

Analisis Watermarking Menggunakan Metode Discrete Cosine Transform (DCT) dan Discrete Fourier Transform (DFT)

Mukhammad Solikhin
Faculty of Informatics and
Electrical Engineering, Institut
Teknologi Del, Laguboti,
Indonesia
mukhammad.solikhin@del.ac.id

Yohanssen Pratama*
Faculty of Informatics and
Electrical Engineering, Institut
Teknologi Del, Laguboti,
Indonesia
yohanssen.pratama@del.ac.id

Purnama Pasaribu
Faculty of Informatics and
Electrical Engineering, Institut
Teknologi Del, Laguboti,
Indonesia
if314055@students.del.ac.id

Josua Rumahorbo
Faculty of Informatics and Electrical Engineering,
Institut Teknologi Del, Laguboti, Indonesia
if314039@students.del.ac.id

Bona Simanullang
Faculty of Informatics and Electrical Engineering,
Institut Teknologi Del, Laguboti, Indonesia
if314036@students.del.ac.id

Abstract— Digital image watermarking is the insertion of watermarks into digital image media. Several types of watermarking methods used are Discrete Cosine Transform (DCT) and Discrete Fourier Transform (DFT). Both of these watermarking methods work in the frequency domain (transform). Digital image watermarking using the frequency domain is carried out on the frequency coefficient. This study used 30 digital image data as material for digital image watermarking analysis with 10 data each in binary, grayscale and color digital images in jpg, png and bmp formats. Digital images in the binary and grayscale domains are conversions from digital images in the true color (RGB) domain. Digital image watermarking includes three main processes, namely embedding the watermarked image on the original digital image, extracting the watermarked image and measuring the correlation between the two digital images. Correlation aims to measure two variables that have the same relationship. The technology used in this research work is MATLAB (Matrix Laboratory) as a high-performance programming language for computing in solving problems with solutions expressed in mathematical notation. The results of the discussion prove that the watermarking process in terms of color, for DCT, RGB is better and binary is better for DFT. And the watermarking process, in terms of the type of watermark inserted, for both DCT and DFT, a good watermark is an invisible watermark.

Keywords—image, DCT, DFT, digital, watermark

I. PENDAHULUAN

Perkembangan teknologi menyebabkan manusia ingin meningkatkan efektifitas dan efisiensi gaya hidup. Penerapan teknologi seperti komputer mempunyai peran penting dalam pengolahan data karena memiliki kemampuan komputasi tinggi sehingga data yang diperoleh menjadi sebuah informasi. Salah satu data tersebut dapat berupa citra digital yang mampu diolah untuk mendapatkan informasi yang lebih baik dan efisien. Citra digital adalah sinyal diskrit yang dapat direpresentasikan sebagai fungsi dari variabel – variabel dua dimensi (Stephen Wolfarm, 2002). Perkembangan teknologi digital seperti melakukan akses serta mendistribusikan berbagai informasi berupa format digital telah diterapkan oleh mayoritas manusia dengan menggunakan kamera digital untuk pengambilan citra digital yang sebelumnya menggunakan kamera analog. Ketersediaan informasi citra digital juga dapat berdampak negatif dengan menyalahgunakan citra digital seperti pengambilan hak cipta dan distribusi secara ilegal. Pihak yang tidak bertanggung jawab dapat mengakses citra digital yang fotogenik untuk memperoleh keuntungan dari pihak yang memiliki citra digital tersebut dengan menyebarkan citra digital yang telah dimanipulasi. Hal ini menimbulkan kekhawatiran bagi pihak pencipta atau pemilik. Penanganan masalah dilakukan peneliti dengan menerapkan *watermarking* pada citra digital.

Watermarking adalah penambahan data rahasia (*watermark*) ke dalam sebuah arsip digital (Shieh et al, 2004). Terdapat dua teknik *watermark* yang diterapkan dalam *watermarking* yaitu teknik *watermarking* yang bekerja pada *domain spasial* (*spatial watermark*) dan teknik *watermarking* yang bekerja pada *domain transform* / frekuensi (*spectral watermark*). Teknik *watermarking* pada *domain spasial* lebih mudah proses pembuatannya tetapi *watermark* yang disisipkan pada citra digital asli tidak tahan terhadap manipulasi citra, sedangkan teknik *watermarking* pada *domain transform* tahan terhadap manipulasi citra (Sangadji & Rezeki, 2009). Proses penyisipan *watermark* pada citra digital yang dilakukan oleh peneliti adalah pada *domain transform*. *Domain transform* adalah teknik penyisipan *watermark* yang dilakukan dengan cara melakukan transformasi pada data penampung, kemudian perubahan dilakukan terhadap koefisien transformasinya (Bayu Adi Persada, 2009). Modifikasi pada *domain transform* dari citra digital mempengaruhi keseluruhan *pixel* dalam blok. Dengan begitu, kemungkinan rusaknya *watermark* oleh manipulasi citra akan menjadi lebih baik (Fahmi, 2007). *Watermarking* pada *domain transform* yang digunakan oleh peneliti menggunakan metode *Discrete Cosine Transform* (DCT) dan *Discrete Fourier Transform* (DFT). *Discrete Fourier Transform* (DFT) adalah metode yang menyatakan penjumlahan sinyal sinus dan kosinus dengan amplitudo dan frekuensi yang bervariasi pada citra digital. Sedangkan *Discrete Cosine Transform* (DCT) adalah sebuah fungsi dua arah yang memetakan himpunan N buah bilangan real menjadi N buah bilangan real. Pada Penelitian ini digunakan metode DCT karena kokoh terhadap manipulasi pada *stego-object*. Selain itu, metode DCT juga tahan terhadap kompresi. Sedangkan kelemahan dari metode ini terletak pada kesulitan dalam pengimplementasiannya karena harus melalui langkah-langkah yang panjang sehingga membutuhkan waktu yang lama dalam melakukan penyisipan. Sementara DFT dijadikan metode yang dibandingkan dengan DCT karena memiliki kemiripan dengan DCT dan berada di domain kompleks.

Berdasarkan kenampakan, proses *watermarking* dibedakan menjadi dua yaitu *visible watermarking* dan *invisible watermarking*. *Visible watermarking* adalah *watermark* yang disisipkan pada citra digital dan dapat dilihat oleh indra penglihatan manusia sedangkan *invisible watermarking* dilakukan dengan menyisipkan *watermark* yang tidak dapat dilihat oleh indra penglihatan manusia (Shieh et al, 2004). Pada penelitian ini, peneliti melakukan proses *visible watermarking* dan *invisible watermarking* menggunakan kedua metode yang menentukan proses *watermarking* yang baik.

Watermarking citra digital dikatakan efektif jika memenuhi persyaratan *robustness* dan *imperceptibility* (Zhi-Ming et al, 2003). *Robustness* adalah ketahanan gambar yang telah disisipkan *watermark* terhadap operasi citra atau *attack*. Sedangkan *imperceptibility* adalah penyisipan *watermark* tidak menimbulkan kecurigaan terhadap pengamatan indra penglihatan manusia. Manipulasi citra digital dapat menyebabkan kerusakan bahkan kehilangan informasi dengan beberapa gangguan yang dapat mempengaruhi *watermarking* yaitu *geometric transformation* sebagai kerusakan pada *watermark* yang disebabkan oleh perubahan posisi geometris citra digital yang telah disisipkan *watermark*. Perubahan geometris antara lain *horizontal flip*, *vertical flip*, *rotation*, *crop* dan *compress* (M. Kutter & F.A.P. Pentticolos, 1999). Peneliti melakukan manipulasi pada citra digital yang telah disisipkan *watermark* untuk mengukur ketahanan dari kedua metode DCT dan DFT dengan menggunakan korelasi. Korelasi adalah ukuran dua variabel yang memiliki hubungan yang sama (Jhon & Daris, 2009).

Pada dasarnya citra digital terdiri dari 3 domain yaitu *Red Green Blue* (RGB), keabuan (*grayscale*) dan hitam-putih (*biner*) (Kusuma et al, 2015). Pada penelitian ini peneliti melakukan *watermarking* dengan metode DCT dan DFT menggunakan domain citra digital dengan format *jpg*, *png* dan *bmp*. Penyisipan *watermark* pada *host* dapat mengubah citra asli. Dari kedua metode tersebut, peneliti membandingkan metode yang tidak terlalu

banyak mengubah citra asli (*imperceptibility*) dengan menggunakan korelasi.

II. METODE

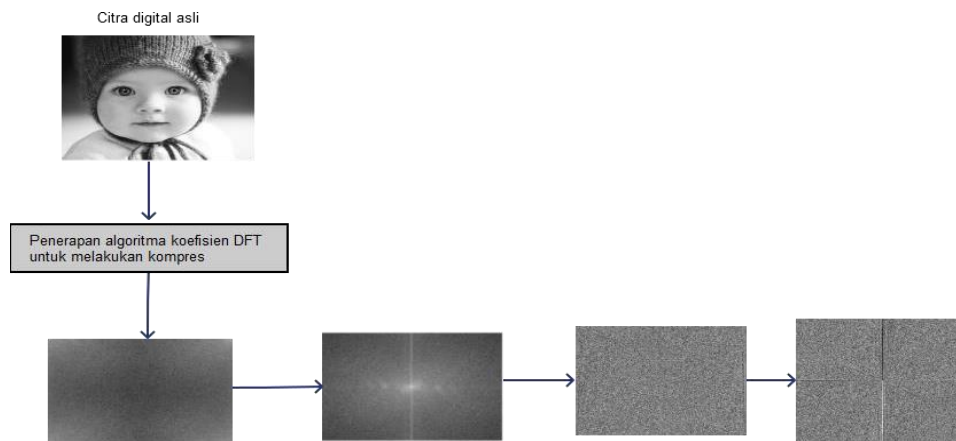
Pada bagian ini diuraikan mengenai metode *watermarking* yaitu *Discrete Cosine Transform* dan *Discrete Fourier Transform*, korelasi yang digunakan untuk menganalisis metode *watermarking*, analisis format citra pada *watermarking* citra digital.

A. Analisis perbandingan metode DCT dan DFT

Transformasi citra ini dilakukan pada ranah frekuensi. Proses *watermarking* dilakukan setelah mengubah citra dari ranah spasial ke ranah frekuensi. Alur proses algoritma DCT dan DFT pada citra digital yang dilakukan adalah :

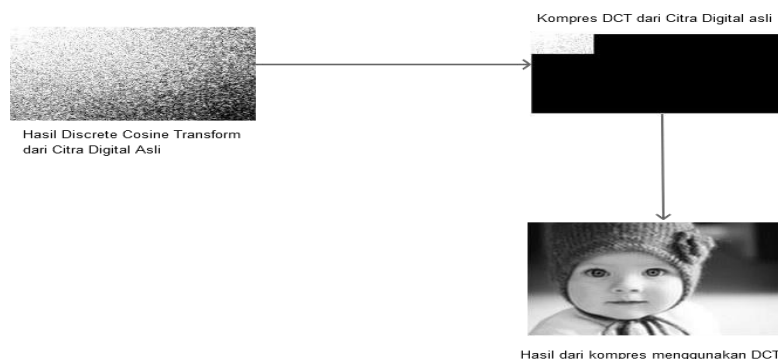
1. Citra asli ditransformasikan dengan metode DCT dan DFT
2. Citra ditransformasikan dengan koefisien frekuensi ke dalam ruang color (RGB)
3. Citra diinvers dengan menggunakan fungsi IDCT dan IDFT

Analisis perbandingan metode *Discrete Cosine Transform* dan *Discrete Fourier Transform* pada citra digital dengan format RGB (Fadilah et al, 2012) dapat dilihat pada gambar 1 berikut :



Gambar 1. Citra digital asli yang diekstrak dengan metode DFT

Proses ekstrak menggunakan algoritma DFT pada citra digital asli dengan koefisien DFT pada pixel citra tersebut. Proses ekstrak dengan metode DCT juga dengan menggunakan koefisien DCT.



Gambar 2. Rekonstruksi dari citra digital yang telah dikompres menggunakan metode DCT

Pada Gambar 2 dapat dilihat proses rekontruksi citra yang telah diekstrak

menggunakan metode DCT dengan invers IDCT untuk mendapatkan citra digital aslinya. Rekontruksi pada metode DFT juga dilakukan seperti pada metode DCT dengan invers IDFT.

B. Analisis citra

Ada beberapa format citra yakni jpg, png, bmp, dan gif. Namun, pada pengerjaan penelitian ini tidak digunakan citra dengan format gif. Hal ini disebabkan karena gif merupakan gabungan beberapa citra dan menampilkannya secara bergantian berdasarkan waktu. Tipe citra gif memungkinkan penambahan warna transparan dan dapat digunakan untuk membuat animasi sederhana, tetapi saat ini standar gif hanya maksimal 256 warna saja. Perbandingan format citra seperti jpg, png, bmp dan gif dapat dilihat pada Tabel 1.

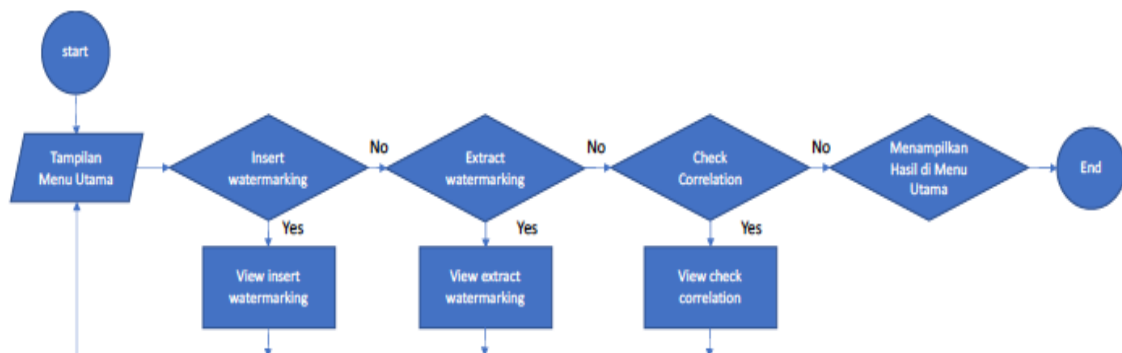
Tabel 1. Perbandingan Format Citra JPG, BMP dan GIF

Tipe	Format Citra			
	JPG	PNG	BMP	GIF
Grayscale	Yes	Yes	Yes	Yes
RGB Color	Yes	Yes	Yes	No
Biner (8 bit color)	Yes	Yes	Yes	No
Animation Option	No	No	No	Yes
Layers	No	No	Yes	Yes

Pada penelitian ini, format citra gif kurang sesuai untuk digunakan dalam proses *watermarking* dengan menggunakan metode DCT dan DFT. Pada format citra ini digunakan domain citra yang sama seperti kriteria citra digitalnya yaitu RGB (*Red Green Blue*), *grayscale* dan *biner*. Pada Tabel 1 dapat dilihat bahwa format citra dalam bentuk gif hanya mendukung kriteria citra *grayscale* dan tipe yang dimiliki oleh format citra gif adalah *animation option* dan *layers*. Citra dengan format jpg dan png juga memiliki kompresi berbasis DCT (*Discrete Cosine Transform*) sedangkan gif memiliki *lossy compression*. Citra dengan format jpg dan png juga memiliki kompresi berbasis DCT (*Discrete Cosine Transform*) sedangkan gif memiliki *lossy compression* (Pramitarini, 2011).

C. Langkah percobaan dan desain eksperimen yang dilakukan

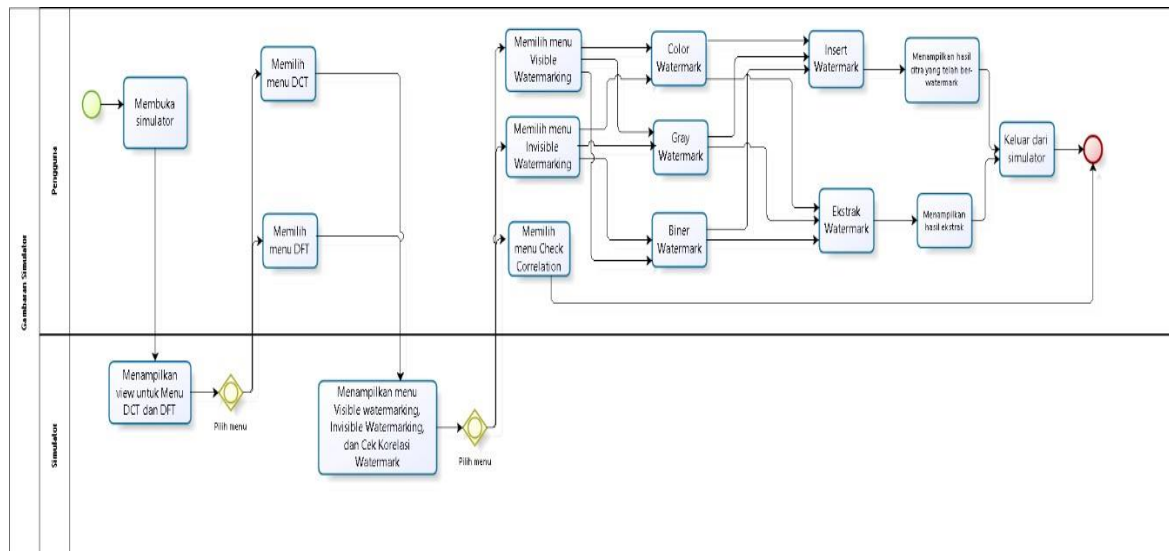
Pada pengumpulan data yang dianalisis diperoleh bahwa *Watermarking* menggunakan metode DCT dan DFT melakukan transformasi kedua algoritma dengan koefisien frekuensi pada domain *red green blue*, *grayscale* dan *biner*. Proses *watermarking* ini menggunakan format citra digital yaitu jpg, png dan bmp. Proses *watermarking* citra digital menerapkan penyisipan *watermark* dan ekstrak *watermark* sesuai dengan analisis perbandingan kompres citra digital menggunakan metode DCT dan DFT. Dari hasil analisis di atas, maka keseluruhan bisnis proses dari pengerjaan penelitian ini digambarkan dalam bentuk *flowchart* seperti yang terdapat pada Gambar 3.



Gambar 3. Flowchart keseluruhan proses

Pada flowchart Gambar 3 diatas, *watermarking* citra digital menggunakan tiga proses utama yaitu *insert watermarking*, *extract watermarking*, dan *check correlation*. *Insert watermarking* menghasilkan citra berwatermark dan dapat dicek koralisnya dengan citra digital asli. Citra ber-watermark juga dapat diekstrak untuk menguji ketahanan *watermark* yang disisipkan pada citra digitak asli dari serangan geometri seperti *rotate*, *flip*, *crop*, dan *compress*. Uji ketahan citra ber-watermark disesuaikan dari pengukuran korelasi.

Untuk mencapai tujuan dari penelitian, maka dilakukan analisis untuk bisnis proses terhadap simulator yang akan dibangun. Adapun bisnis proses yang terdapat pada simulator digambarkan dalam bentuk BPMN (*Business Process Modeling Notation*).



Gambar 4. Bisnis proses pada program

Pada Gambar 4 dijelaskan bahwa kegiatan yang dapat dilakukan pada simulator yaitu *insert watermark*, *extract watermark*, dan cek korelasi. Dimana sebelum kegiatan tersebut dilakukan, ada beberapa hal yang harus dilakukan pengguna yakni :

1. Pengguna harus membuka simulator terlebih dahulu
2. Memilih menu metode DCT atau DFT, tergantung pada pengguna memilih metode apa yang akan digunakan
3. Setelah memilih jenis metode, pengguna memilih menu *watermarking* apa yang akan dilakukan yakni *visible*, *invisible*, atau untuk melakukan pengecekan korelasi
4. Jika pengguna ingin melakukan *watermarking*, pengguna memilih kriteria warna citra *watermark*
5. Setelah itu, pengguna dapat melakukan penyisipan *watermark* terhadap citra atau melakukan pengestrakan citra yang telah ter-*watermark*.

Dalam pengecekan keaslian watermark kami gunakan korelasi yang telah disediakan oleh matlab dengan perintah `corr2(A,B)`

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \bar{A})^2\right) \left(\sum_m \sum_n (B_{mn} - \bar{B})^2\right)}}$$

where $\bar{A} = \text{mean2}(A)$, and $\bar{B} = \text{mean2}(B)$.

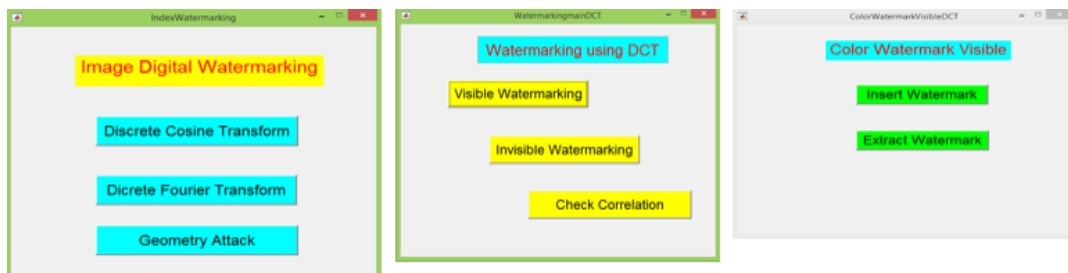
yang artinya menghitung korelasi 2 Dimensi dari matrik 2D yang nilainya antara 0 sampai 1, tetapi bila watermark yang akan kita cek berdimensi 3 atau bertipe RGB $m \times n \times 3$, maka kita harus mengubah citra tersebut menjadi 2D dengan mengganti tipe matrik

rgb2gray (disediakan oleh Matlab juga), langkah-langkah pengecekan adalah masukkan watermark hasil ekstraksi dan masukkan juga watermark uji, setelah itu dilakukan pengecekan apakah ada dari dua gambar tersebut yang bertipe RGB. Jika ada yang bertipe RGB maka ubah komponen matrik ke tiga dari 3 menjadi 1 dengan menggunakan fungsi rgb2gray setelah itu masukkan batas bawah korelasi yang diterima, kemudian hitung korelasi kedua gambar, setelah itu bandingkan jika korelasi yang dihasilkan lebih kecil dari batas yang dimasukkan maka hasil komentar yang keluar adalah watermark uji ditolak, sebaliknya jika korelasi yang dihasilkan lebih dari korelasi yang dibatasi maka hasil yang keluar adalah watermark uji diterima.

III. HASIL DAN PEMBAHASAN

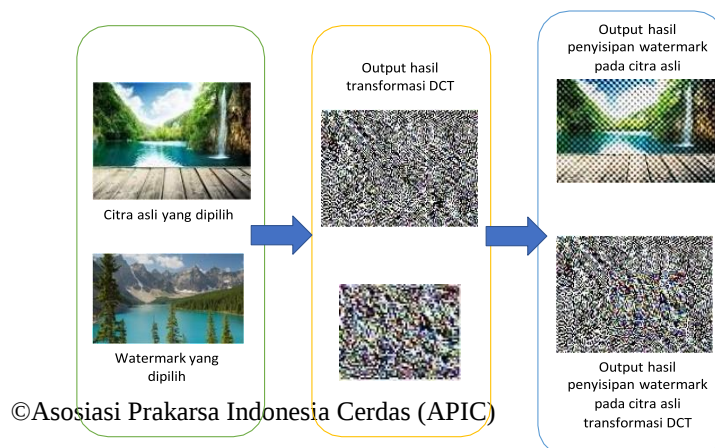
Hasil simulator dibuat dengan menggunakan *mfile* dan beberapa tampilan handle grafik yang merupakan program visual dari MATLAB versi R2015b. *Handle* grafik adalah elemen dari MATLAB untuk menampilkan data dan pembuatan GUI (*Graphics User Interface*). Tampilan awal dari simulator *watermarking* citra digital pada Gambar 5.

Pada tampilan awal program ini, tombol *Discrete Cosine Transform* berfungsi untuk melakukan proses *watermarking* dengan metode DCT, tombol *Discrete Fourier Transform* melakukan proses *watermarking* dengan metode DFT dan tombol *geometry attack* berfungsi untuk memberikan serangan geometri pada citra berwatermark. Proses *watermarking* dengan metode DCT dan DFT menyertakan proses *watermarking* berdasarkan kenampakan yaitu *visible watermarking* dan *invisible watermarking*. *Watermarking* ini menggunakan domain citra *biner*, *grayscale*, dan *color*. Proses utama yang dilakukan pada *watermarking* citra digital dengan metode DCT dan DFT adalah penyisipan citra *watermark* pada citra digital, ekstrak citra berwatermark dan mengukur korelasi. Pengukuran korelasi pada *watermarking* citra digital berwatermark dengan metode DCT dan DFT memiliki fungsi yang sama. Tampilan GUI untuk melakukan fungsi pengukuran korelasi dan untuk melakukan penyisipan citra *watermark* dan ekstrak citra berwatermark pada *watermarking* visible dengan domain citra *color* (RGB) dengan metode DCT dapat dilihat pada Gambar 5.



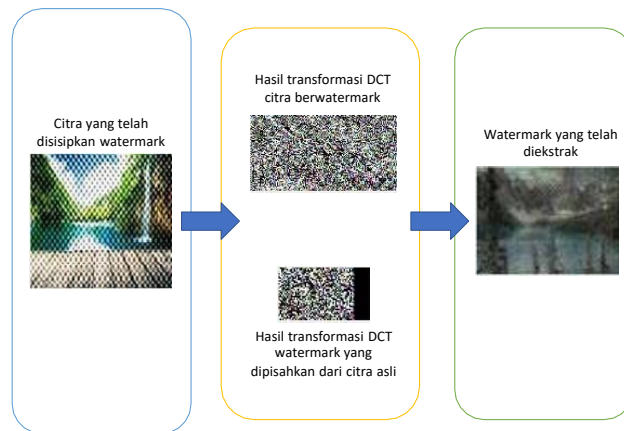
Gambar 5. Tampilan utama watermarking citra digital menggunakan metode DCT dan DFT

Berikut pada gambar 6 adalah proses penyisipan (insert) watermark pada citra digital:



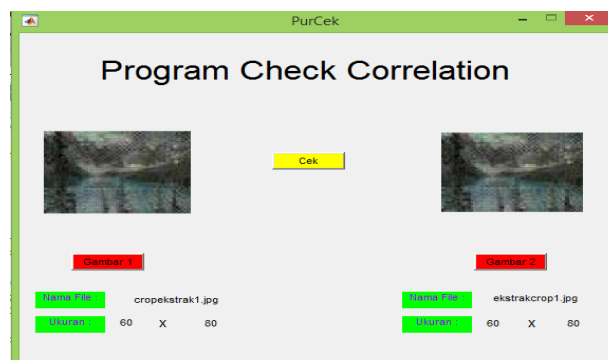
Gambar 6. Hasil penyisipan (insert) watermark pada citra digital

Sementara berikut pada gambar 7 adalah proses extract watermark dari citra digital yang sebelumnya sudah disisipkan oleh watermark:



Gambar 7. Hasil watermark yang telah diekstrak

Pada Gambar 8, tombol *Check Correlation* berfungsi mengukur korelasi yang menentukan ketahanan (*robustness*) *watermark* dan pengaruh dari *watermark* terhadap citra digital asli (*host*) menggunakan metode DCT dan DFT. Tampilan GUI untuk mengukur korelasi antara dua citra sesuai dengan tujuan pada penelitian dapat dilihat pada Gambar 7.



Gambar 8. GUI check correlation

A. Hasil Evaluasi Cek Korelasi

Pada penyelesaian penelitian ini pengecekan dilakukan dalam beberapa analisis, antara lain:

1. Analisis citra asli berupa *Red Green Blue* (RGB), keabuan (*gray scale*) serta hitam-putih (*biner*) dengan citra yang telah disisipi *watermark* menggunakan metode DCT dan DFT
2. Analisis citra asli dengan citra yang telah disisipi *watermark visible* dan *watermark invisible*

Pada evaluasi yang pertama, hasil yang diharapkan ialah mendapatkan sebuah nilai korelasi dari dua citra yang dibandingkan dimana citra yang dibandingkan ialah sebuah citra yang telah disisipi *watermark* menggunakan metode DCT atau DFT dengan citra aslinya yang warnanya berupa *Red Green Blue* (RGB), keabuan (*gray scale*) serta hitam-putih (*biner*). Tujuan dilakukannya evaluasi ini ialah agar mengetahui metode mana antara DCT dan DFT yang tidak banyak mengubah citra aslinya pada citra RGB, *gray scale*, dan biner.

Maka, dari hasil perhitungan korelasi yang diperoleh kedua tabel evaluasi diperoleh hasil perbandingan kedua metode untuk penentuan citra bertipe warna yang tidak banyak

mengubah *watermark* .

Tabel 2. Hasil perbandingan metode DCT dan DFT

Jenis warna	Jenis Metode	
	DCT	DFT
RGB	0,85624755	0,892653
Gray scale	0,850414	0,847622
Biner	0,8497925	0,841789

Pada Tabel 2 diperoleh hasil perhitungan rata-rata dari setiap metode berdasarkan tipe warna gambar. Dari Tabel 2 diperoleh hasil evaluasi bahwa :

1. Untuk DCT, gambar bertipe RGB yang paling baik untuk melakukan *watermarking*
2. Untuk DFT gambar bertipe biner yang paling baik untuk melakukan *watermarking*

Pada evaluasi yang kedua, hasil yang diharapkan ialah mendapatkan sebuah nilai rata-rata dari nilai korelasi perbandingan yang dilakukan pada evaluasi pertama pada *watermark* yang *visible* atau *watermark* yang *invisible*. Tujuan dilakukannya evaluasi kedua ini ialah agar mengetahui jenis *watermark* manakah yang paling kuat dengan melihat rata-rata nilai korelasi yang paling tinggi.

Berdasarkan perhitungan yang dilakukan pada hasil evaluasi korelasi pada evaluasi pertama, maka diperoleh rata-rata berikut :

Tabel 3. Hasil perbandingan watermark visible dan invisible

Jenis watermark	Rata-rata DCT	Rata-rata DFT
Watermark yang visible	0,731188667	0,841752
Watermark yang invisible	0,973114033	0,879624

Berdasarkan Tabel 3 dapat ditarik kesimpulan bahwa untuk metode DCT maupun DFT, jenis *watermark* yang lebih bagus untuk teknik penyisipan ialah *watermark* yang *invisible*.

B. Hasil evaluasi cek ketahanan Watermark

Pada subbab ini akan dijelaskan hasil evaluasi dari ketahanan metode terhadap serangan. Ketahanan metode terhadap serangan yang dimaksud ialah menguji ketahanan suatu citra yang telah disisipi *watermark* menggunakan masing-masing metode lalu terkena serangan yang sama lalu di-ekstrak yang kemudian dicek korelasi dari kedua *watermark* hasil ekstrak dari kedua metode tersebut. Hasil yang diharapkan ialah mendapatkan sebuah nilai korelasi dari kedua *watermark* yang dibandingkan. Tujuan dilakukannya evaluasi ini ialah agar mengetahui metode mana antara DCT dan DFT yang paling tahan terhadap serangan geometri.

Berdasarkan proses perhitungan korelasi antara citra RGB yang telah disisipi *watermark* menggunakan metode DCT kemudian diberikan serangan geometri dengan *watermark* yang disisipkan, maka diperoleh data korelasi untuk serangan *compress* pada Tabel 4.

Tabel 4. Data korelasi untuk serangan Compress pada DCT untuk citra RGB

Tipe Gambar	Nama Gambar	Jenis Watermark	
		Visible	Invisible
JPG	gambar1.jpg	0.88943	0.72171
	gambar2.jpg	0.92759	0.68897
	gambar3.jpg	0.92989	0.68408
PNG	gambar4.png	0.99649	0.81866
	gambar5.png	0.97308	0.85248
	gambar6.png	0.98059	0.87456
BMP	gambar7.bmp	0.969	0.8274
	gambar8.bmp	0.96983	0.84866
	gambar9.bmp	0.96405	0.85626
	gambar10.bmp	0.95965	0.86959
Rata-rata		0,95596	0,804237

Sementara berdasarkan proses perhitungan korelasi antara citra RGB yang telah disisipi *watermark* menggunakan metode DFT kemudian diberikan serangan geometri dengan *watermark* yang disisipkan, maka diperoleh data korelasi untuk serangan *compress* pada Tabel 5.

Tabel 5. Data korelasi untuk serangan Compress pada DFT untuk citra RGB

Tipe Gambar	Nama Gambar	Jenis Watermark	
		Visible	Invisible
JPG	gambar1.jpg	0,99367	0,99405
	gambar2.jpg	0,98513	0,98156
	gambar3.jpg	0,98632	0,98632
PNG	gambar4.png	1	1
	gambar5.png	1	1
	gambar6.png	1	1
BMP	gambar7.bmp	1	1
	gambar8.bmp	1	1
	gambar9.bmp	1	1
	gambar10.bmp	1	1
Rata-rata		0,996512	0,996193

Maka, berdasarkan hasil perhitungan rata-rata yang diperoleh, maka dilampirkan hasil perbandingan kedua metode terhadap serangan geometri.

Tabel 6. Hasil perbandingan kedua metode terhadap serangan geometri

Domain Gambar	Jenis Serangan	DCT		DFT	
		Visible	Invisible	Visible	Invisible
RGB	Compress	0,95596	0,804237	0,996512	0,996193
	Flip	1	1	1	1
	Rotate	0,4750079	0,3901249	NaN	NaN
	Crop	1	1	1	1
Grayscale	Compress	0,948417	0,77808	0,998861	0,997514
	Flip	1	1	1	1
	Rotate	0,389792333	0,3829473	NaN	NaN
	Crop	1	1	1	1
Biner	Compress	0,998349	0,624138	0,995926	0,996985
	Flip	1	1	1	1
	Rotate	0,3540229	0,3350077	NaN	NaN
	Crop	1	1	1	1

Berdasarkan Tabel 6 diperoleh hasil evaluasi berikut :

1. Untuk gambar bertipe RGB, metode yang tahan terhadap serangan *compress* ialah metode DFT
2. Untuk gambar bertipe Grayscale, metode yang tahan terhadap serangan *compress* ialah metode DFT
3. Untuk gambar bertipe Biner, metode yang tahan terhadap serangan *compress* ialah metode DFT
4. Untuk ketiga domain gambar, metode DCT dan DFT sama-sama tahan terhadap serangan *flip* dan *crop*
5. Untuk ketiga domain gambar, metode DCT dan DFT tidak dapat dibandingkan untuk mengetahui metode mana yang tahan terhadap serangan *rotate* dikarenakan DFT tidak mendukung untuk ekstrak setelah diberi serangan *rotate* pada citra ber watermark.
6. Untuk hasil pencarian nilai korelasi dari serangan *rotate* pada DFT menghasilkan NaN. Hal ini dikarenakan *rotate* tidak dapat dilakukan pada metode DFT karena setelah citra digital yang telah disisipkan watermark diberi serangan *rotate* dan kemudian dilakukan ekstraksi, maka hasil yang keluar adalah citra yang hitam. Sehingga jika dihitung nilai korelasinya maka yang keluar adalah NaN.

C. Pembahasan Hasil Evaluasi

Berikut adalah hasil evaluasi dari hasil yang didapatkan pada penelitian ini:

- **Pembahasan hasil evaluasi korelasi citra asli dengan citra yang disisipi watermark**

Untuk melakukan pengecekan korelasi antara 2 citra yakni korelasi citra yang telah disisipi *watermark* dengan citra asli maka digunakan program DCT dan DFT yang telah dibuat dengan mengimplementasikan kedua algoritma pada bahasa pemrograman Matlab. Evaluasi korelasi yang dilakukan yakni membandingkan korelasi citra asli berupa *RGB*, *gray scale* serta *biner* dan citra yang telah disisipkan dengan *watermark* menggunakan metode DCT dan DFT. Untuk mendapatkan nilai korelasi seperti yang telah dilampirkan pada subbab hasil evaluasi, maka dibutuhkan beberapa sampel citra asli dan juga sampel citra yang akan disisipkan pada citra asli. Dan juga citra tersebut terdiri dari 3 jenis warna yakni *RGB*, *gray scale* dan juga *biner* sehingga dapat dianalisis untuk mendapatkan hasil analisis seperti pada tabel 6. Proses yang pertama kali dilakukan sebelum melakukan

pengecekan korelasi ialah proses *watermarking* menggunakan metode DCT dan DFT. Setelah citra yang telah disisipi *watermark* terbentuk maka citra tersebut siap di-cek korelasinya dengan citra aslinya. Kemudian nilai korelasi dari setiap perbandingan dirata-ratakan berdasarkan tiap jenis warna citra asli untuk setiap jenis *watermark*-nya juga per metode. Setelah nilai rata-rata didapat, maka dibandingkan dengan rata-rata yang dimiliki DCT dengan rata-rata yang dimiliki DFT. Dari hasil perbandingan tersebut maka dapat ditarik kesimpulan metode mana yang tidak banyak mempengaruhi citra asli. Sedangkan untuk analisis citra asli dengan citra yang telah disisipi *watermark* yang *visible* atau *invisible* digunakan hasil analisa yang telah dilakukan yakni analisa korelasi citra asli

RGB, *gray scale* serta hitam-putih (*biner*) dan citra yang telah disisipkan dengan *watermark* menggunakan metode DCT dan DFT (*imperceptibility*). Setelah data hasil perhitungan korelasi tersebut terkumpul, maka langkah selanjutnya ialah menjumlahkan semua nilai korelasi yang dimiliki oleh *watermark invisible* dengan semua jenis warna lalu dihitung rata-ratanya begitu juga dengan *watermark invisible*. Setelah rata-rata kedua *watermark* didapat maka dapat ditarik kesimpulannya *watermark* mana yang paling kuat.

- **Pembahasan hasil evaluasi pengujian ketahanan watermark**

Evaluasi yang dilakukan ialah menguji ketahanan suatu *watermark* hasil ekstrak dari suatu citra yang telah disisipi *watermark* menggunakan kedua metode setelah citra yang tersisipi *watermark* tersebut terkena serangan geometrik seperti *crop*, *flip*, *rotate* dan *compress*. Hasil pengujian dari evaluasi ini berupa angka yakni nilai korelasi dari perbandingan *watermark* dengan *watermark* hasil ekstrak yang sebelumnya telah diberi serangan geometrik. Proses yang pertama kali dilakukan sebelum melakukan pengecekan korelasi ialah proses *watermarking* menggunakan metode DCT dan DFT, lalu citra yang telah disisipi *watermark* tersebut diberi serangan geometrik kemudian citra tersebut diekstrak sehingga keluarlah sebuah citra *watermark*. Setelah proses ini selesai maka pengecekan antara *watermark* yang disisipkan dengan *watermark* hasil ekstrak dapat dilakukan. Nilai korelasi dari *watermark* hasil ekstrak dari setiap metode dengan serangan yang sama dicatat sehingga dapat dibandingkan antara kedua metode. Sehingga hasil akhir dari analisis ini dapat ditarik kesimpulan metode mana yang paling tahan dengan suatu serangan tertentu. Citra digital yang telah disisipkan *watermark* akan diberikan serangan geometri seperti *cropping*, *flip*, *rotate* dan *compress*. Pengujian ketahanan pada serangan geometri dilakukan dengan ekstrak citra ber-*watermark* yang telah diberi serangan. Proses ekstrak yang telah dilakukan membuktikan bahwa DFT serangan geometri *crop*, *flip* dan *compress* dapat dilakukan, sedangkan serangan geometri *rotate* tidak didukung karena hasil ekstrak tidak baik sehingga tidak dapat dicari korelasinya.

IV. KESIMPULAN

Pada proses penyisipan *watermarking* dilihat dari jenis domain gambar, diperoleh kesimpulan bahwa untuk metode DCT gambar bertipe RGB yang paling baik untuk melakukan *watermarking*, sementara untuk metode DFT gambar bertipe Biner yang paling baik untuk melakukan *watermarking*. Selain itu pada proses penyisipan *watermarking* apabila dilihat dari jenis *watermark* yang disisipkan, maka diperoleh kesimpulan bahwa jenis *watermark* yang *invisible* yang lebih baik untuk metode DCT dan DFT. Sementara pada pengujian ketahanan metode terhadap serangan geometri dapat disimpulkan bahwa untuk gambar bertipe RGB, metode yang tahan terhadap serangan *compress* ialah metode DFT, untuk gambar bertipe *grayscale*, metode yang tahan terhadap serangan *compress* ialah metode DFT, untuk gambar bertipe *biner*, metode yang tahan terhadap serangan *compress* ialah metode DFT, dan untuk ketiga domain gambar, metode DCT dan DFT sama-sama tahan terhadap serangan *flip* dan *crop*

UCAPAN TERIMAKASIH

©Asosiasi Prakarsa Indonesia Cerdas (APIC)

Terimakasih kepada Institut Teknologi Del yang telah memfasilitasi dan memberikan dukungan sehingga penelitian ini dapat terlaksana dengan baik.

REFERENSI

- [1] Dhiman , S., & Singh, O. (2016). *Analysis of Visible and Invisible Image Watermarking. International Journal of Computer Applications.*
- [2] Digidoyo, P., Gonydjaja, R., & Mutiara, R. R. (2005). *Penyisipan Watermark Pada Citra Grayscale Berbasis SVD.* Jakarta : Universitas Gunadarma
- [3] Dwiandiyanta, B. Y. (2011). *Perbandingan Watermarking Citra dengan Alihragam Wavelet dan Discrete Cosine Transform.* Buana Informatika.
- [4] Emami, M. S. (2014). *Spatial Domain Approaches for Real-Time Ownership Identification.*Malasya : *Journal of advances in infomation technology*, 1-2.
- [5] Fadilah, U., Sawitri, R. D., Suprijono, H., & Wulandari, S. A. (2012). *Perbandingan Kinerja Sistem Kompresi Pada Citra Digital Retinopathy Berbasis Tansformasi DFT Dan DCT .*Semarang : Universitas Dian Nuswantoro
- [6] Fahmi.(2007).*Studi dan Implementasi Watermarking Citra Digital dengan Menggunakan Fungsi Hash.*Indonesia : Institut Teknologi Bandung.
- [7] Gilani, S. M., & Skodras, A. N. (2000). *DLT Based Digital Image Watermarking.*
- [8] Hakim, A. R. (2012, Juni). *Analisa Perbandingan Watermarking Image Mengguakan Discrete Wavelet Transform.* Jakarta : Universitas Indonesia, pp. 14-16.
- [9] Harahap, H., Budiman, G., & Novamizanti, L. (2016). Implementasi Teknik Watermarking menggunakan FFT dan Spread Spectrum Watermarkpada Data Audio Digital. *elkomika.*
- [10] Hopnner, K. (2005). *Strategies for including graphics in LATEX document.* TUGboat, 3.
- [11] Hartung, F., & Kutter, M. (1999). *Multimedia Watermarking Techniques.* IEEE.
- [12] Hidayat, E. Y., & Adnan, F. N. (2013, Juni 23). *Hybrid DWT-DCT Watermarking Citra Digital Menggunakan Metode Comparison Based Correlation Embedding.* *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2012*, p. 2.
- [13] Irianto, S. Y. (2013). *Analisis Citra Digital Dan Content Based Image Retrieval.*
- [14] Jhon, & Daris. (2009). *Understanding Correlation.* U.S.
- [15] Joshi, Amit, Vivekanand Mishra, dan R.M.Patrikar.2012.*Real Time Implementation of Watermarking.*
- [16] Kusuma, A. A., Iwut, I., & Fauzi, H. (2015). *Analisis Korelasi Kemerahan Warna Citra Kelopak Mata Dalam Bagian Bawah Dengan Hemoglobin Darah.*
- [17] Kusumanto , R., & Tompunu , A. N. (2011). *Pengolahan Citra Digital Untuk Mendeteksi Obyek Menggunakan Pengolahan Warna Model Normalisasi RGB.*
- [18] Ming Zhing, L. Rong-Yan, & W. Lei.2003. *Adaptive Watermark Scheme with RBF Neural Networks.* International Conference on Neural Networks and Signal Processing.
- [19] Kutter, M. & F. A. P. Petitcolas. 1999. *A fair benchmark for image watermarking systems* *Electronic Imaging '99. Security and Watermarking of Multimedia Contents*, vol. 3657, The International Society for Optical Engineering, Sans Jose, CA, USA
- [20] Munir, Rinaldi.2010.*Image Watermarking untuk Citra Berwarna dengan Metode Berbasis Korelasi dalam Ranah DCT.*Indonesia.Institut Teknologi Bandung.
- [21] Noviardi, W. (2008, Mei 21-23). *Penyisipan Logo Berbasis Discrete Cosine Transform.*
- [22] Oktaviani, R. (2013). *Operasi Dasar Pengolahan Citra Digital.* Jakarta: Komunitas eLearning Ilmu Komputer.
- [23] Persada, Bayu Adi.2009.*Perbandingan Teknik Penyembunyian Data Dalam Domain Spasial dan Domain Frekuensi pada Image Watermarking.*Bandung.Institut

Teknologi Bandung.

- [24] Prabhishek , S., & Chadha, R. S. (2013). A Survey of Digital Watermarking Techniques, Applications and Attacks. *IJEIT*.
- [25] Pramitarini, Yushintia.2011. Analysis of Delivery Compressed JPEG Image Direct Sequence Spread Spectrum (DS-SS) Technique.Surabaya : Department of Telecommunications PENS ITS
- [26] Sangadji, I. M., & Rezeki, R. (2009). *Pengukuran Kualitas Citra Terwatermarking*. Jakarta : *Jurnal Petir* Vol. 2 , 47.
- [27] Saputra, Y., & Pratiwi, A. (2011). *Analisis Perbandingan Kinerja Komputer Metode Fast Fourier Transform (FFT) dan Metode Discrete Cosine Transform untuk Kompresi Citra Pada Aplikasi Kompresi Data*.
- [28] Shieh, C. S., Huang, H. C., Wang, F. H., & Pan, J. S. (2004). *An Embedding Algorithm for Mutiple Watermarks*. *Journal of Information Science and Engineering*.
- [29] Sofwan, M., & Gunawan, D. (2013). *Analisa Watermarking Menggunakan Transformasi Laguerre*.
- [30] Tjiharjadi, S., & Sanwill. (2006). *Watermarking Citra Digital Menggunakan Teknik Amplitude Modulation*. *Jurnal Informatika*.

- [31] Tyas, L. A. (2011). *Watermarking Citra Digital Berbasis DWT-SVD dengan Detektor Non-Blind*. 2.
- [32] Ulfah, R. M. (2008). *Analisis Variabel Pembentuk Kepuasan Konsumen Pada Ritel Hipermarket di Depok*.
- [33] Wolfram, Stephen. (2002). *A New JPEG Image Watermarking Algorithm Based On Cellular Automata*. California