = phi(m) * phi (n)

phi(p^a) = (p^a) - p^(a-1)

Contoh:

-- phi(7) = 6

-- phi(840) = phi(8) * phi(105) = phi(2^3) * phi(3*5*7)

= [(2^3) - (2^2)] * phi(3) * phi(5) * phi(7)

2.11.3 Key Generation

Misalkan A ingin B mengirimnya sebuah pesan melalui jalur yang aman. A akan memberikan public key-nya kepada B dan menyimpan private key untuk dirinya.

Prosesnya sebagai berikut :

a. Pilih 2 bilangan prima besar seperti p,q dimana p tidak sama dengan q.
b. Hitung M = p x q
c. Hitung phi(M) = phi(p) * phi(q)
d. Pilih sebuah integer 'e' dimana 1 < e < phi(M) dan 'e' serta phi(M) adalah coprime.
e. Hitung 'd' integer sehingga (d * e) mod M = 1
f. (M,e) adalah public key dimana M adalah modulo dan e adalah eksponen encryption.
g. (M,d) adalah private key dimana M adalah modulo dan d adalah eksponen decryption.

2.11.4 Enkripsi dan Dekripsi Pesan

Enkripsi

Misalkan B ingin mengirim sebuah pesan 'H' kepada A. prosesnya :

a. Alice harus membuat keynya; sehingga ia memiliki private dan public keys.

private key = (M,d)

public key = (M,e)

b. Mengubah 'H' menjadi sebuah bilangan yang menggunakan alphabet yang valid dengan tabel bilangan. Sebuah contoh mudah adalah :

mapping A = 1, B = 2 ... Z = 26.

sehingga H = 8

c. C = 8^e (mod M)

C adalah sebuah bilangan ter-encrypt.

d. B mengirimkan bilangan tersebut kepada A sehingga A dapat melakukan decode ulang menggunakan private keynya.

Dekripsi

Misalkan A menerima sebuah pesan ter-encrypt, ia akan men-decrypt-nya menggunakan tahapan-tahapan berikut:

a. Alice mempunyai private key dari langkah-langkah di atas (M,d)

b. N = C^d (mod M)

c. N adalah bilangan. Gunakan konversi table alphabet untuk mengubah N menjadi karakter yang direpresentasikannya.

Beberapa contohnya :

Contoh 1

a. Generate Key (kita dapat melewati langkah ini untuk menemukan p dan q)

1. M = 101 , sebuah bilangan prima --> phi(M) = 100

2. a] Misalkan e = 13

b] Cari d (e*d) mod M = 1

Gunakan persamaan (a*x) mod M = 1

d = 77

b. Kata "HELLO" digunakan sebagai pesan, dan diubah menurut numerical representation-nya.

HELLO = 08 05 12 12 15

c. Encoding pesan.

8^13 mod 101 = 18

5^13 mod 101 = 56

12^13 mod 101 = 53

15^13 mod 101 = 7

Sehingga pesan ter-encrypt atau ciphertext adalah 18,56,53,53,07.

d. Decoding pesan.

18^77 mod 101 = x1

56^77 mod 101 = x2

53^77 mod 101 = x3 = x4

07^77 mod 101 = x5