PROPOSAL

PENELITIAN DISERTASI DOKTOR
TAHUN KE-2

JUDUL PENELITIAN

EKSTRAKSI FITUR CITRA BERBASIS DCT DENGAN SKEMA PENYEMBUNYIAN INFORMASI UNTUK PERLINDUNGAN DAN PEMULIHAN KERUSAKAN DOKUMEN DIGITAL

Tim Peneliti:

Dr. Ir. Suwadi, M.T. (Departemen Teknik Elektro/FTE/ITS)
Dr. Ir. Wirawan, DEA (Departemen Teknik Elektro/FTE/ITS)
Lusia Rakhmawati (Mahasiswa S3 Teknik Elektro/FTE/ITS)

LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT
INSTITUT TEKNOLOGI SEPULUH NOPEMBER
SURABAYA 2020

Ringkasan penelitian tidak lebih dari 500 kata yang berisi latar belakang penelitian, tujuan dan tahapan metode penelitian, luaran yang ditargetkan, serta uraian TKT penelitian yang diusulkan.

RINGKASAN

Sejak satu dekade terakhir, dengan adanya internet terjadi pertumbuhan yang pesat terhadap penggunaan data multimedia. Digitalisasi informasi memberikan manfaat yang besar dalam penurunan kapasitas penyimpanan dan untuk memudahkan transfer informasi melalui Internet. Namun, hal itu menyebabkan beberapa masalah serius, seperti pelanggaran hak cipta, masalah autentikasi dan perubahan konten itu sendiri. Perlindungan intelektual hak milik merupakan isu penting untuk memastikan integritas dan kepemilikan citra yang diterima. Untuk mengimbangi kesalahan kanal dan memperbaiki citra yang dirusak, banyak metode deteksi kerusakan dan pemulihan citra telah diusulkan. Penelitian ini menggunakan teknik penyembunyian informasi atau *watermarking* dengan memanfaatkan beberapa informasi penting yang diperoleh dari citra itu sendiri yang dipilih sebagai *watermark* dan kemudian dapat diperoleh kembali pada dekoder untuk menutupi bagian yang rusak. Ekstraksi fitur adalah elemen penting dalam desain pemulihan citra dan algoritma watermarking dan kualitasnya dapat memiliki pengaruh besar pada hasil kinerja teknik penyembunyian informasi. Tujuan yang ingin diungkap dalam penelitian ini adalah untuk mengembangkan metodologi yang efektif untuk ekstraksi fitur dalam domain Discrete Cosine Transform (DCT) dan menerapkannya dalam desain citra adaptif self-recovery dan algoritma citra watermarking. Metodologinya adalah menggunakan koefisien DCT yang paling signifikan yang bisa ada rentang frekuensi untuk mendeteksi dan mengklasifikasikan pola tingkat abu-abu. Dengan cara ini, variasi tingkat abu-abu dengan rentang frekuensi spasial yang lebih luas dapat dilihat tanpa peningkatan kompleksitas komputasi dan diharapkan mampu membedakan pola tingkat abu-abu untuk orientasi tepi sederhana seperti pada kebanyakan metode berbasis DCT yang ada. Hasil dari penelitian ini diharapkan mampu memberikan kontribusi untuk perlindungan intelektual hak milik yang dapat memastikan integritas dan kepemilikan dokumen digital yang diterima. Tingkat kesiapan teknologi yang diusulkan adalah tingkat 5

Kata kunci maksimal 5 kata

Discrete Cosine Transform (DCT)*, authentication and tampering localization, Digital watermarking*

Latar belakang penelitian tidak lebih dari 500 kata yang berisi latar belakang dan permasalahan yang akan diteliti, tujuan khusus, dan urgensi penelitian. Pada bagian ini perlu dijelaskan uraian tentang spesifikasi khusus terkait dengan skema.

LATAR BELAKANG

Saat ini penggunaan data multimedia digital meningkat tajam karena kemudahan dalam proses produksi, penyimpanan, pengelolaan, dan pendistribusiannya. Dengan kemudahan tersebut tidak menutup kemungkinan disalahgunakan oleh pihak yang tidak bertanggungjawab untuk mengubah isi dari informasi digital yang kemudian menyebarkannya demi tujuan yang negatif. Selanjutnya, dengan digitalisasi informasi memberikan manfaat yang besar dalam penurunan kapasitas penyimpanan dan memudahkan transfer informasi melalui Internet. Namun, hal itu menyebabkan beberapa masalah serius, seperti pelanggaran hak cipta, masalah otentikasi

dan perubahan konten itu sendiri {(Shoaib & Mahajan, 2015); (Vyas dkk, 2014); (Wang dkk, 2010)}. Oleh karena itu, kebutuhan autentikasi multimedia digital menjadi isu penting untuk melindungi dari penyalahgunaan orang yang tidak tepat serta memastikan integritas dan kepemilikan citra yang diterima (Thongkor dan Amornraksa, 2012).

Integritas dan keaslian citra digital dapat dijamin dengan menggunakan teknik peneyembunyian informasi atau *watermarking* {(Dhole & Patil, 2015); (Han dkk, 2013)}. Teknik *watermarking* bertujuan menyisipkan tanda digital (disebut sebagai *watermark*) ke dalam media asal (disebut *host*). *Watermark* merupakan *string* data yang bisa terlihat (*perceptible*) atau tidak terlihat (*imperceptible*) (Cao dkk, 2017). *Watermark* yang tidak terlihat adalah informasi yang tersembunyi dalam citra dapat berupa logo perusahaan, pesan yang menunjukkan kepemilikan citra, bagian dari citra *host*, dan bahkan salinan penuh dari citra *host* itu sendiri {(Vyas dkk, 2014); (Hsu & Tu, 2011)}. Hal ini nantinya dapat diekstraksi dengan menggunakan skema pra-desain ekstraksi untuk berbagai tujuan, termasuk verifikasi integritas konten, otentikasi kepemilikan, pesan rahasia dan sebagainya. Kelemahan teknik yang dikembangkan di (Chen & Lu, 2012), fokus pada deteksi apakah gambar dirusak atau tidak, tidak jelas menentukan lokasi dan jumlah informasi yang dirusak.

Teknik *fragile* dan *semi-fragile watermarking* merupakan metode yang banyak digunakan untuk proses autentikasi. Teknik *fragile watermarking* bertujuan mendapatkan autentikasi yang akurat, sehingga bila terdapat kerusakan, teknik ini mampu mendeteksi dan melokalisasi modifikasi sekecil apapun. Sedangkan teknik semi-fragile watermarking bertujuan membatasi modifikasi konten penting dan mendeteksi perubahan konten yang tidak sesuai. Pemakaian kedua jenis watermarking tersebut saat ini diarahkan bukan hanya mendeteksi dan melokalisasi perubahan konten, namun juga dapat memulihkan konten yang mengalami kerusakan {(Chen dkk, 2012); (Qin, 2012)}. Metode ini tidak hanya mendeteksi dan mencari modifikasi dalam citra, tetapi juga memulihkan daerah yang diubah tersebut dengan informasi yang tersembunyi dalam citra. *Watermark* tidak lagi sebuah logo atau sepotong pesan, melainkan citra itu sendiri {(Zhang dkk, 2011); (Shruthy & Varghese, 2015); (Singh, 2016); (Cao dkk, 2017)}. Citra asal biasanya dikurangi menjadi ukuran yang sesuai yang disebut sebagai fitur citra, yang masih berisi informasi yang cukup untuk mewakili data citra asli. Fitur citra ini kemudian tertanam ke dalam citra asli melalui berbagai teknik untuk membentuk citra yang ter-*watermark*. Kualitas citra ter-*watermark* biasanya cukup tinggi, citra ini yang kemudian

dipublikasikan di internet sebagai pengganti citra asli. Dalam kasus ini, bilamana citra ter-*watermark* rusak, maka fitur citra yang disisipkan tersebut dapat diekstraksi untuk merekonstruksi citra.

Kebanyakan metode pemulihan citra yang ada memanfaatkan properti kehalusan dari citra, dimana intensitas dari satu piksel ke piksel terdekatnya bervariasi secara halus. Metode tersebut fokus pada blok-blok bersebelahan yang valid secara spasial atau temporal untuk menutupi kerusakan {(Vyas dkk, 2014); (Hsu & Tu, 2011)}. Karena beberapa bagian dari citra dapat memiliki variasi intensitas yang tinggi, maka metode tersebut tidak selalu bekerja cukup baik bila dilihat dari kualitas citra untuk blok-blok yang komplek (Chetan & Shivananda, 2014). Metode yang ada untuk deteksi kerusakan dan perbaikan citra memerlukan banyak data yang disisipkan kedalam citra asli untuk kepentingan autentikasi dan perbaikan citra. Hal ini secara signifikan mengurangi kualitas persepsi dari citra terwatermark. Selanjutnya lokalisasi proses deteksi kerusakan dan pemulihan tidak efisien (Hemida dkk, 2017). Metode yang ada juga tidak memvalidasi deteksi kerusakan dan pemulihan terhadap beberapa serangan penyisipan, penghapusan dan penggantian data digital

Tinjauan pustaka tidak lebih dari 1000 kata dengan mengemukakan *state of the art dan* peta jalan (*road map*) dalam bidang yang diteliti. Bagan dan *road map* dibuat dalam bentuk JPG/PNG yang kemudian disisipkan dalam isian ini. Sumber pustaka/referensi primer yang relevan dan dengan mengutamakan hasil penelitian pada jurnal ilmiah dan/atau paten yang terkini. Disarankan penggunaan sumber pustaka 10 tahun terakhir.

TINJAUAN PUSTAKA

Berdasarkan penelusuran literatur untuk tahap pengembangan yang pertama, penelitian ini mengadopsi teknik *self-embedding watermarking*, dimana beberapa informasi fitur yang signifikan diekstrak dari citra asli dan disisipkan kembali ke dalam citra itu sendiri. Kemudian, citra asli dengan data yang disisipkan dikodekan dan ditransmisikan. Pada dekoder, data yang disisipkan di rekonstruksi dan citra asli di dapatkan kembali berdasarkan rekonstruksi data yang disisipkan bersamaan dengan metode *post-processing*. Karena beberapa informasi dari data yang hilang disisipkan ke dalam paket yang diterima, kemungkinan bahwa pemulihan kerusakan dapat dilakukan lebih baik dengan bantuan data yang disisipkan tersebut. Sepanjang algoritma *watermarking* didesain dan data yang akan disisipkan dipilih secara hati-hati, akan menjadi metode yang potensial untuk meningkatkan performansi pemulihan citra digital yang ditransmisikan melalui jaringan *error-prone*.

Adapun kinerja skema *self-embedding* pada umumnya diberikan dalam hal kualitas citra terwatermark dan pemulihan kondisi setelah mengalami kerusakan. Kualitas citra yang dipulihkan dapat dievaluasi melalui nilai PSNR dan kondisi restorasi bergantung kepada tingkat gangguan (yaitu jumlah modifikasi). Kualitas citra yang pulih ini dan tingkat gangguan sangat terkait satu sama lain, dan pertukaran antara keduanya perlu diseimbangkan dengan benar. Karena ini *trade-off*, tidak ada model umum untuk masalah pemulihan konten meskipun adanya berbagai skema yang mampu memulihkan konten yang dirusak (Chamlawi, 2009) (Wang dkk, 2010) (Eswaraiah & Reddy, 2014). Secara umum permasalahan skema *self-embedding fragile watermarking* yang ada dapat dikelompokkan sebagai berikut:

a. Pemetaan blok yang tidak aman

Dalam skema *self-embeding watermarking* pemetaan blok diperlukan untuk proses penyisipan watermark sebagai sebuah paylod pada blok tersebut. Terdapat beberapa metode pemetaan blok, kebanyakan menggunakan transformasi linier: transformasi 2-D (Zhang & Wang, 2008), (Li dkk, 2011), dan transformasi linear 1-D (Zhang dkk, 2017), (Bravo-Solorio & Nandi, 2011), (Lin dkk, 2004) dan transformasi Arnold (Chow, 2017). Namun, karena terbatasnya jumlah derajat kebebasan, transformasi linear mudah didapat dari hanya beberapa citra sampel, dan lemah dari sudut pandang keamanan (Shruthy & Varghese, 2015), (Lin dkk, 2006). Untuk mengatasi masalah ini, pada penelitian ini penggunaan transformasi linier bisa dilakukan dengan pemilihan kunci yang menggunakan bilangan prima.

b. Modifikasi yang tidak terdeteksi

Karena keterbatasan pada kemampuan penyisipan *watermark*, fitur dari blok citra umumnya terdiri dari koefisien transformasi terkuantisasi, misalnya koefisien koordinat orde tinggi yang dikuantifikasi tinggi (Yu dkk, 2014) atau diambil dari modulo intensitas rata-rata citra asli (Zhang & Wang, 2008).

Dalam Xiao & Shih, penulis mengusulkan skema watermarking hirarkis. Dalam skema ini, prosedur deteksi kerusakan empat tingkat digunakan dengan menggunakan 2 bit autentikasi dan dilakukan pada ukuran 2×2 sub-blok dari blok ukuran 4×4. Skema ini tidak kuat terhadap serangan kolase dan vektor kuantisasi (VQ) karena bit-bit autentikasi suatu blok terpisah dari blok-blok lainnya. Serangan yang tidak mengubah fitur ini akan gagal dideteksi, sehingga perlu ditambahkan bit autentikasi yang mengandung struktur intensitas rata-rata blok.

c. Kegagalan lokalisasi kerusakan

Karena skema *self-embedding watermarking* umumnya mencakup fitur satu blok citra ke blok lain, ketergantungan *block-wise* yang dihasilkan membuat sulit untuk mendeteksi dan melokalisir gangguan. Untuk mengatasi masalah ini, Lin dkk mengusulkan agar validitas blok gambar ditentukan oleh data autentikasi tambahan di blok. Secara khusus, pada penelitian ini *pay load watermark* dibedakan menjadi data autentikasi dan data restorasi. Data autentikasi untuk blok dipasang di blok itu sendiri, sedangkan data pemulihan dipasang di blok yang berbeda.

d. Kualitas pemulihan

Dalam banyak skema *self-embedding*, bit pemulihan dari suatu sub-blok tertentu selalu disembunyikan di blok itu sendiri atau blok lain dari citra. Pemulihan ini dapat gagal ketika blok atau blok yang berisi bit pemulihannya juga mengalami kerusakan, dinamakan *coincidence problem*. Jika sebagian besar citra mengalami kerusakan, kualitas citra yang dipulihkan umumnya buruk.

Dari kelebihan dan kelemahan beberapa metode dan permasalahan yang ada, dapat diambil posisi penelitian yang diusulkan seperti ditunjukkan pada Gambar 1, dimana akan mencoba menggabungkan beberapa metode dan mengungkap skema baru untuk proses autentikasi dan restorasi citra dengan perbandingan diantara metode yang sudah ada seperti pada Tabel 2 yang menunjukkan 7 hal yang menjadi acuan dalam pengembangan metode, yaitu: ukuran blok, pemetaan blok, pembangkitan bit autentikasi, pembagian bit restorasi, domain penyisipan watermark, proses deteksi, serta proses restorasi.

Citra asli dibagi menjadi blok-blok yang tidak overlap dengan ukuran blok tetap mempertahankan 2× 2 piksel karena berdasarkan eksperimen yang telah dilakukan oleh Chetan & Shivananda (2014) dengan ukuran blok yang berbeda-beda mendapatkan hasil pengukuran seperti terlihat pada Tabel 1. Hal ini menunjukkan bahwa blok ukuran 2×2 memberikan akurasi yang lebih besar dalam mendeteksi kerusakan.

Setelah citra asli dibagi menjadi blok-blok, untuk menyisipkan informasi diperlukan pengacakan blok menggunakan transformasi linier 1D. Penggunaan transformasi linier 1 D dilakukan dengan pemilihan kunci yang tepat agar mendapatkan pemetaan blok satu-satu.

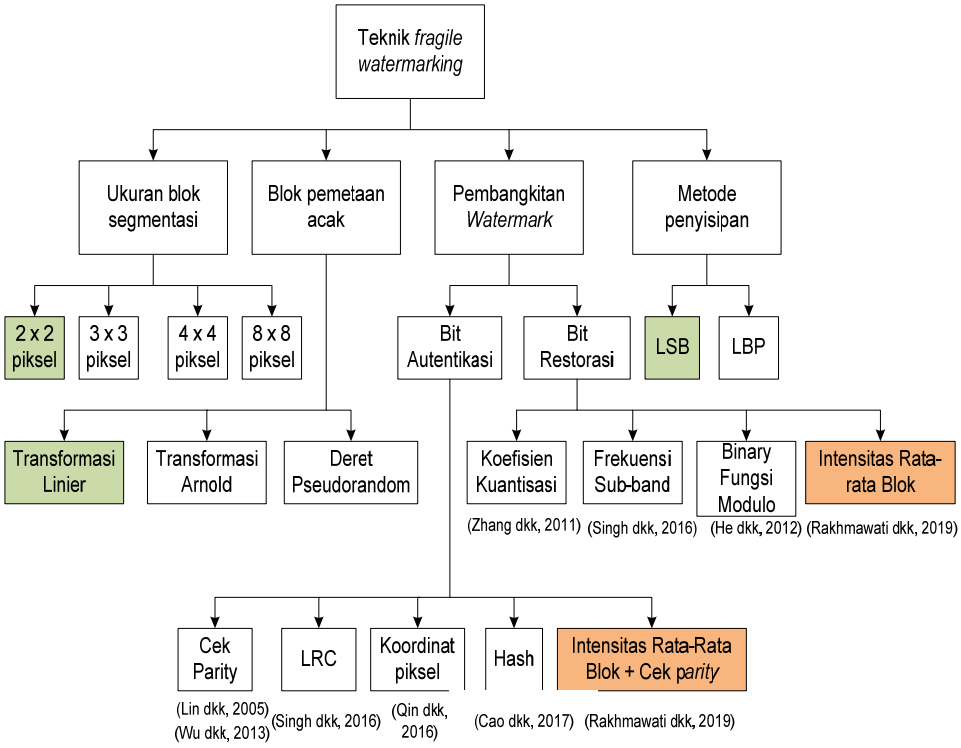
Secara umum, berdasarkan studi literatur bahwasanya paylod berkisar antara 1 sampai dengan 3 bpp. Kualitas citra terwatermark dilihat dari tingginya nilai PSNR, sehingga untuk mengurangi distorsi nilai LSB yang mungkin adalah maksimal mengganti 3 LSB dan dan tetap mempertahankan nilai MSB.

Dengan menggunakan 3 LSB diharapkan lebih banyak informasi yang dapat disisipkan dengan tetap menjaga kualitas citra terwatermark. Bit autentikasi dipilih menggunakan bit parity dan bit yang diambil dari intensitas rata-rata tiap blok 2×2 dengan mengunakan sebuah kunci rahasia yang dapat menghemat memori.

Kelemahan skema *fragile watermarkin* adalah *watermark* dapat dihancurkan oleh operasi pemrosesan citra yang umum seperti kompresi JPEG, peningkatan kontras dan penyaringan. Oleh karena itu, pada tahap selanjutnya dikembangkan teknik *robust watermarking* untuk meningkatkan ketahanan *watermark* dalam proses ekstraksi pada domain frekuensi. Pada penelitian ini menggunakan DCT untuk penyisipan berbasis blok yang lebih tahan terhadap kompresi JPEG. Dengan memanfaatkan kelebihan dan kelemahan kedua metode watermark tersebut, pada roadmap penelitian yang terakhir dikembangkan secara bersamaan teknik *dual watermarking* dapat menolak beberapa operasi pemrosesan citra umum dengan kemampuan deteksi dan restorasi yang baik.

Tabel 1. Akurasi deteksi kerusakan dengan ukuran blok yang berbeda

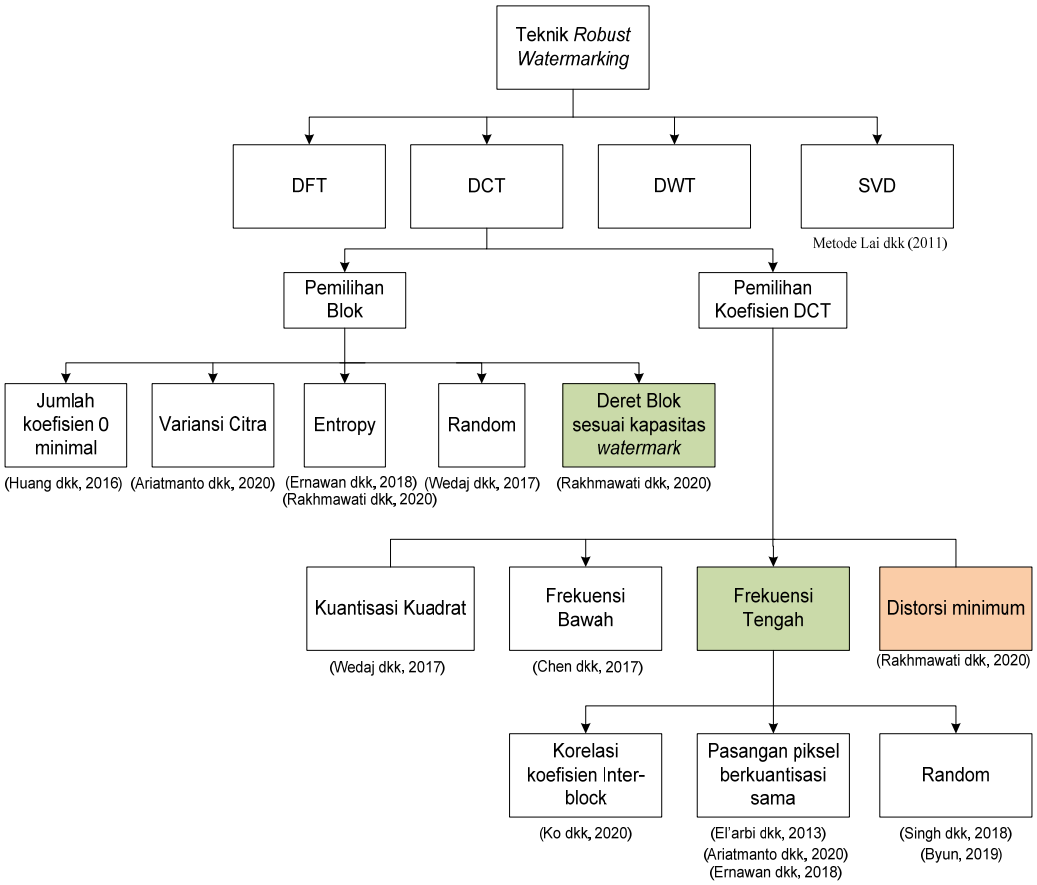
Ukuran blok (piksel)	**Akurasi deteksi kerusakan (%)**
2x2	97
4x4	91
6x6	87
8x8	79



Gambar 1. Posisi teknik *self-embedding fragile watermarking* yang diusulkan

Tabel 2 Perbandingan metode yang diusulkan diantara metode yang sudah ada

Metode Fragile Watermarking	**He dkk (2012)**	**Lin dkk (2005)**	**Singh dkk (2016)**	**Cao dkk (2017)**	**Metode Yang diusulkan (2019)**
Ukuran Blok	3×3	2×2	2×2	2×2	2×2
Pemetaan Blok	Deret Pseudorandom	Transformasi Linier 2-D	Transformasi Linier 2-D	Deret pseudorandom	Transformasi linier 1-D
Bit autentikasi	Intensita rata-rata blok	Cek parity	LRC & Threshold	Hash data	Cek parity & Intensitas rata-rata blok
Bit restorasi	Binary Fungsi modulo	Frekuensi Sub-band	Koefisien Kuantisasi	Deret bit MSB	Intensitas-rata-rata blok
Domain	Spasial: 2 LSB	Spasial: 3 LSB	Spasial: 3 LSB	Spasial: 3 LSB	Spasial: 3 LSB
Proses Deteksi	Tidak Hirarki	Hirarki	Hirarki	Hirarki	Tidak Hirarki
Proses restorasi	Tidak Hirarki	Tidak Hirarki	Tidak Hirarki	Tidak Hirarki	Hirarki



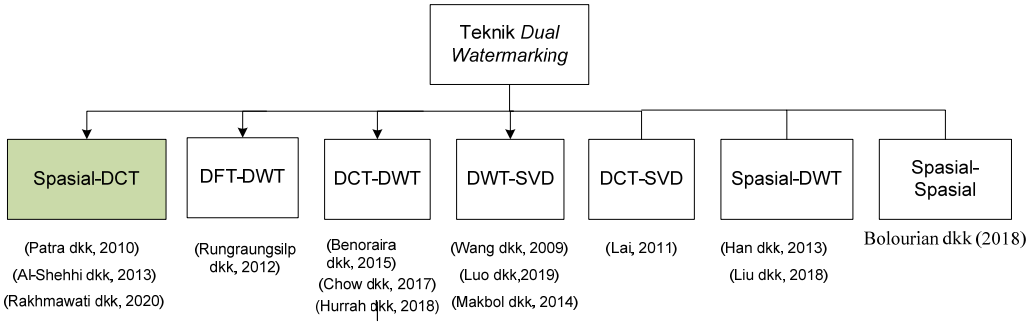
Gambar 2. Posisi teknik *robust watermarking* yang diusulkan

Kelemahan teknik *fragile watermarking* sebagaimana disebutkan oleh (Singh dkk, 2016) adalah *watermark* tidak tahan terhadap operasi pemrosesan citra umum seperti kompresi JPEG, peningkatan kontras, dan penyaringan. Oleh karena itu, pada tahap 2 dikembangkan metode *robust watermarking* dimana posisi penelitian yang dikembangkan bisa dilihat pada Gambar 2. Selanjutnya ditahap 3 kedua metode tersebut dikombinasikan membentuk skema *dual watermarking* dengan beberapa kontribusi didalamnya, terutama dapat melakukan 3 fungsi *watermarking* secara simultan dalam satu citra asli. Adapun posisi penelitian dual watermarking dapat dilihat pada Gambar 3.

Dalam merancang skema *robust watermarking*, dua persyaratan yang saling bertentangan harus dipenuhi pada saat yang sama: (1) *watermark* harus tidak terlihat, dan (2) *watermark* harus kuat dan sangat sulit untuk dihilangkan. Adapun perbandingan metode yang diusulkan tapat dilihat pada Tabel 3.

Tabel 3. Perbandingan metode *robust watermarking* yang diusulkan diantara metode yang sudah ada

Metode *Robust Watermarking*	**Jenis Citra**	**Metode penyisipan**	**Pemilihan Blok**	**Pemilihan lokasi penyisipan**
Metode Lai dkk (2011)	Citra Abu	SVD	Entropy terendah	Threshold
Metode Ariatmanto dkk(2020)	Citra Abu	DCT	Varians terendah	Frekuensi tengah- 5 lokasi piksel dengan aturan tertentu
Metode Ko dkk (2020)	Citra Abu	DCT	Random	Frekuensi Tengah- korelasi koefisien interblok
Metode Byun dkk (2019)	Citra Warna	DCT	Random	Frekuensi Tengah- korelasi koefisien interblok
Metode Liu dkk (2018)	Citra Warna	DWT 1 level	Deret integer blok- subband LL	Sub-band HH
Metode Haghighi dkk (2018)	Citra Abu dan Warna	DWT 2 Level	Deret integer blok- subband LL	Sub-band LL,LH,HL, HH
Metode Yang diusulkan	Citra Abu dan Warna	DCT	Deret integer blok DCT	Frekuensi tengah- eksperimental dan Distorsi minimum



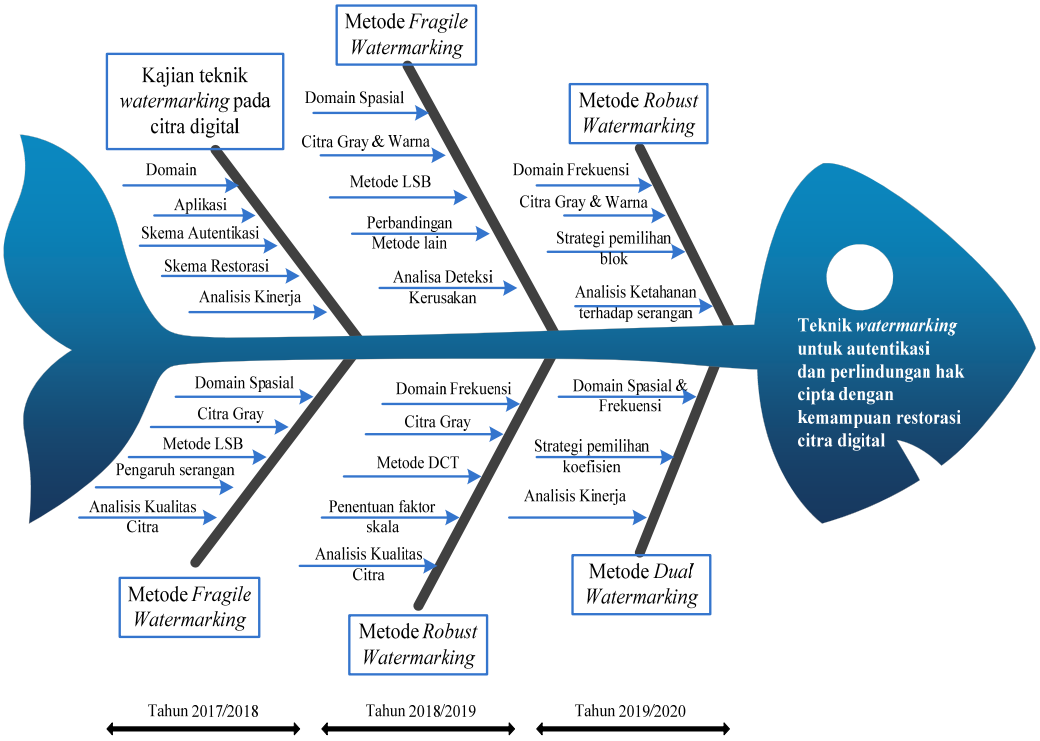
Gambar 3. Posisi teknik *dual watermarking* yang diusulkan

Tabel 4 Perbandingan metode *dual watermarking* yang diusulkan diantara metode yang sudah ada

Parameter	**Hurrah dkk (2018)**	**Liu dkk (2018)**	**Bolourian dkk (2018)**	**Skema Yang diusulkan**
Tipe *Watermark*	Binary	Gray	Gray	Binary
Tipe *Dual Watermarking*	Fragile + Robust	Fragile + Robust	Fragile + Fragile	Fragile + Robust
Domain Penyisipan	Spasial + DCT	Spasial + DWT	Spasial + Spasial	Spasial + DCT

Proses Deteksi	Not Blind + Blind	Not Blind + Blind	Blind + Blind	Blind + Blind
Perlindunngan Hak Cipta	Yes	Yes	No	Yes
Autentikasi Citra	Yes	Yes	Yes	Yes
Restorasi Citra	No	No	Yes	Yes

Tahap 3 dilakukan teknik *dual watermarking* yang menggabungkan antara spasial domain dan frekuensi domain, adapun posisi penelitian yang dilakukan dapat dilihat pada Gambar 3, dimana keunggulan utamanya adalah dapat memfasilitasi 3 fungsi dalam satu citra, yaitu untuk perlindungan hak cipta, autentikasi citra dan restorasi citra seperti terlihat pada Tabel 2.9. Adapun roadmap penelitian yang dilakukan dapat dilihat pada diagram fishbone Gambar 4.

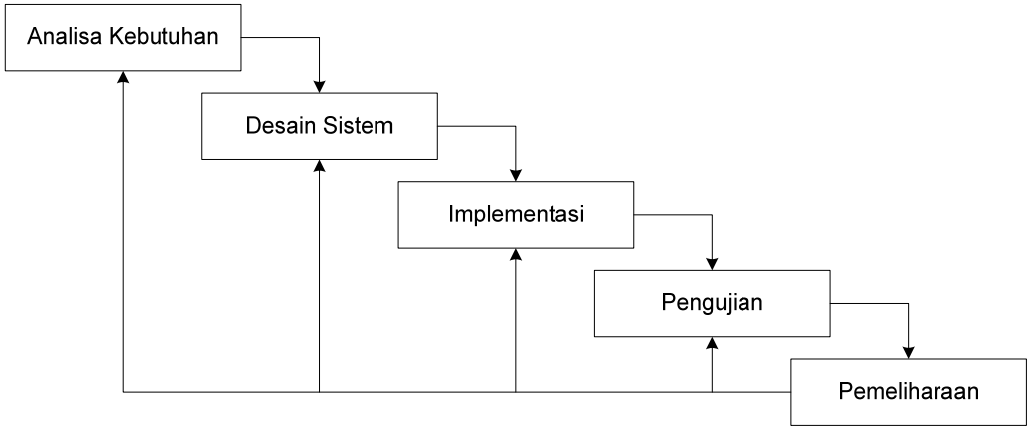


Gambar 4. Diagram *fishbone* penelitian yang diusulkan

Metode atau cara untuk mencapai tujuan yang telah ditetapkan ditulis tidak melebihi 600 kata. Bagian ini dilengkapi dengan diagram alir penelitian yang menggambarkan apa yang sudah dilaksanakan dan yang akan dikerjakan selama waktu yang diusulkan. Format diagram alir dapat berupa file JPG/PNG. Bagan penelitian harus dibuat secara utuh dengan penahapan yang jelas, mulai dari awal bagaimana proses dan luarannya, dan indikator capaian yang ditargetkan. Di bagian ini harus juga mengisi tugas masing-masing anggota pengusul sesuai tahapan penelitian yang diusulkan.

METODE

Adapun pengembangan aplikasi rekayasa perangkat lunak dalam penelitian ini menggunakan model *waterfall* seperti terlihat pada Gambar 5, dimana tahapan yang harus dilalui meliputi analisa kebutuhan, desain sistem, implementasi, integrasi dan pengujian, serta pemeliharaan.



Gambar 5. Tata urutan perancangan simulasi dan implementasi

1.1. Analisa Kebutuhan

Tahap analisis yaitu tahap untuk mengidentifikasi dan mendapatkan data mengenai kebutuhan apa saja yang diperlukan dalam perancangan dan pengimplementasian sistem dan pemikiran untuk perancangan selanjutnya.

a. Analisis kebutuhan pemakai

   Analisis mengenai kebutuhan apa saja yang dibutuhkan oleh pemakai yang harus diterapkan pada sistem atau perangkat lunak. Dalam hal ini pemakai membutuhkan sebuah komputer dengan minimum 3.30 GHz Intel i3 processor, memori 4.00 GB, dan sistem operasi Windows 7.

b. Analisis kerja

   Analisis mengenai data unjuk kerja yang akan dilakukan oleh sistem yang dirancang. Data unjuk kerja meliputi tiga jenis evaluasi, yaitu evaluasi *imperceptibility*, ketahanan *watermark*, dan deteksi kerusakan. Evaluasi *imperceptibility* dari citra terwatermark dan citra hasil restorasi menggunakan ukuran PSNR dan SIM, masing-masing dihitung

menggunakan persamaan 2.20 dan persamaan 2.21. Untuk evaluasi ketahanan ekstraksi *watermark* menggunakan ukuran SIM pada persamaan 2.22 dan BER pada persamaan 2.23. Sedangkan evaluasi keberhasilan proses deteksi dihitung menggunakan PFD pada persamaan 2.32.

c. Analisis data

Analisis mengenai data apa saja yang akan diproses baik sebagai masukan maupun sebagai keluaran. Sebagai masukan adalah citra abu dan citra warna dengan ukuran $M \times M$, dimana M merupakan kelipatan dua, dalam penelitian ini menggunakan ukuran 512× 512. Selanjutnya data luaran adalah menghasilkan citra yang telah disisipi watermark serta citra hasil restorasi setelah mengalami kerusakan dengan kualitas yang baik.

d. Analisis teknologi

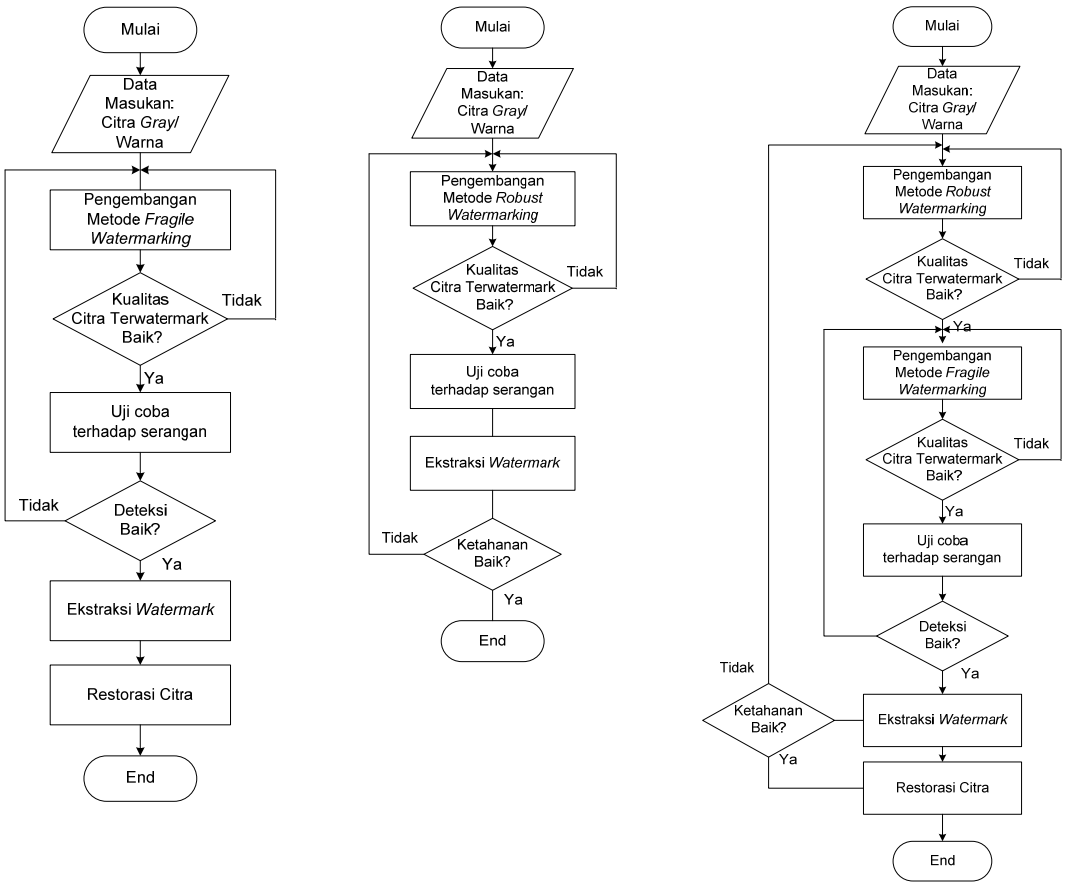
Analisis mengenai teknologi apa yang akan dipakai dalam sistem yang akan dirancang. Pada penelitian ini simulasi dilakukan dengan menggunakan Matlab R2015a.

1.2. Desain Sistem

Desain merupakan tahap melakukan pemikiran untuk mendapatkan cara terefektif dan efisien mengimplementasikan sistem dengan bantuan data yang didapatkan dalam tahap analisis. Di dalam desain akan didapatkan sebuah kerangka untuk mengimplementasikan sistem. Ada beberapa tahap dalam desain yaitu:

a. Desain umum blok diagram kerja

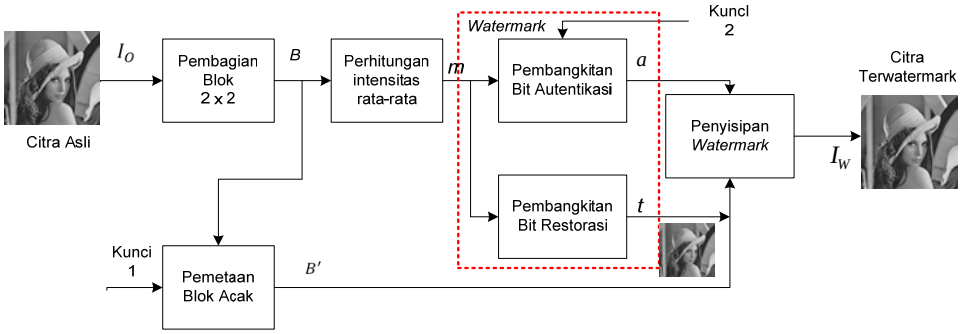
Desain mengenai blok diagram kerja sistem secara keseluruhan yang masih bersifat umum seperti terlihat pada Gambar 6. Hal ini menunjukkan bahwa pengembangan teknik watermarking sebagaimana di jelaskan pada bagan *fishbone* Gambar 3.1 terdiri dari tiga tahap utama, yaitu teknik *fragile watermarking*, teknik *robust watermarking,* dan *dual watermarking*.



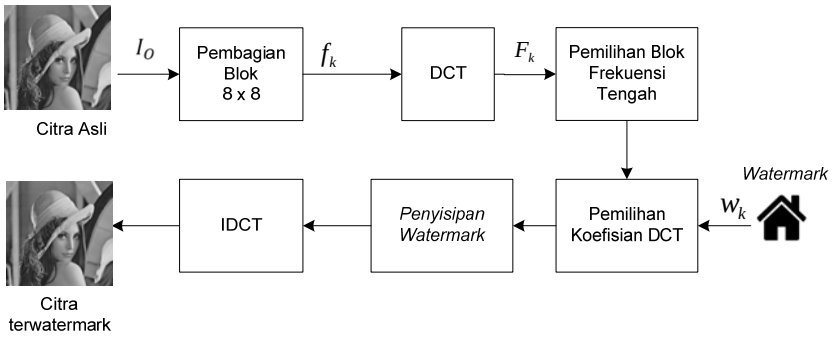
Gambar 6 Blok Diagram Tahapan Penelitian. (a) Tahap 1: metode *fragile watermarking*. (b) Tahap 2: metode r*obust watermarking*. (c) Tahap 3: metode *Dual Watermarking*

b. Desain blok diagram

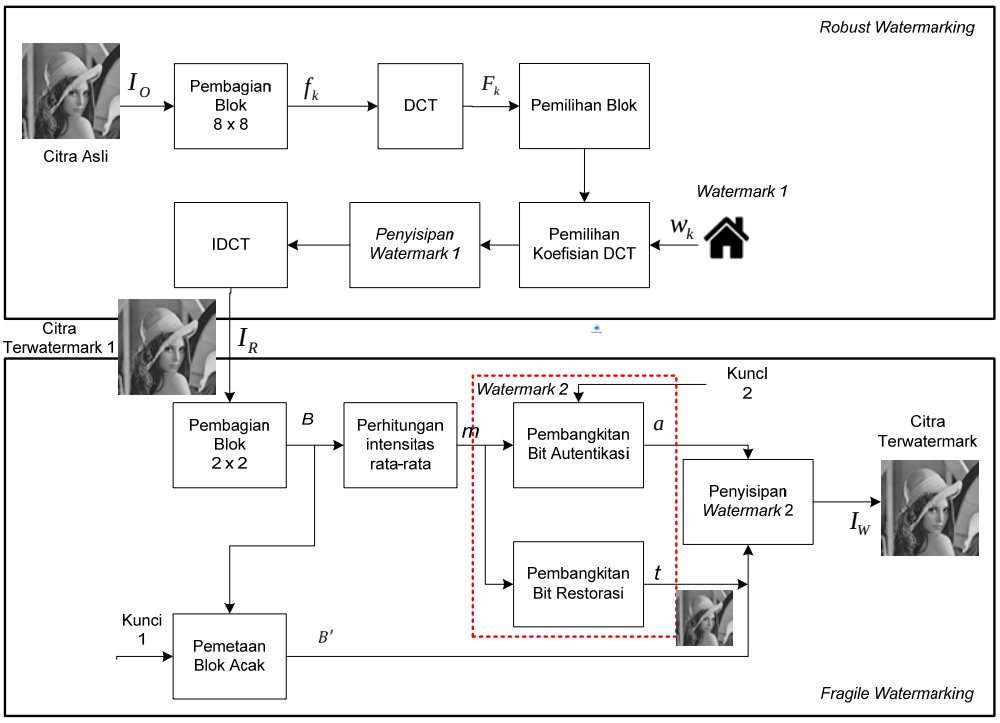
Desain blok diagram menggambarkan urutan proses dan hubungan antara proses secara mendetail didalam suatu sistem seperti ditunjukkan pada Gambar 7 yang menjelaskan prosedur pembangkitan dan penyisipan komponen watermark disisi enkoder dan proses autentikasi dan restorasi citra digital disisi dekoder untuk skema yang diusulkan dengan pengembangan pada kotak merah untuk pembangkitan dua buah watermark dan proses penyisipan menggunakan modifikasi teknik LSB.



(a)



(b)



(c)

Gambar 7. Blok diagram teknik penyisipan watermark: (a) *fragile watermarking*.(b) *robust watermarking*. (c) *dual watermarking*

Jadwal penelitian disusun dengan mengisi langsung tabel berikut dengan memperbolehkan penambahan baris sesuai banyaknya kegiatan.

JADWAL

Tahun ke-1

No	Nama Kegiatan	Bulan											
		1	2	3	4	5	6	7	8	9	10	11	12
1	Studi Literatur												
2.	Pemodelan dan simulasi												
3.	Uji coba dan analisis												
4.	Dokumentasi												
5.	Penyusunan laporan												
6.	Seminar Hasil Penelitian												

Tahun ke-2

No	Nama Kegiatan	Bulan											
		1	2	3	4	5	6	7	8	9	10	11	12
1	Studi Literatur												
2.	Pemodelan dan simulasi												
3.	Uji coba dan analisis												
4.	Dokumentasi												
5.	Penyusunan laporan												
6.	Seminar Hasil Penelitian												

Daftar pustaka disusun dan ditulis berdasarkan sistem nomor sesuai dengan urutan pengutipan. Hanya pustaka yang disitasi pada usulan penelitian yang dicantumkan dalam Daftar Pustaka.

DAFTAR PUSTAKA

Al-shehhi, Sultan, A. Mohammed, A.Dalia, A. Hussain, W. Naoufel, & K. Alavi, (2013), "Robust and Fragile Watermarking Scheme Based on DCT and Hash Function for Color Satellite Images", *2013 Sixth International Conference on Developments in eSystems Engineering*, Abu Dhabi, 2013, pp. 253-258, doi: 10.1109/DeSE.2013.53.

Ariatmanto, D. & F. Ernawan, (2020) "An improved robust image watermarking by using different embedding strengths," *Multimed Tools Appl*, 2020.

Benoraira, Ali, K. Benmahammed, N. Boucenna, (2015), "Blind image watermarking technique based on differential embedding in DWT and DCT domains", *Eurasip Journal on Advances in Signal Processing*, 2015(1).

Bolourian B. Haghighi, A. H. Taherinia, and A. Harati, (2018), "TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet

transform and halftoning technique," *Journal of Visual Communication and Image Representation*, vol. 50, no. December 2016, pp. 49–64, 2018.

Bravo-Solorio, S. & A.K. Nandi (2011), "Secure fragile watermarking method for image authentication with improved tampering localisation and self-recovery capabilities", *Signal Processing*, Vol. 91, pp. 728–739. doi:10.1016/j.sigpro.2010.07.019.

Byun, Sung-Woo, S. Heui-Su, Seok Lee, (2017), "Fast and Robust Watermarking Method Based on DCT Specific Location", Vol. 7, pp. 100707-100718.

Cao, F., B. An, J. Wang, D. Ye, & H. Wang (2017), "Hierarchical Recovery for Tampered Images Based on Watermark Self-Embedding", Displays.

Chamlawi, Rafiullah, I.Usman, A.Khan (2009), "Dual Watermarking Method for Secure Image Authentication and Recovery", *IEEE 13th International* , pp.1-4.

Chang, Jun-Dong, B. Chen, & C. Tsai (2013), "LBP-based Fragile Watermarking Scheme for Image Tamper Detection and Recovery", *IEEE 2nd International Symposium on Next-Generation Electronics (ISNE)*, pp. 173–176.

Chen, Tao , H. Lu (2012), "Robust spatial LSB watermarking of color images against JPEG compression", *IEEE 5th Int. Conf. Adv. Comput. Intell. ICACI 2012*, pp. 872–875.

Chen,T-Y, M. Hwang, & J. Jan (2012), "A secure image authentication scheme for tamper detection and recovery", *The Imaging Science Journal*, vol. 60, pp. 219–233.

Chen Lei & S. Wang, (2017),"A secure blind watermarking scheme based on DCT domain of the scrambled image", http://arxiv.org/abs/1708.09535

Cheng, Baotian, R. Ni, & Y. Zhao (2012), "A Refining Localization Watermarking for Image Tamper detection and Recovery", *IEEE 11 th International conference on Signal processing*, pp. 1–5.

Chetan, K.R. , N. Shivananda (2014), "A new fragile watermarking approach for tamper detection and recovery of document images", *International Conference on Advances in Computing,Communications and Informatics (ICACCI)*, pp. 1494–1498.

Chow, Y., Susilo, W., Tonien, J. & Zong, W. (2017). A QR Code Watermarking Approach based on the DWT-DCT Technique. Lecture Notes in Computer Science, 10343 314-331. Auckland, New Zealand ASCIPS 2017: 22nd Australasian Conference on Information Security and Privacy

Dhole, V. S., & N. N. Patil (2015), "Self-Embedding Fragile Watermarking for Image Tampering Detection and Image Recovery using Self Recovery Blocks", *IEEE International Conference on Computing Communication Control and Automation*, pp. 752–757.

Doyoddorj, M., K-H Rhee (2012), "Design and Analysis of a Fragile Watermarking Scheme Based on Block-Mapping", *Int. Cross-Domain Conf. andWorkshop Availability, Reliab. Secur., pp.* 654–668.

Ekici, O., B. Sankur, and M. Akcay (2004), "Comparative evaluation of semifragile watermarking algorithms", *J. Electron. Imaging*, Vol.13, pp.209-229.. doi:10.1117/1.1633285.

Ernawan, F & Muhammad N. Kabira, (2018), "Robust Image Watermarking Technique With an Optimal DCT-Psychovisual Threshold", IEEE Access, Vol. 6, pp.20464-20480.

Eswaraiah, R. & E. Sreenivasa Reddy (2014) , "ROI-Based Fragile Medical Image Watermarking Technique for Tamper Detection and Recovery using Variance", *IEEE Seventh International Conference on Contemporary Computing (IC3)*, pp. 1–6.

Freitas , P. G., R. Rigoni, and M. C. Q. Farias (2016), "Secure self-recovery watermarking

scheme for error concealment and tampering detection", *J. Brazilian Comput. Soc.* Vol. 22, No. 5, pp.1-13.

Hamid , M. (2016), "DCT-Based Image Feature Extraction and Its Application in Image Self-Recovery and Image Watermarking", Thesis Concordia Univesity, Canada.

Han, Q, L. Han, E. Wang, and J. Yang (2013), "Dual Watermarking for Image Tamper Detection and Self-recovery", *IEEE Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, no. 1.

He, H., F. Chen, H. Tai, T. Kalker, & J. Zhang (2012), "Performance Analysis of a Block-Neighborhood- Based Self-Recovery Fragile Watermarking Scheme", *IEEE Trans. Inf. Forensics Secur.*, Vol. 7, No. 1, pp. 185–196.

He, H, J. Zhang, and F. Chen. (2009), "Adjacent-block based statistical detection method for self-embedding watermarking techniques", *Signal Processing*, Vol. 89, pp. 1557–1566.

Hemida, O., Y. Huo, F. Chen, & H. He (2017), "Block-DCT Based Alterable-Coding Restorable Fragile Watermarking Scheme with Superior Localization", *Annual Summit and Conference*, pp. 846–851.

http://sipi.usc.edu/database/

Hsu, C-S., S-F. Tu (2011), "Image tamper detection and recovery using differential embedding strategy", *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, pp. 399–402.

Huang F., S. Kim, Xiaochao Qu, Hyoung Joong Kim, & Jiwu Huang, (2016), "Reversible data hiding in JPEG images," *IEEE Transactions on Circuits Systems and Video Technology*, vol. 26, no. 9, pp. 1610–1621.

Huo, Y, H. He, & F. Chen (2012), "Alterable-capacity fragile watermarking scheme with restoration capability", *OPTICS*, Vol.285, pp. 1759–1766. doi:10.1016/j.optcom.2011.12.044.

Huo, Y., H. He, and F. Chen, (2013), " Semi-fragile watermarking scheme with discriminating general tampering from collage attack", *Asia-Pacific Signal Inf. Process. Assoc. Annu. Summit Conf.*, pp. 1–6.

Hurrah N. N., S. A. Parah, N. A. Loan, J. A. Sheikh, M. Elhoseny, and K. Muhammad, (2019), "Dual watermarking framework for privacy protection and content authentication of multimedia," *Future Generation Computer Systems*, vol. 94, pp. 654–673.

Khan, A., A. Siddiqa, S. Munib, and S.A. Malik (2014),"A recent survey of reversible watermarking techniques", Information Science, pp.1-22.. doi:10.1016/j.ins.2014.03.118.

Kiatpapan, S. & T. Kondo (2015), "An Image Tamper Detection and Recovery Method Based on Self-Embedding Dual Watermarking", *IEEE 12th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON),* 2015 .

Kunhu, A., H. Al-ahmad, & S. Al Mansoori (2017), "A Reversible Watermarking Scheme for Ownership Protection and Authentication of Medical Images", *IEEE International Conference on Electrical and Computing Technologies and Applications*.

Kingsbury N, The dual-tree complex wavelet transform: a new technique for shift invariance and directional filters, in Proc. 8th IEEE DSPWorkshop: Bryce Canyon, 1998, pp 319–322.

Ko, Hung-Jui, C. Huang , G. Horng , S. Wang, (2020), "Robust and blind image watermarking in DCT domain using inter-block coefficient correlation", Information Science, Vol. 517, pp. 128-147.

Lai, Chih Chin, (2011), "An improved SVD-based watermarking scheme using human visual

characteristics", Optics Communication,Vol.284 (4), pp.938-944.
Li, C., Y. Wang, B. Ma, & Z. Zhang (2011), "A novel self-recovery fragile watermarking scheme based on dual-redundant-ring structure", *Comput. And Electr. Eng.*, Vol.37, pp. 927–940. doi:10.1016/j.compeleceng.2011.09.007.
Li, Y. and L. Du (2014), "Semi-Fragile Watermarking for Image Tamper Localization and Self-Recovery", *IEEE Int. Conf. Secur. Pattern Anal. Cybern.*, pp. 328–333.
Lin, P.L., C-K. Hsieh, &P-W. Huang (2005), "A hierarchical digital watermarking method for image tamper detection and recovery", *Pattern Recognit.*, vol. 38, no. 12, pp. 2519–2529.
Lin, P-L., P-W Huang, A-W. Peng (2006), "An Image Watermarking Scheme with Tamper Detection and Recovery", *IEEE Int. Conf. Innov. Comput. Inf. Control.*, pp. 1–4.
Lin, P-L, P-W Huang, A-W Peng (2004), "A fragile watermarking scheme for image authentication with localization and recovery", *IEEE. Int. Symp. Multimed. Softw. Eng.*, pp. 146–153. doi:http://doi.ieeecomputersociety.org/10.1109/MMSE.2004.9.
Liu, X-L., C-C. Lin, C-C. Chan, & S-M Yuan (2016), "A Survey of Fragile Watermarking-based Image Authentication Techniques", Vol.7, pp.1282–1292.
Luo, An Wei, L.H. Gong, & N.R. Zhou, (2020), "Adaptive and blind watermarking scheme based on optimal SVD blocks selection", Vol. 79(1-2), pp. 243-261.
Zou, Wei PingAdaptive and blind watermarking scheme based on optimal SVD blocks selection
Mousavi, S.M. and A. Naghsh (2014)., "Watermarking Techniques used in Medical Images : a Survey", *J Digit Imaging* . doi:10.1007/s10278-014-9700-5.
Patra, J.C., J.E. Phua, & C. Bornand (2010), "A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression", *Digit. Signal Process.*, Vol. 20, pp. 1597–1611. doi:10.1016/j.dsp.2010.03.010.
Qi, X, X. Xin (2015), "A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization," *J. Vis. Commun. Image Represent.*, vol. 30, pp. 312–327.
Qin, C., C-C. Chang, and P-Y Chen (2012), "Self-embedding fragile watermarking with restoration capability based on adaptive bit allocation mechanism", *Signal Processing*, Vol. 92, pp. 1137–1150. doi:10.1016/j.sigpro.2011.11.013.
Qin, C., P. Ji, X. Zhang, J. Dong, and J. Wang (2017), "Fragile Image Watermarking With Pixel-wise Recovery Based on Overlapping Embedding Strategy'', *Signal Processing*, Vol. 138, pp. 280–293. doi:10.1016/j.sigpro.2017.03.033.
Rakhmawati, L, W. Wirawan, & S. Suwadi, "A recent survey of self-embedding fragile watermarking scheme for image authentication with recovery capability," *EURASIP Journal on Image and Video Processing*, vol. 2019, no. 1, 2019.
Rakhmawati, L, W. Wirawan, & S. Suwadi, "Exploiting Self-Embedding Fragile Watermarking Method for Image Tamper Detection and Recovery," *International Journal of Intelligent Engineering and Systems*, Vol. 12, No. 4, 2019.
Rungraungsilp, Suppat, K.Mahasak, W. Tanee, & P. Kanchana,(2012), "Data Hiding Method for QR Code Based on Watermark by comparing DFT with DWT Domain", International Conference on Computer and Communication Technologies (ICCCT'2012) May 26-27, Phuket.
Sarreshtedari, S., & M. A. Akhaee (2015), "A Source-Channel Coding Approach to Digital Image Protection and Self-Recovery," *IEEE Transactions on Image Processing*, Vol. 24, No. 7, pp. 2266–2277.
Sarreshtedari,S., M. A. Akhaee, & A. Abbasfar (2015), "Digital Image Self-Recovery Using

Unequal Error Protection", *Eur. Signal Process. Conf.*, pp. 71–75.

Shoaib, S. and R. C. Mahajan (2015), "Authenticating Using Secret Key in Digital Video Watermarking Using 3-Level DWT", *IEEE International Conference on Communication, Information & Computing Technology (ICCICT),* pp. 1–5.

Shruthy, V.C. & S. Varghese (2015), "An Efficient Self-Embedding Watermarking Scheme for Colour Image Tamper Detection and Recovery", *Int. J. Comput. Sci. Mob. Comput.* , Vol. 4, pp. 383–390.

Shih, Frank Y, (2017). *Digital watermarking and steganography : fundamentals and techniques*, Second edition, Taylor & Francis, CRC Press, Boca Raton.

Singh, D. & S.K. Singh (2016),"Effective self-embedding watermarking scheme for image tampered detection and localization with recovery capability", *J. Vis. Commun. Image Represent.*, Vol.38, pp. 775–789. doi:10.1016/j.jvcir.2016.04.023.

Sreenivas, K. and V.K. Prasad (2016), "Improved Block Encoding Method For An Image Self-Recovery Approach", *IEEE Int. Conf. Inf. Commun. Embed. Syst.*, pp. 3–7.

Tang, Chang, J. Wu, C. Zhang, P. Wang, & W. Li. (2016), "Salient Object Detection via Weighted Low Rank Matrix Recovery", *IEEE Signal Processing Letters*, vol. XX, no. c, pp. 1–5.

Thongkor, K. , T. Amornraksa (2012) ,"Digital Image Watermarking for Photo Authentication in Thai national ID card", *IEEE International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pp. 0–3.

Tiwari, A., M. Sharma, and R.K. Tamrakar(2017), "Watermarking based image authentication and tamper detection algorithm using vector quantization approach", *AEUE - Int. J. Electron. Commun.* , Vol. 78, pp. 114–123. doi:10.1016/j.aeue.2017.05.027.

Tong, X., Y. Liu, M. Zhang, and Y. Chen (2013), "A novel chaos-based fragile watermarking for image tampering detection and self-recovery", *Signal Process. Image Commun.* , Vol. 28, pp. 301–308. doi:10.1016/j.image.2012.12.003.

Vyas, Chinmay ,and M. Lunagaria (2014), "A Review on Methods for Image Authentication and Visual Cryptography in Digital Image," *IEEE International Conference on Computational Intelligence and Computing Research*.

Wang, Wei, A.Men, and B.Yang (2010), "A feature-based semi-fragile watermarking scheme in DWT domain", *IEEE Int. Conf. Netw. Infrastruct. Digit. Content,* pp. 768–772.

Wang, N. & C-H. Kim (2009), "Tamper Detection and Self-Recovery Algorithm of Color Image Based on Robust Embedding of Dual Visual Watermarks Using DWT-SVD", *Proc. Int. Symp. Commun. Inf. Technol,* pp .157–162.

Wedaj, F.T, S. Kim, H. J Kim, & F.Huang, (2017), Improved reversible data hiding in JPEG images based on new coefficient selection strategy, vol.63.

Wu, C-M., Y-S. Shih (2013), "A Simple Image Tamper Detection and Recovery Based on Fragile Watermark with One Parity Section and Two Restoration Sections", *Opt. Photonics J.*, Vol. 3, No. 2, pp. 103–107.

Xiao, D. & F.Y. Shih (2012), "An improved hierarchical fragile watermarking scheme using chaotic sequence sorting and subblock post-processing", *OPTICS,* Vol. 285, pp. 2596–2606. doi:10.1016/j.optcom.2012.02.002.

Xin, Liping (2016), "Research on the Application of Error Correction Technology in Self-recovery Digital Watermarking," *IEEE 11th Conference on Industrial Electronics and Applications*, pp. 140–143.

Yu, M., J. Wang, G. Jiang, Z. Peng, F. Shao, and T. Luo (2014), ”New fragile watermarking method for stereo image authentication with localization and recovery”, *AEUE - Int. J. Electron. Commun* , Vol.69, pp. 361–370. doi:10.1016/j.aeue.2014.10.006.

Yu , X., C. Wang, and X. Zhou (2017), “Review on Semi-Fragile Watermarking Algorithms for Content Authentication of Digital Images”, *Future Internet*, Vol.9, pp. 1–17. doi:10.3390/fi9040056.

Zhang, H., C. Wang, and X. Zhou (2017), “Fragile Watermarking for Image Authentication Using the Characteristic of SVD”, Vol. 10, pp 1–12. doi:10.3390/a10010027.

Zhang, R., D. Xiao, and Y. Chang(2018), “A Novel Image Authentication with Tamper Localization and Self-Recovery in Encrypted Domain Based on Compressive Sensing”, *Secure Commun. Networks*.. doi:https://doi.org/10.1155/2018/1591206.

Zhang, X., S. Wang, Z. Qian, and G. Feng (2011), “Reference Sharing Mechanism for Watermark Self-Embedding”, *IEEE Trans. Image Process*. , Vol. 20 , pp. 485–495. doi:10.1109/TIP.2010.2066981.

Zhang, X., S. Wang (2008), “Fragile Watermarking with Error Free Restoration Capability”, *IEEE Trans. Multimed.*, Vol.10, pp. 1490–1499. doi:10.1109/TMM.2008.2007334.

Zhang, X., Z. Qian, Y. Ren, G. Feng (2011), “Watermarking With Flexible Self-Recovery Quality Based on Compressive Sensing and Compositive Reconstruction”, *IEEE Trans. Inf. Forensics Secur.* , Vol. 6, pp.1223–123

.