HASIL PENELITIAN

OTENTIKASI CITRA DENGAN MENGGUNAKAN KOMBINASI METODE SECURE HASH ALGORITHM-384 (SHA-384) DAN DISCRETE COSINE TRANSFORM

IMAGE AUTHENTICATION UTILIZED COMBINATION OF SECURE HASH ALGORITHM-384 (SHA-384) AND DISCRETE COSINE TRANSFORM

ANILAH TIRTASARI
P2700208006

PROGRAM STUDI TEKNIK ELEKTRO
PROGRAM PASCASARJANA
UNIVERSITAS HASANUDDIN
MAKASSAR
2012

OTENTIKASI CITRA DENGAN MENGGUNAKAN KOMBINASI METODE SECURE HASH ALGORITHM-384 (SHA-384) DAN DISCRETE COSINE TRANSFORM

Tesis

Sebagai Salah Satu Syarat Untuk Mencapai Gelar Magister

Program Studi

Teknik Elektro

Disusun dan diajukan oleh

ANILAH TIRTASARI

Kepada

PROGRAM PASCASARJANA

UNIVERSITAS HASANUDDIN

MAKASSAR

2012

TESIS

OTENTIKASI CITRA DENGAN MENGGUNAKAN KOMBINASI METODE SECURE HASH-384 (SHA-384) DAN DISCRETE COSINE TRANSFORM

Disusun dan diajukan oleh

ANILAH TIRTASARI

Nomor Pokok P2700208006

telah dipertahankan di depan Panitia Ujian Tesis

Pada tanggal 31 Juli 2012

dan dinyatakan telah memenuhi syarat

Menyetujui

Komisi Penasihat,

Dr.Ir. Zahir Zainuddin, M.Sc	**Drs. Suarga, M.Sc.,M.Math, Ph.D**
Ketua	**Anggota**
Ketua Program Studi Teknik Elektro	**Direktur Program Pascasarjana Universitas Hasanuddin**
Prof. Dr. Ir. H. Salama Manjang, MT	**Prof.Dr.Ir.Mursalim, M.Sc**

PERNYATAAN KEASLIAN TESIS

Yang bertangan tangan di bawah ini :

Nama : Anilah Tirtasari

Nomor Induk Mahasiswa : P2700208006

Program Studi : Teknik Elektro

Konsentrasi : Teknik Informatika

Menyatakan dengan sebenarnya bahwa tesis yang saya tulis ini benar-benar merupakan karya saya sendiri, bukan merupakan pengambilalihal tulisan atau pemikiran orang lain. Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan tesis ini hasil karya orang lain, saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar, July 2012

Yang menyatakan,

Anilah Tirtasari

PRAKATA

Puji syukur penulis panjatkan kehadirat Allah S.W.T. karena berkat limpahan Rahmat dan Karunia-Nya sehingga penulis dapat menyelesaikan tulisan hasil penelitian tesis yang berjudul: “OTENTIKASI CITRA DENGAN MENGGUNAKAN KOMBINASI METODE SECURE HASH ALGORITHM-384 (SHA-384) DAN DISCRETE COSINE TRANSFORM (DCT).

Dalam proses penyusunan tesis ini berbagai hambatan yang dihadapi penulis. Namun atas bantuan, bimbingan dan kerjasama dari berbagai pihak sehingga tesis ini dapat selesai. Olehnya itu, perkenankan penulis dengan segala kerendahan hati menyampaikan ucapan terimakasih dan penghargaan yang setinggi-tingginya kepada :

1. Bapak Prof. Dr. Salama Manjang, M.T selaku Ketua Program Studi Magister Teknik Elektro pada Program Pascasarjana Universitas Hasanuddin Makassar
2. Bapak Dr. Ir. Zahir Zainuddin, M.Sc sebagai Pembimbing Utama yang dengan penuh kesabarannya membimbing penulis, memberikan masukan-masukan, serta arahan-arahan hingga terselesainya tesis ini.
3 Bapak Drs. Suarga, MSc., M.Math, Ph.D selaku Pembimbing kedua yang telah memberikan bimbingan, petunjuk, dan arahan serta mengkritisi sejak penelitian sampai pada penyelesaian penulisan tesis ini.
4. Bapak Prof.Dr. Ir. Nadjamuddin Harun, MS dan Bapak Dr.Ir. Zulfajri B. Hasanuddin selaku Penguji dalam uji sidang tesis yang telah banyak memberikan masukan, arahan untuk perbaikan tesis ini.
5. Kepada seluruh staf dan karyawan Fakultas Teknik Jurusan Elektro Universitas Hasanuddin Makassar

6. Kedua Orang tua penulis, yang dengan penuh kasih sayang dan ketulusan mendoakan penulis agar selalu diberi kekuatan lahir dan batin hingga dapat menyelesaikan pendidikan di Program Pascasarjana Universitas Hasanuddin Makassar
7. Kedua saudara penulis yang telah banyak memberikan pengorbanan, semangat, doa, hingga penulis dapat menyelesaikan tesis ini
8. Teman teman angkatan 2008 Program Magister Teknik Elektro yang telah memberikan dukungan moril kepada penulis
9. Kepada rekan rekan di Jurusan Matematika FMIPA Unhas yang telah meluangkan waktu untuk saling berbagi ilmu bersama
10. Semua pihak yang telah turut membantu penyelesaian tesis ini yang tidak sempat penulis sebutkan satu persatu

Dengan segala keterbatasan waktu dan kemampuan yang ada, semoga penelitian yang mengangkat judul “OTENTIKASI CITRA DENGAN MENGGUNAKAN KOMBINASI METODE SECURE HASH ALGORITHM-384 (SHA-384) DAN DISCRETE COSINE TRANSFORM (DCT).” ini dapat diterima dan bermanfaat bagi umat manusia. Kritikan dan saran yang sifatnya membangun sangat diharapkan demi memperoleh hasil yang lebih baik.

Makassar, Juli 2012

Anilah Tirtasari

ABSTRACT

ANILAH TIRTASARI. *Image Authentication Utilized Combination of Secure Hash Algorithm-384 (SHA-384) and Discrete Cosine Transform* (supervised by Zahir Zahinuddin and Suarga).

Nowdays, the data security and secrecy of an image in computer network has been an essential and developing issue. Therefore, we need a method to keep authenticity of an image.

This study aims to authenticate an image using combination of Secure Hash Algorithm-384 (SHA-384) and Discrete Cosine Transform (DCT) methods. SHA-384 is used to calculate the hash value of an image. It will then be inserted into the image through watermarking and resulted as a watermarked image. The DCT method is used in the watermarking process. The authenticity is examined by comparing the image hash value of the extracted result with hash value of the original image through Bit Error Rate (BER) result.

The BER result achieved in this research was only about 50% such that the images can not be concluded as an authentic yet.

Keywords: *Image, SHA-384, Discrete Cosine Transform (DCT), Bit Error Rate (BER), Authentic.*

ABSTRAK

ANILAH TIRTASARI. O*tentikasi Citra Dengan Menggunakan Kombinasi Metode Secure Hash Algorithm-384 (SHA-384) dan Discrete Cosine Transform (DCT)* (dibimbing oleh Zahir Zainuddin dan Suarga).

Keamanan dan kerahasiaan data berupa citra pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Oleh karena itu diperlukan suatu Metode untuk menjaga keotentikan citra tersebut.

Tujuan dari penelitian ini adalah untuk melakukan otentikasi terhadap suatu citra menggunakan kombinasi antara metode *Secure Hash Algorithm-384 (SHA-384)* dan *Discrete Cosine Transform (DCT)*.

Metode SHA-384 digunakan untuk menghitung nilai hash suatu citra. Nilai hash yang diperoleh kemudian disisipkan ke dalam citra dengan proses watermarking menghasilkan citra terwatermark. Metode yang digunakan dalam proses watermarking ini adalah metode DCT. Untuk menguji keaslian citra dilakukan dengan membandingkan nilai hash hasil pengekstrakan dengan nilai hash citra asli melalui perhitungan *Bit Error Rate (BER).*

Pada penelitian ini nilai BER untuk seluruh citra uji sekitar 50% dan belum dapat dikatakan otentik.

Kata kunci : Citra, SHA-384, Discrete Cosine Transform (DCT), *Bit Error Rate* (BER), Otentik.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

.

BAB I

PENDAHULUAN

A. Latar Belakang

Perkembangan dunia digital, terutama dengan berkembangnya Internet, menyebabkan informasi dalam berbagai bentuk dan media dapat tersebar dengan cepat tanpa batas ruang dan waktu. Namun, karena informasi dalam bentuk data multimedia rentan terhadap perubahan, penyebaran data melalui Internet ini juga memberikan kesempatan kepada pihak yang tidak berhak untuk membuat salinan tanpa izin dari pemilik yang sah, bahkan menyebarkannya untuk tujuan komersial. Hal ini dapat menimbulkan persoalan hak cipta bagi data multimedia yang tersebar (Cahyana et al, 2007).

Citra digital adalah satu dari sekian varian data digital yang sering disalahgunakan. Pengguna citra digital seringkali memanipulasi citra digital untuk mendapatkan tampilan citra digital baru sesuai dengan keinginannya. Terkait dalam hal ini beberapa pemilik citra digital tidak ingin citra digital miliknya dapat berubah, atau paling tidak mereka mengetahui jika citra miliknya telah berubah atau termanipulasi (Barata, A.I , 2005)

Salah satu cara untuk mengetahui keaslian (*authentication*) suatu citra adalah dengan kolaborasi metode *image hashing* dan *digital watermarking*. *Image hashing* adalah menghitung nilai hash suatu citra digital dengan suatu fungsi hash tertentu, sedangkan *digital watermarking* atau *watermarking* adalah penambahan data rahasia (*watermark*) ke dalam citra digital yang keberadaannya tidak menggangu tampilan citra digital yang disisipi. Perhitungan nilai hash dilakukan dengan *Secure Hash Algorithm*-384 (SHA-384). Nilai hash ini merupakan identitas citra yang akan dijadikan watermark dan disisipkan kedalam citra. Adapun teknik *watermarking* dalam hal ini penyisipan dan pengekstrakan *watermark* dilakukan dengan *Discrete Cosine Transform* (DCT). Keotentikan suatu citra ditentukan dengan membandingkan kedua nilai hash, yaitu sebelum penyisipan dan setelah pengekstrakan. Citra tersebut dikatakan masih asli apabila kedua nilai hash sama sampai batas toleransi tertentu.

Adapun alasan menggunakan metode kombinasi SHA 384 dan DCT untuk otentikasi citra adalah karena kebanyakan metode otentikasi yang lain menggunakan kombinasi media gambar sebagai citra yang disisipi (*host*) dan tulisan ataupun logo sebagai citra yang menyisipi (*watermark*). Jika menggunakan SHA 384 sebagai watermark, maka yang disisipkan kedalam citra tersebut tidak lain adalah identitas citra itu sendiri sehingga ada keunikan tersendiri dimana ada *dependency* antara citra *host* dengan *watermark*nya. Sedangkan pemilihan DCT sendiri karena DCT merupakan jenis transformasi yang lazim digunakan dalam pengolahan citra.

B. Rumusan Masalah

Adapun rumusan masalah penelitian ini adalah;

1. Bagaimana melakukan otentikasi citra dengan menggunakan metode Secure Hash Algorithm-384(SHA-384) dan *Discrete Cosine Transform* (DCT).
2. Bagaimana visibilitas nilai hash yang disembunyikan ke dalam citra.

C. Tujuan Penelitian

Adapun tujuan penulisan penelitian ini adalah;

1. Mengaplikasikan metode Secure Hash Algorithm-384 (SHA-384) dan *Discrete Cosine Transform* (DCT) ini untuk melakukan otentikasi terhadap suatu citra.
2. Menghitung nilai Peak Signal to Noise Ratio (PSNR) untuk melihat visibilitas nilai hash yang disembunyikan.

D. Manfaat Penelitian

Adapun manfaat yang diharapkan dari penelitian ini adalah sebagai berikut:

1. Untuk meningkatkan pemahaman tentang penggunaan metode Secure Hash Algoritm-384 (SHA-384) dan Discrete Cosine Transform (DCT) untuk melakukan otentikasi citra.
2. Sebagai bahan perbandingan untuk penelitian otentikasi citra yang lain.
3. Menawarkan sebuah metode untuk melindungi data citra dari upaya penggandaan atau manipulasi secara illegal misalnya pada citra hasil seni fotografi, citra medis, dan sebagainya.
4. Membantu fotografer profesional dan museum untuk melindungi karya ciptanya.

E. Batasan Penelitian

Dalam penelitian ini, batasan masalah yang digunakan adalah;

1. Citra asli, yaitu berupa citra gray scale dan citra berwarna 24 bit
2. Citra dalam format JPG
3. Proses perhitungan nilai hash yang digunakan untuk mendeteksi keotentikan suatu citra adalah SHA-384

4. Penyisipan dan pengekstrakan citra menggunakan Metode DCT

5. Diasumsikan citra awal sebagai citra asli

F. Sistematika Penelitian

Pada BAB I membahas tentang latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, ruang lingkup, sistematika penelitian.

Pada BAB II ini membahas tentang teori-teori yang mendukung penulisan penelitian ini. Pembahasan meliputi tentang Citra Digital, Fungsi Hash, Otentikasi Citra, PSNR, serta Kerangka Pikir.

Pada Bab III membahas mengenai metode penelitian, yang merinci tentang jenis penilitian, lokasi dan waktu penelitian, serta tahapan penelitian.

Pada Bab IV membahas mengenai hasil dan pembahasan dari skema rancangan sistem, implementasi, uji coba dan analisis sistem

Bab V merupakan penutup yang berisi kesimpulan hasil penelitian dan saran untuk penelitian berikutnya.

BAB II

TINJAUAN PUSTAKA

A. Citra Digital

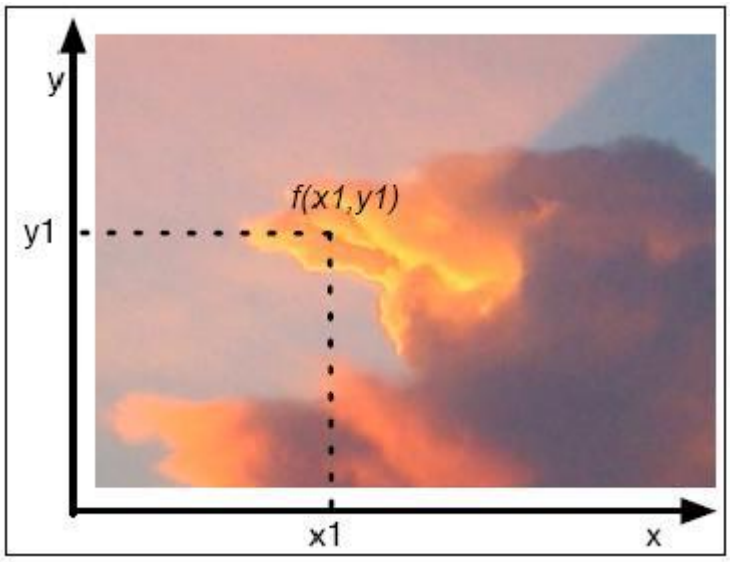
Menurut Sutoyo (2009), citra adalah suatu representasi dari suatu objek. Citra sebagai keluaran suatu sistem perekaman dapat bersifat optik berupa foto, analog (dihasilkan oleh perangkat analog), atau bersifat digital (dihasilkan perangkat digital).

Sebuah citra digital dapat diwakili oleh sebuah matriks yang terdiri dari M kolom dan N baris, dimana perpotongan antara kolom dan baris disebut piksel (*piksel=picture element*), yaitu elemen terkecil dari sebuah citra. Piksel mempunyai dua parameter, yaitu koordinat dan intensitas atau warna. Nilai yang terdapat pada koordinat (x,y) adalah f(x,y) yaitu besar intensitas atau warna dari piksel di titik itu. Oleh sebab itu, sebuah sebuah citra digital dapat ditulis dalam bentuk matriks berikut.

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \dots & f(0,M-1) \\ f(1,0) & \dots & \dots & f(1,M-1) \\ \dots & \dots & \dots & \dots \\ f(N-1,0) & f(N-1,1) & \dots & f(N-1,M-1) \end{bmatrix} \text{.....} \quad (1)$$

Berdasarkan gambaran tersebut, secara matematis citra digital dapat dituliskan sebagai fungsi intensitas *f(x,y)*, di mana harga *x*

(baris) dan *y* (kolom) merupakan koordinat posisi dan *f(x,y)* adalah nilai fungsi pada setiap titik *(x,y)* yang menyatakan besar intensitas citra atau warna dari piksel di titik tersebut



Gambar 1. Koordinat citra digital

1. Citra grayscale

Citra grayscale merupakan citra digital yang hanya memiliki satu nilai kanal pada setiap pikselnya, dengan kata lain nilai bagian RED = GREEN= BLUE. Nilai tersebut digunakan untuk menunjukkan tingkat intensitas. Warna yang dimiliki adalah warna dari hitam,keabuan, dan putih. Tingkatan keabuan di sini merupakan warna abu dengan berbagai tingkatan dari hitam hingga menjadi putih. Citra grayscale memiliki kedalaman warna 8 bit (256 warna keabuan).

2. Citra warna

Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red, Green, Blue* - RGB).

RGB adalah suatu model warna yang terdiri dari merah, hijau, dan biru, digabungkan dalam membentuk suatu susunan warna yang luas. Setiap warna dasar, misalnya merah, dapat diberi rentang-nilai. Untuk monitor komputer, nilai rentangnya paling kecil = 0 dan paling besar = 255. Pilihan skala 256 ini didasarkan pada cara mengungkap 8 digit bilangan biner yang digunakan oleh mesin komputer. Dengan cara ini, akan diperoleh warna campuran sebanyak 256 x 256 x 256 = 1677726 jenis warna. Sebuah jenis warna, dapat dibayangkan sebagai sebuah vektor di ruang 3 dimensi yang biasanya dipakai dalam matematika, koordinatnya dinyatakan dalam bentuk tiga bilangan, yaitu komponen-x, komponen-y dan komponen-z. Misalkan sebuah vektor dituliskan sebagai $\mathbf{r}$ = (x,y,z). Untuk warna, komponen-komponen tersebut digantikan oleh komponen R(ed), G(reen), B(lue). Jadi, sebuah jenis warna dapat dituliskan sebagai berikut: warna = RGB(30, 75, 255). Putih = RGB (255,255,255), sedangkan untuk hitam= RGB(0,0,0). (Rachmawati, 2008)

B. Fungsi Hash

1. Pengetian fungsi hash

Fungsi hash adalah suatu cara menciptakan fingerprint dari berbagai data masukan. Fungsi hash akan mengganti data tersebut untuk menciptakan fingerprint, yang biasa disebut nilai hash. Fungsi hash biasanya diperlukan bila kita menginginkan pengambilan sidik jari suatu pesan sebagaimana sidik jari manusia yang menunjukkan identitas pemilik sidik jari. Fungsi ini diharapkan pula mempunyai kemampuan yang serupa dengan sidik jari manusia, dimana sidik jari pesan diharapkan menunjuk ke satu pesan dan tidak menunjuk kepada pesan lainnya.

Fungsi ini juga dinamakan fungsi kompresi karena biasanya masukan fungsi satu arah ini selalu lebih besar dari pada keluarannya, sehingga seolah-olah mengalami kompresi. Namun kompresi hasil fungsi ini tidak dapat dikembalikan keasalnya sehingga disebut sebagai fungsi satu arah (*one way function*). Keluaran fungsi hash dikenal dengan istilah message digest, karena seolah-olah merupakan inti sari pesan. Padahal tidak demikian, sebab inti sari pesan mestinya merupakan ringkasan pesan yang masih dapat dipahami maknanya, sedangkan di fungsi hash terjadi perlakuan sebaliknya, orang tidak tahu pesan aslinya.

Standarisasi fungsi hash yang ditetapkan di dalam FIPS (*Federal Information Processing Standards*) adalah SHS (*Secure Hash Standard*) (Sebastian.A ,2007)

2. Sifat-sifat fungsi hash

Fungsi hash satu arah (*one way hash function*) adalah fungsi hash yang bekerja satu arah, yaitu suatu fungsi hash yang dengan mudah dapat menghitung nilai hash dari pesan, tetapi sangat sukar untuk menghitung pesan dari nikai hash. Sebuah fungsi hash satu arah *H(M)*, beroperasi padasuatu pesan M dengan panjang sembarang, dan menghasilkan nilai hash h yang memiliki panjang tetap. Perubahan sekecil apapun pada M akan menghasilkan nilai hash yang berbeda.

Sifat-sifat fungsi hash adalah sebagai berikut:

1. Fungsi H(M) dapat diterapkan pada blok data berukuran berapa saja
2. H(M) menghasilkan nilai h dengan panjang tetap (fixed-length output)
3. Mudah menghitung H(M) untuk sembarang nilai M yang diberikan.

4. Untuk setiap h yang dihasilkan, tidak mungkin dikembalikan nilai M sedemikian sehingga H(M) = h. Itulah sebabnya fungsi H dikatakan fungsi hash satu arah (one-way hash function).

5. Untuk setiap M yang diberikan, tidak mungkin mencari M' ≠ M yang memenuhi H(M') = H(M').

Nilai fungsi satu arah biasanya berukuran kecil, sedangkan pesan berukuran besar. Fungsi hash sangat berguna untuk menjaga keotentikan sebuah data. Sudah banyak algoritma fungsi hash yang diciptakan, namun fungsi hash yang umum digunakan saat ini adalah SHA (*Secure Hash Algorithm*). (Sebastian.A, 2007)

3. Secured Hash Algorithm (SHA)

Secara umum, algoritma fungsi SHA dapat dideskripsikan dan dibagi menjadi dua bagian:

1. Preprocessing. Sebelum proses perhitungan dilakukan, terlebih dahulu membagi pesan menjadi blok-blok dengan panjang tertentu, penambahan bit pengganjal serta mengatur nilai awal untuk digunakan pada perhitungan nilai hash.

2. Perhitungan hash. Dilakukan proses pembangkitan message schedule (W_t) dari pesan yang telah diblok-blok dengan panjang tertentu, dan kemudian message schedule tersebut bersama

dengan fungsi-fungsi lainnya serta konstanta-konstanta yang telah terdefinisi, digunakan secara iteratif untuk membangkitkan nilai hash akhir.

Fungsi SHA memiliki perbedaan pada ukuran pesan, ukuran blok, dan ukuran word data yang digunakan selama proses komputasi. Perbedaan fungsi SHA secara lengkap dapat dilihat pada Tabel 1 sebagai berikut:

Tabel 1. Perbedaan karakteristik variansi fungsi SHA

Fungsi	Ukuran Pesan (bit)	Ukuran Blok (bit)	Ukuran Word (bit)	Ukuran Message Digest (bit)
SHA-1	$< 2^{64}$	512	32	160
SHA-256	$<2^{64}$	512	32	256
SHA-384	$<2^{128}$	1024	64	384
SHA-512	$<2^{128}$	1024	64	512

Sumber : NIST, Secure Hash Standard. Fips 180-2.pdf, August 2002, p.3

Versi pertama dari SHS yaitu SHA-1 (Secure Hash Algorithm) sesuai dari FIPS 180-1 pada bulan April 1997. SHA-1 merupakan jenis fungsi hash yang saat ini paling banyak diimplementasikan. Dengan adanya kemajuan teknologi, tentunya ukuran kebutuhan ukuran message juga semakin besar begitu juga dengan tingkat ketahanan dari Attacker. Sehingga NSA (National Security Agency) mengembangkan SHS sehingga pada bulan Agustus 2002, versi kedua dari SHS terdiri dari

beberapa fungsi hash yaitu SHA-256, SHA-384, dan SHA-512. (FIPS 2002). Dalam tulisan ini fungsi hash yang akan dibahas adalah SHA-384.

4. SHA-384

Fungsi SHA-384 dapat digunakan untuk menghitung nilai hash dari sebuah pesan, dimana pesan tersebut memiliki panjang maksimum 2^{128} bit. Hasil akhir dari algoritma SHA-384 adalah sebuah nilai hash dengan panjang 384 bit.

Dalam proses komputasinya, SHA-384 menggunakan 6 fungsi lojik, dimana tiap fungsi beroperasi menggunakan tiga buah *word* 64 bit (x, y, dan z) dan keluarannya berupa sebuah *word* 64 bit yang baru. Berikut ini adalah fungsi-fungsi dalam SHA-384

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

$$Maj(x,y,z) = (x \wedge y) \oplus (x \wedge z) \oplus (y \wedge z)$$

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

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

$$\sigma_0^{\{512\}} (x) = ROTR^{1} (x) \oplus ROTR^{8} (x) \oplus SHR^{7} (x)$$

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

Sebelum membahas lebih jauh mengenai SHA-384, beberapa parameter-parameter dan simbol-simbol pada proses perhitungan yang digunakan dalam mengoperasikan fungsi hash ini perlu diketahui. Parameter dan simbol tersebut terangkum pada tabel 2 berikut

Tabel 2. Parameter dalam SHA-384

PARAMETER	KETERANGAN
a, b, c,.., h	*variabel* yang digunakan untuk penampung *w-bit word* data selama proses *hash* berlangsung.
H	*variabel* yang digunakan untuk penampung nilai *hash.*
K_t	*variabel* yang digunakan untuk menampung nilai konstanta.
k	Bit Pengganjal.
L	*P*anjang pesan dalam ukuran bit.
M	Jumlah *bit* dari blok pesan.
n	Jumlah bit yang dirotasikan atau digeser.
N	Banyaknya blok pesan.
T	B*it* sementara yang digunakan ketika proses.
Wt	M*essage schedule*
$\wedge$	operator bit *AND*
v	operator bit OR
$\oplus$	operator bit XOR
$\neg$	operator NOT.
+	Operator bit penambahan
PARAMETER	**KETERANGAN**
SHR^n (*x*)	Operasi SHR^n (x) dimana x adalah 64-bit dan n adalah nilai integer dengan interval 0 ≤ n < 32*. Ekuivalen dengan pergeseran terhadap x dengan pergeseran sebanyak n kali ke kanan.*
$ROTR^n$(*x*)	Operasi $ROTR^n$*(x) ekuivalen dengan rotasi terhadap x dengan rotasi sebanyak n kali ke kanan.*

Sumber : NIST,Secure Hash Standard. Fips 180-2.pdf, August 2002, p.4-5

Nilai hash awal pada algoritma SHA-384 sesuai rekomendasi FIPS 180-2 adalah sebagai berikut:

Tabel 3. Nilai hash awal untuk SHA-384

$H_0^{(0)}$	$cbbb9d5dc1059ed8$
$H_1^{(0)}$	$629a292a367cd507$
$H_2^{(0)}$	$9159015a3070dd17$
$H_3^{(0)}$	$152fecd8f70e5939$
$H_4^{(0)}$	$67332667ffc00b31$
$H_5^{(0)}$	$8eb44a8768581511$
$H_6^{(0)}$	$db0c2e0d64f98fa7$
$H_7^{(0)}$	$47b5481dbefa4fa4$

SHA-384 memakai 80 konstanta 64 bit yang ditampung pada variabel $K_0^{\{384\}}$, $K_1^{\{384\}}$, $K_{79}^{\{384\}}$. Dalam hexadesimal konstanta dapat dilihat pada tabel 3.

Tabel 4. Nilai Konstanta untuk SHA-384

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	84c87814a1fDab72	8cc702081a6439ec
90befffa23631e28	a4506cebde82bde9	bef9a3f7b2c67915	c67178f2e372532b
ca273eceea26619c	d186b8c721c0c207	eada7dd6cde0eb1e	f57d4f7fee6ed178
06f067aa72176fba	0a637dc5a2c898a6	113f9804bef90dae	1b710b35131c471b
28db77f523047d84	32caab7b40c72493	3c9ebe0a15c9bebc	431d67c49c100d4c
4cc5d4becb3e42b6	597f299cfc657e2a	5fcb6fab3ad6faec	6c44198c4a475817

Sumber : NIST, Secure Hash Standard. **Fips 180-2.pdf.** August **2002, p. 10-11**

C. Otentikasi Citra

Secara umum, otentikasi citra diperhitungkan sebagai suatu prosedur yang memberi garansi bahwa *content* gambar tidak berubah, atau paling tidak karakterisitik-karakteristik visual (atau semantik) gambar terjaga setelah memanipulasi seperti kompresi JPEG. Informasi otentikasi ditambahkan pada citra untuk digunakan mengidentifikasi keaslian suatu citra.

Berdasarkan kebutuhan akan keutuhan citra (*integrity*) dan kebutuhan *legitimacy*, berbagai variasi teknik telah diusulkan untuk proses otentikasi citra. Berdasarkan cara yang dipilih untuk menyampaikan data otentikasi, teknik-teknik ini dibagi menjadi dua buah kategori yaitu :

1. Teknik berbasis *labelling*
2. Teknik berbasis *watermarking*

Perbedaan utama diantara kedua kategori ini adalah bahwa teknik berbasis *labelling* menciptakan data otentikasi atau *signature* yang ditulis ke dalam sebuah file yang terpisah atau sebuah *header* yang dipisahkan dari data mentah yang kemudian tersimpan dalam file yang sama. Sementara teknik berbasis *watermarking* dapat diselesaikan tanpa *overhead* sebuah file yang terpisah atau data otentikasi dilekatkan sebagai *watermark* dalam data mentah itu sendiri. (Mahyuddin, 2009).

Pada tulisan ini penulis hanya akan membahas teknik berbasis watermarking untuk otentikasi citra. Teknik watermarking dibanding teknik labelling memiliki kelebihan karena pada teknik watermarking informasi yang disisipkan melekat pada citra sedangkan pada teknik berbasis labelling informasi tambahan diletakkan pada bagian header sehingga keberadaannya mudah dimanipulasi.

1. Watermarking

Watermarking merupakan salah satu bentuk dari steganografi (Ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data yang lain). *Watermarking* juga dapat dikatakan sebagai ilmu yang mempelajari teknik-teknik penyimpanan suatu data (digital) kedalam data *host* digital yang lain (Istilah *host* digunakan untuk data/sinyal digital yang ditumpangi.).

Steganografi memiliki hasil keluaran (*output*) yang sama dengan bentuk aslinya apabila ditangkap oleh indera manusia biasa. Sehingga dapat dikatakan watermarking merupakan suatu cara untuk penyembunyian atau penanaman data / informasi tertentu (baik hanya berupa catatan umum maupun rahasia) ke dalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia (indera penglihatan atau indera pendengaran).

Dalam menyembunyikan pesan atau informasi rahasia, ada kriteria yang harus dipenuhi. (Munir, 2006)

1. *Imperceptbility*. Keberadaan pesan tidak dapat dipersepsi oleh indrawi. Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Begitu pula dengan suara, telinga haruslah mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.

2. *Fidelity*. Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan yang terjadi harus tidak dapat dipersepsi oleh indrawi.
3. *Recovery*. Pesan yang disembunyikan dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan informasi, maka sewaktu-waktu informasi yang disembunyikan ini harus dapat digunakan lebih lanjut sesuai keperluan.

2. Sejarah steganografi dan watermarking

Penggunaan steganografi sebetulnya telah digunakan berabad-abad yang lalu bahkan sebelum istilah steganografi ataupun watermarking itu sendiri muncul. Dalam sejarah Yunani kuno, masyarakatnya biasa menggunakan seorang pembawa pesan sebagai perantara pengiriman pesan. Pengirim pesan tersebut akan dicukur rambutnya, untuk kemudian dituliskan suatu pesan pada kepalanya yang sudah botak. Setelah pesan dituliskan, pembawa pesan harus menunggu hingga rambutnya tumbuh kembali sebelum dapat mengirimkan pesan kepada pihak penerima. Pihak penerima kemudian akan mencukur rambut pembawa pesan tersebut untuk melihat pesan yang tersembunyi. Metode lain yang digunakan oleh masyarakat Yunani kuno adalah dengan menggunakan lilin sebagai media penyembunyi pesan mereka. Pesan dituliskan pada suatu lembaran, dan lembaran tersebut akan ditutup dengan lilin untuk menyembunyikan pesan yang telah tertulis. Pihak penerima kemudian akan menghilangkan lilin

dari lembaran tersebut untuk melihat pesan yang disampaikan oleh pihak pengirim.(Armyta,2006). Selain Bangsa Yunani steganografi pun juga dikenal oleh Bangsa Romawi, yaitu dengan menggunakan tinta tak-tampak (*invisible ink*) untuk menuliskan pesan. Tinta tersebut dibuat dari campuran sari buah, susu, dan cuka. Jika tinta digunakan untuk menulis maka tulisannya tidak tampak. Tulisan di atas kertas dapat dibaca dengan cara memanaskan kertas tersebut.

Pada akhir 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 setengah jadi. Ketika kertas dikeringkan terbentuklah suatu kertas yang ber-*watermark*. Kertas ini biasanya digunakan oleh seniman atau sastrawan untuk menulis karya mereka. Kertas yang sudah dibubuhi tanda-air tersebut sekaligus dijadikan identifikasi bahwa karya seni di atasnya adalah milik mereka.

Ide *watermarking* pada data digital (sehingga disebut *digital watermarking*) dikembangkan di Jepang tahun 1990 dan di Swiss tahun 1993. *Digital watermarking* semakin berkembang seiring dengan semakin meluasnya penggunaan internet, objek digital seperti video, citra, dan suara yang dapat dengan mudah digandakan dan disebarluaskan. (Munir, 2004).

3. Beberapa penelitian watermarking

Penelitian tentang *watermarkin*g telah banyak dilakukan, baik yang bekerja pada domain spasial ataupun domain frekuensi. Istilah domain spasial mengacu pada piksel penyusun citra. Teknik watermarking jenis ini menanamkan data langsung dengan cara memodifikasi nilai intensitas atau warna dari pixel-pixel tertentu dari citra (van Schyndel *et.al*., 1994), sedangkan teknik domain frekuensi mentransformasikan citra dari domain spasial ke domain frekuensi kemudian menyisipkan pesan pada nilai koefisien transformasinya. Contoh teknik yang bekerja pada domain spasial adalah teknik penyisipan *Least Significant Bit* (LSB) (Johnson and Jajodia, 1998). Pada citra RGB metode ini bekerja dengan cara menyisipkan informasi pada bit-bit paling kanan dari setiap elemen RGB. Perubahan bit paling kanan hanya menimbulkan perubahan nilai RGB sebesar 1 dari 256 warna yang ada, yang sulit dipersepsi dengan mata telanjang. Sayangnya watermark yang disembunyikan dengan metode LSB ini dapat mudah dideteksi yaitu dengan mensubtitusi seluruh bit paling kanan pada kanal warna dengan nilai sebaliknya. Metode LSB mudah untuk dideteksi karena penyisipan informasi dilakukan secara langsung dalam bit-bit dokumen tanpa melalui proses pengacakan.

Teknik watermarking lain adalah metode RS yang dikembangkan oleh Fridrich. Pada metode RS citra dibagi kedalam 3 bagian (*regular, singular, unusuable*). Informasi disisipkan pada daerah RS (*regular dan singular*). Hasilnya distorsi pada kualitas citra yang disisipi rendah dan

memiliki kemiripan dengan citra sebelum disispi, tetapi metode ini memiliki kapasitas penyisipan yang terbatas. (J. Fridrich, 2002). Metode lain yang juga menawarkan kualitas citra yang cukup baik setelah disisipi watermark adalah metode (Ni et al, 2003) yang berdasarkan perubahan histogram citra. Pada metode ini walaupun distorsi pada gambar induk yang disisipi kecil, namun terdapat kekurangan dalam kapasitas penyisipan. Kapasitas penyisipan dibatasi oleh jumlah frekuensi dari nilai piksel yang paling sering muncul pada citra.

Pada penelitian ini teknik watermarking yang akan dilakukan adalah watermarking dalam domain frekuensi menggunakan *DCT* dengan mengacu pada algoritma Cox. Algoritma Cox dipilih karena memiliki sifat yang kokoh (robust) dibanding metode LSB dan mampu mengatasi kekurangan yang telah dipaparkan pada metode lain diatas. Adapun modifikasi yang dilakukan penulis adalah mengganti citra biner dengan nilai hash citra sebagai informasi yang akan disisipkan kedalam citra.

4. *Discrete Cosine Transform* (*DCT*)

Discrete Cosine Transform (*DCT*) adalah sebuah fungsi dua arah yang memetakan himpunan *N* buah bilangan *real* menjadi himpunan *N* buah bilangan *real* pula. Secara umum, *DCT* satu dimensi menyatakan sebuah sinyal diskrit satu dimensi sebagai kombinasi linier dari beberapa fungsi basis berupa gelombang kosinus diskrit dengan amplitudo tertentu. Masing-masing fungsi basis memiliki frekuensi yang berbeda-beda,

karena itu, transformasi *DCT* termasuk ke dalam transformasi domain frekuensi. Amplitudo fungsi basis dinyatakan sebagai koefisien dalam himpunan hasil transformasi *DCT*. *DCT* satu dimensi didefinisikan pada persamaan berikut:

$$C(u) = \sum_{u=0}^{N-1} \alpha(u) C(u) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad (2)$$

untuk $0 \leq u \leq N-1$.

C(*u*) menyatakan koefisien ke-*u* dari himpunan hasil transformasi *DCT*. *f*(*x*) menyatakan anggota ke-*x* dari himpunan asal. *N* menyatakan banyaknya suku himpunan asal dan himpunan hasil transformasi. α(*u*) dinyatakan oleh persamaan berikut:

untuk $0 \leq u \leq N-1$.

$\alpha(u) = \sqrt{\frac{1}{N}}$ untuk u = 0;

$\alpha(u) = \sqrt{\frac{2}{N}}$ untuk $1 \leq u \leq N-1$.

Transformasi balikan yang memetakan himpunan hasil transformasi *DCT* ke himpunan bilangan semula disebut juga *inverse DCT* (*IDCT*). *IDCT* didefinisikan oleh persamaan di bawah ini:

$$f(x) = \sum_{u=0}^{N-1} \alpha(u) C(u) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \quad (3)$$

untuk $0 \leq u \leq N-1$..

DCT dua dimensi dapat dipandang sebagai komposisi dari *DCT* pada masing-masing dimensi. Sebagai contoh, jika himpunan bilangan *real* disajikan dalam *array* dua dimensi terhadap masing-masing baris dan kemudian melakukan *DCT* satu dimensi terhadap masing-masing kolom dari hasil *DCT* tersebut. *DCT* dua dimensi dapat dinyatakan sebagai berikut dengan persamaan:

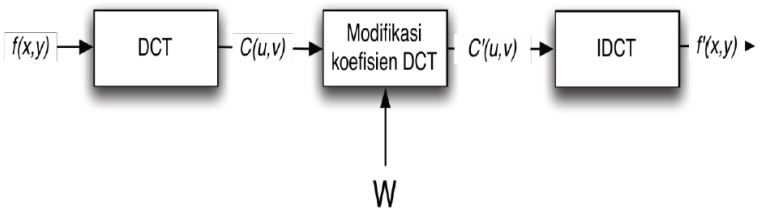
$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2M}\right] cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (4)$$

sedangkan transformasi balikannya (invers) dinyatakan dengan

$$f(x,y) = \alpha(u)\alpha(v)\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} C(u,v)\cos\left[\frac{\pi(2x+1)u}{2M}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right] \quad (5)$$

5. Watermarking dengan *DCT*

Secara umum, setiap proses *watermarking* dengan *metode* apapun terdiri dari dua tahapan, yaitu penyisipan *watermark* dan ekstraksi atau pendeteksian *watermark.* Penyisipan *watermark* pada citra dengan metode *DCT* dilakukan dengan cara terlebih dahulu melakukan transformasi *DCT* terhadap citra yang akan disisipi *watermark*. Setelah dilakukan transformasi, kemudian dilakukan modifikasi terhadap koefisien-koefisien *DCT* sesuai dengan *bit watermark* yang akan disisipkan. Setelah dilakukan modifikasi, dilakukan *inverse DCT* untuk mengembalikan data citra ke ranah spasial. Skema proses *watermarking* di ranah *DCT* dapat dilihat pada



Gambar 2. Skema watermarking citra di ranah *DCT*

f(x,y) melambangkan matriks nilai piksel citra asal, C(u,v) melambangkan matriks koefisien *DCT* citra asal, W melambangkan data watermark yang disisipkan, C'(u,v) melambangkan matriks koefisien *DCT* yang sudah dimodifikasi, dan f'(x,y) melambangkan matriks nilai piksel sesudah penyisipan watermark.

Modifikasi koefisien *DCT* dilakukan berdasarkan persamaan di bawah ini:

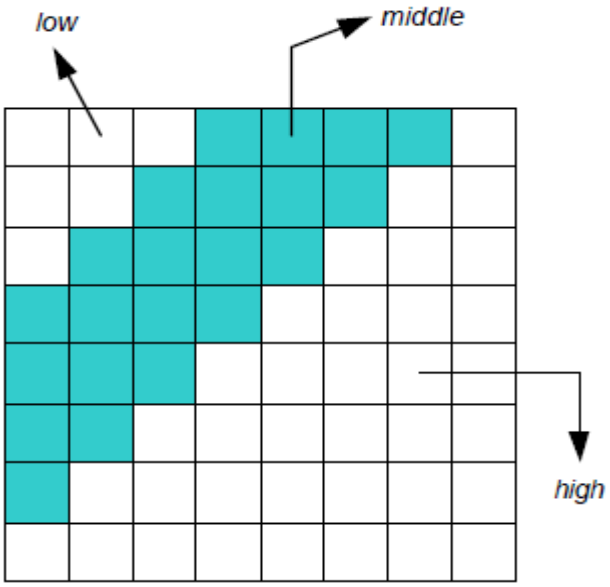
$$ci' = ci\,(1 + \alpha wi) \qquad (6)$$

ci' adalah koefisien *DCT* setelah modifikasi, *ci* koefisien *DCT* sebelum modifikasi, *α* adalah kekuatan penyisipan *watermark* ya*ng* bernilai 0,1 dan *wi* adalah nilai bit *watermark* yang disisipkan.

a. Penyisipan watermark.

Ranah *DCT* membagi citra ke dalam tiga *subband* frekuensi (*low*, *middle*, dan *high*), lihat Gambar 3. Penyisipan pada bagian *low frequency*

dapat merusak citra karena mata manusia lebih peka pada frekuensi yang lebih rendah daripada frekuensi lebih tinggi. Sebaliknya bila *watermark* disisipkan pada bagian *high frequency*, maka *watermark* tersebut dapat terhapus . Oleh karena itu, untuk menyeimbangkan antara *robustness* dan *imperceptibility*, maka *watermark* disisipkan pada bagian *middle frequency.* (Agung, 2007)



Gambar 3. Pembagian tiga kanal frekuensi pada blok 8x8

Berkas *watermark* yang akan disisipkan dinotasikan dengan *W = w1,…,wn. n* merupakan jumlah *bit watermark* yang akan disisipkan. *Bit-bit watermark* tersebut akan disisipkan ke dalam citra (*C = ci,…,cn*) sehingga menghasilkan citra yang mengandung *watermark* (*C' = c'1,…,c'n*). Bit-bit dimasukkan kedalam citra melalui penyusuran tiap blok untuk mencari

daerah-daerah yang memiliki koefiesien menengah sampai seluruh bit tertanam kedalam citra. Dalam proses penyisipannya nilai w_i akan diubah menjadi -1 jika *bit* yang akan disisipkan adalah 0 atau 1 jika *bit* yang disisipkan adalah 1. Selanjutnya algoritma pembangkitan bilangan acak semu dipergunakan untuk membuat deretan bilangan real sebanyak jumlah *bit watermark* yang akan disisipkan. Setiap bilangan real acak yang dibuat akan dikalikan dengan koefisien hasil pengubahan *bit* {-1,1}. Deretan bilangan real acak yang telah dikalikan dengan koefisien pengubahan *bit* {-1,1} akan dijadikan *bit watermark* yang akan disisipkan pada matriks koefisien *DCT* citra asal.

Setelah *bit-bit watermark* tersebut disisipkan ke dalam matriks koefisien *DCT* dari suatu citra digital, maka akan dilakukan invers *DCT* untuk mendapatkan kembali sebuah visualisasi citra yang ber-*watermark.*

b. Pengekstrakan watermark.

Proses pengekstrakan *watermark* dilakukan untuk mengambil kembali (ekstraksi) berkas informasi *watermark* yang terdapat pada sebuah citra yang telah mengandung *watermark.*

Untuk melakukan operasi ekstraksi *watermark,* diperlukan citra uji (ber-*watermark*), citra asal, dan berkas *watermark* asal. Dengan melakukan transformasi *DCT* pada kedua citra, maka dapat diketahui koefisien *DCT* per blok untuk setiap citra.

Perbandingan koesifien *DCT* antara kedua citra tersebut dilakukan untuk dilacak keberadaan *bit-bit watermark* yang telah disisipkan. Perbedaan atau selisih nilai pasti akan terdapat pada sejumlah koefisien jika memang telah terjadi proses penyisipan *watermark* pada citra tersebut. Dalam proses ekstraksi ini, setiap koefisien-koefisien dari citra asal dan citra uji dibandingkan satu per satu hingga menemukan koefisien yang berbeda nilai. Jumlah koefisien yang berbeda atau memiliki selisih nilai menunjukkan jumlah *bit watermark* yang telah disisipkan.Proses perbandingan tersebut akan terus dilakukan hingga koefisien terakhir pada masing-masing citra. Untuk memastikan *watermark* hasil ekstraksi terbentuk dengan baik, dibutuhkan *watermark* yang telah disisipkan. Hal ini diperuntukkan sebagai dasar pembentukan kembali *watermark* dengan ukuran panjang yang pasti.

Salah satu cara untuk melakukan perbandingan *watermark* adalah dengan menghitung *bit error rate* (*BER*), yaitu perbandingan antara *bit* yang salah dengan banyaknya *bit watermark* asli secara keseluruhan. Persamaan *BER* dijabarkan sebagai berikut:

$$BER = \frac{\sum p_i}{N} \times 100\% \quad (7)$$

Dimana pi adalah bit yang salah dan N adalah banyaknya seluruh bit watermark asli. *BER* yang kecil menunjukkan bahwa tingkat kesalahan bit antar gambar yang rendah. Makin rendah nilai *BER* maka semakin mendekati watermark asli. Batas toleransi nilai *BER* adalah 35% (Baldman

2003). Nilai *BER* digunakan sebagai indikator perbedaan antara *watermark* asli dengan *watermark* hasil pengambilan atau ekstraksi.

Menurut analisa studi Persada 2009, tidak mungkin *watermark* ekstraksi memiliki bentuk yang sama persis dengan *watermark* asal. Hal ini disebabkan pada transformasi domain frekuensi dan kompresi citra *JPEG,* terjadi kehilangan informasi karena sifat kompresi *JPEG* yang *lossy* sehingga bit yang dapat kembali maximal 80% dari bit semula.

D. *PSNR* (*Peak Signal to Noise Ratio*)

Untuk mengetahui berapa besar pengaruh nilai hash yang disembunyikan dalam citra, maka perlu dilakukan perbandingan antara kualitas citra asli dengan kualitas citra terwatermark. Proses ini dikenal dengan istilah fidelity.

Pengukuran fidelity dapat diperoleh dengan menghitung nilai *MSE* (Mean Squared Error) dan *PSNR* (Peak Signal to Noise Ratio). Perhitungan nilai MSE dari citra berukuran N x M, dilakukan sesuai dengan rumus berikut:

$$MSE = \frac{1}{3MN} \sum_{i=1}^{3} \sum_{y=1}^{M} \sum_{x=1}^{N} [I\,(x,y) - I'(x,y)]^2 \qquad (8)$$

Pada persamaan (8), *I(x,y)* menyatakan nilai intensitas citra asli di posisi (x,y), sedangkan *I'(x,y)* menyatakan nilai intensitas citra ter-watermark di

posisi (x,y). i adalah indeks matriks (Red = 1, Green = 2, Blue = 3). Nilai *MSE* yang besar, menyatakan bahwa penyimpangan atau selisih antara citra ter-watermark dengan citra aslinya cukup besar. Sedangkan untuk perhitungan nilai *PSNR*, dapat dilakukan dengan rumus berikut (Fajri,2008)

$$PSNR = 10 \log \frac{(255)^2}{MSE} \quad (9)$$

PSNR digunakan untuk mengukur kualitas sinyal terhadap noise. Sinyal disini menyatakan citra asal dan noise menyatakan citra rekonstruksi. Nilai *PSNR* yang diperoleh akan menginformasikan besar atau kecilnya pengaruh nilai hash terhadap citra. Semakin besar nilai *PSNR*(db) maka kualitas citra ter-watermark tersebut akan nampak seperti citra aslinya. Namun bila nilai *PSNR*(db) yang diperoleh kecil, maka citra ter-watermark tersebut akan nampak perubahan pada gambar.

Citra digital dengan nilai *PSNR* tertentu dapat dikategorikan ke dalam 5 kategori sebagai berikut (Munir,2004):

Tabel 5. Kualitas *PSNR* untuk citra dan video

PSNR (dB)	Picture Quality
60	Excellent, no noise apparent
50	Good, a small amount of noise but picture quality good
40	Reasonable, fine grain or snow in the picture, some fine detail lost
30	Poor picture with a great deal of noise
20	Unusable

Sumber: CCTV advisory service (http://www.cctvinformation.co.uk/i/CCTV)

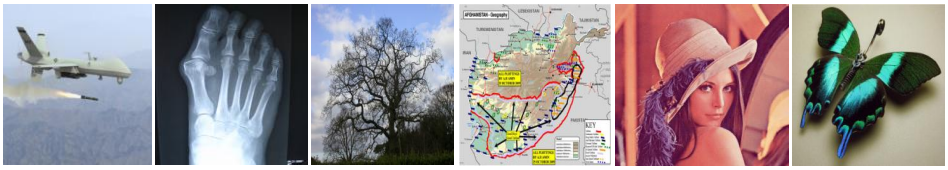
E. KERANGKA PIKIR

Fungsi hash sebagai fungsi satu arah telah banyak digunakan dalam bidang keamanan informasi, begitupun DCT merupakan transformasi yang cukup populer dalam pengolahan citra. Otentikasi citra dengan teknik watermarking adalah suatu cara untuk menyisipkan informasi kedalam citra baik berupa gambar ataupun tulisan sebagai bukti kepemilikan citra. Bila yang disisipkan biasanya berupa logo maka suatu citra akan memiliki keunikan tersendiri jika yang disisipkan berupa kode khusus yang merupakan sidik jari citra itu sendiri.

Gambar 4 berikut menjelaskan secara ringkas kerangka pikir penelitian ini

Rumusan Maslah

a. Bagaimana menghitung nilai hash dari beberapa citra berwarna dan citra gray scale.



b. Bagaimana menyisipkan nilai hash sebagai watermark kedalam masing-masing citra berwarna dan citra grayscale.
c. Bagaimana mengekstrak kembali nilai hash citra pada citra terwatermark.
d. Bagaimana visibilitas nilai hash pada citra terwatermark

Tujuan Penelitian

1. Mengaplikasikan metode Secure Hash Algorithm-384 (SHA-384) dan *Discrete Cosine Transform* (*DCT*) untuk melakukan otentikasi terhadap suatu citra.
2. Menghitung nilai *PSNR* untuk melihat visibilitas nilai hash yang disembunyikan.

Solusi

a. Menghitung nilai HASH dengan metode SHA-384
b. Menyisipkan nilai hash dengan metode *DCT*
c. Mengekstrak nilai hash dengan metode *DCT*
d. Membandingkan bit hash asli yang disisipkan dengan bit hash yang diekstrak

Hasil Penelitian

Nilai Hash dan Citra Terwatermark

Gambar 4. Kerangka pikir penelitian