

BAB 1

USULAN GAGASAN

1.1 Deskripsi Umum Masalah

Watermarking merupakan teknologi yang berfungsi untuk menyisipkan informasi tertentu ke dalam citra digital, bertujuan untuk melindungi hak cipta serta menjaga keaslian dan integritas dari citra tersebut [1], [2]. Permasalahan yang diangkat dalam proyek *capstone* ini berkaitan dengan pentingnya menciptakan *Watermarking* yang tidak hanya *robust*, tetapi juga *reversible*. *Robust* memastikan bahwa informasi tetap terjaga meskipun citra mengalami manipulasi atau kompresi sedangkan *reversible* memungkinkan citra asli dapat dikembalikan tanpa kehilangan informasi setelah proses ekstraksi *watermark* dilakukan [3], [4].

Masalah ini semakin kompleks mengingat peningkatan jumlah konten digital yang dibagikan secara luas, serta kebutuhan untuk melindungi konten tersebut dari penyalahgunaan. Contoh penerapan yang signifikan termasuk perlindungan hak cipta untuk fotografer, branding perusahaan melalui logo pada konten iklan, dan keamanan data dalam dokumen sensitif [3]. Di sektor pendidikan, institusi dapat menggunakan *Watermarking* untuk melindungi materi ajar, sedangkan dalam industri media, teknologi ini membantu melawan pembajakan konten [1]. Kesadaran masyarakat juga meningkat, berkat kampanye edukasi dari organisasi hak cipta dan adopsi fitur otomatis di platform media sosial.

Pertimbangan teknis seperti algoritma yang efisien, keamanan data, serta ketahanan terhadap berbagai bentuk serangan seperti kompresi, pemotongan, atau modifikasi citra juga menjadi fokus utama. Dalam hal ini, beberapa solusi telah diusulkan di dalam literatur, seperti metode berbasis transformasi frekuensi misalnya *Discrete Wavelet Transform* (DWT), *Discrete Cosine Transform* (DCT), *Slantlet Transform* (SLT), dan metode *spatial domain*, namun masing-masing memiliki kekurangan, terutama dalam hal *robustness* dan *reversibility* [1], [2]. Proyek ini bertujuan untuk mengeksplorasi lebih lanjut solusi yang tidak hanya menjaga keamanan informasi dalam citra digital, tetapi juga mampu mempertahankan kualitas dan keutuhan citra asli.

1.2 Analisis Masalah

Adapun aspek utama yang akan dianalisis adalah aspek teknis, mengingat ini berkaitan erat dengan bidang keilmuan yang mendasari proyek *capstone* ini. Selain itu, aspek ekonomi dan aspek keamanan juga akan dibahas untuk memberikan pemahaman yang lebih luas tentang kompleksitas masalah ini.

1.2.1 Aspek Teknis

Dari segi teknis, *Watermarking* yang *robust* dan *reversible* (RRW) menghadirkan tantangan besar dalam hal desain algoritma. *Robustness* mengacu pada kemampuan *watermark* untuk bertahan meskipun terjadi kompresi, modifikasi, atau manipulasi citra [1], [2], [3], sementara *reversibility* berarti citra asli dapat dipulihkan sepenuhnya setelah proses ekstraksi *watermark*. Tantangan utama dari aspek teknis adalah menemukan keseimbangan antara ketahanan *watermark* terhadap serangan dan kemampuan untuk mengembalikan citra asli secara utuh.

Permasalahan ini semakin rumit dengan meningkatnya kualitas alat manipulasi citra, seperti perangkat lunak pengeditan gambar yang canggih. Algoritma yang ada saat ini sering kali memiliki keterbatasan dalam menjaga kedua aspek tersebut secara bersamaan. Pada beberapa kasus, algoritma yang memberikan ketahanan yang kuat sering kali mengorbankan kualitas citra asli atau tidak dapat dilakukan secara reversibel.

1.2.2 Aspek Ekonomi

Dari perspektif ekonomi, masalah ini terkait dengan perlindungan terhadap hak kekayaan intelektual dalam bentuk konten digital, seperti foto, ilustrasi, dan video. Tanpa sistem *Watermarking* yang *robust* dan *reversible* [4], perusahaan dan individu menghadapi risiko besar dari pencurian atau manipulasi konten yang berpotensi menimbulkan kerugian finansial. Industri kreatif, seperti fotografi dan desain grafis, sangat bergantung pada teknologi yang dapat melindungi hasil karya mereka dari pembajakan.

Selain itu, penggunaan teknologi yang efisien dapat membantu mengurangi pemborosan atau biaya tersembunyi dalam proses litigasi hukum terkait hak cipta. Dengan penggunaan teknologi yang baik, bukti kepemilikan dapat lebih mudah diverifikasi, sehingga meminimalkan biaya terkait sengketa hukum.

1.2.3 Aspek Keamanan

Aspek keamanan juga menjadi fokus penting dalam masalah ini. *Watermarking* yang tidak kuat bisa menjadi sasaran serangan, seperti pemotongan atau *resampling*, yang berusaha untuk menghapus atau memanipulasi *watermark* tanpa merusak citra secara signifikan [3], [4]. Hal ini menjadi perhatian serius dalam dunia digital yang semakin rentan terhadap serangan siber. Perlindungan citra digital melalui *Watermarking* harus mampu menangkal berbagai metode serangan dengan memastikan bahwa informasi tetap utuh dan terlindungi.

Keamanan juga mencakup privasi data yang disisipkan dalam *watermark*. Dalam beberapa konteks, *watermark* dapat berisi informasi sensitif atau rahasia yang jika terungkap atau dihilangkan dapat menimbulkan dampak negatif yang signifikan.

1.2.4 Aspek Hukum

Dari aspek hukum, *Watermarking* yang efektif memainkan peran penting dalam menjaga dan membuktikan kepemilikan hak cipta [1], [2], [3]. Teknologi ini sangat relevan dalam konteks regulasi kekayaan intelektual dan Undang-Undang Hak Cipta. Jika *watermark* yang diterapkan tidak dapat memberikan bukti kepemilikan yang kuat karena tidak cukup *robust*, maka proses hukum untuk melindungi karya dari pembajakan menjadi sulit dilakukan. *Watermarking* yang dapat diandalkan akan memudahkan verifikasi kepemilikan di pengadilan dan membantu menghindari kebingungan atau perdebatan tentang sumber asli konten yang dipersengketakan. Hal ini penting terutama dalam perselisihan hak cipta yang melibatkan bukti visual.

1.3 Analisis Solusi yang Ada

Berikut ini merupakan rangkuman solusi yang diperoleh dari berbagai jurnal akademik yang secara mendalam meninjau aspek-aspek keunggulan, kelemahan, serta keterbatasan yang terdapat dalam penelitian-penelitian sebelumnya, dengan tujuan memberikan wawasan yang lebih komprehensif mengenai topik yang dibahas.

1.3.1 Skema Menggunakan Normalisasi dan Penyematan Adaptif Berbasis Simulasi Serangan (RRW)

Keunggulan dari skema ini terletak pada penggunaan teknik normalisasi adaptif yang berbasis simulasi serangan, yang terbukti mampu meningkatkan ketahanan *watermark* terhadap berbagai jenis serangan umum (*common signal processing*), seperti *Additive White Gaussian Noise* (AWGN), kompresi *Joint Photographic Experts Group* (JPEG), serta distorsi geometris seperti rotasi dan skala. Selain itu, skema ini menggunakan *quantizer multi-level* yang memungkinkan peningkatan kapasitas penyisipan *watermark* tanpa mengorbankan ketahanannya terhadap serangan [4]. Penggunaan *Polar Harmonic Transform* (PHT) dalam proses *embedding* juga memberikan keunggulan tersendiri, karena memiliki kompleksitas komputasi yang rendah serta stabilitas numerik yang tinggi, sehingga kinerja sistem dalam menghadapi serangan geometris menjadi lebih optimal.

Kekurangan dari metode ini antara lain adalah tingginya beban komputasi yang dihasilkan akibat penggunaan simulasi serangan adaptif untuk meningkatkan ketahanan, terutama ketika

diaplikasikan pada citra dengan skala besar. Selain itu, meskipun metode ini menawarkan ketahanan dan reversibilitas yang baik, penerapannya menjadi kurang ideal dalam lingkungan dengan keterbatasan sumber daya, seperti pada perangkat *embedded* atau aplikasi *real-time*, karena kompleksitas komputasi yang cukup tinggi.

Keterbatasan yang dimiliki metode ini mencakup tantangan dalam menjaga keseimbangan antara ketidakterlihatan (*invisibility*) *watermark* dan ketahanan terhadap serangan. Pendekatan adaptif memang memberikan ketahanan yang tinggi, namun serangan yang sangat kuat tetap dapat menurunkan kualitas visual dari gambar yang telah disisipi *watermark*. Selain itu, karena metode ini berfokus pada transformasi *Polar Harmonic*, efektivitasnya terhadap distorsi geometris yang lebih kompleks masih terbatas dan belum sepenuhnya optimal.

1.3.2 Skema Berdasarkan *Spread Spectrum* (RRW)

Keunggulan dari skema ini adalah kemampuannya dalam memberikan ketahanan yang tinggi terhadap berbagai jenis serangan dengan cara menyebarkan bit *watermark* ke seluruh bagian citra [5], [6]. Teknik penyebaran ini memungkinkan *watermark* tetap dapat dipertahankan bahkan ketika citra mengalami serangan kuat seperti kompresi JPEG, noise tipe *Salt and Pepper*, maupun gangguan AWGN. Selain itu, penggunaan kode *Spread Spectrum* yang bersifat adaptif memberikan jaminan bahwa citra asli dapat dipulihkan sepenuhnya jika tidak ada serangan, dan tetap dapat direkonstruksi sebagian ketika terjadi serangan, sehingga menjaga aspek *reversibility* dalam kondisi yang menantang.

Kekurangan dari metode ini terletak pada terbatasnya kapasitas penyisipan data. Karena karakteristik dari teknik *Spread Spectrum*, jumlah data yang dapat disisipkan lebih sedikit dibandingkan metode lain seperti *quantization multi-level*. Selain itu, efektivitas skema ini dapat menurun ketika dihadapkan dengan serangan gabungan atau serangan geometris yang kompleks, karena struktur penyebaran *watermark* cenderung lebih lemah terhadap transformasi yang tidak linier.

Keterbatasan utama dari skema ini adalah perlunya penyesuaian ambang (*threshold*) yang rumit untuk proses pemulihan *watermark* di bawah kondisi serangan. Hal ini sering kali membutuhkan informasi tambahan (*side information*) yang dapat mengurangi efisiensi dan menyulitkan penerapan dalam sistem waktu nyata. Meskipun tahan terhadap serangan pemrosesan sinyal umum seperti kompresi JPEG, performa dari metode ini tetap belum optimal ketika menghadapi distorsi geometris yang lebih kompleks, seperti rotasi besar atau transformasi perspektif ekstrem.

1.3.3 Skema RRW Menggunakan Momen Zernike lokal dengan Pemilihan Titik Fitur

Keunggulan utama dari skema ini terletak pada pendekatan inovatif yang menggabungkan Momen *Zernike* lokal dengan pemilihan titik-titik fitur yang strategis, sehingga memungkinkan pencapaian tingkat ketahanan *watermark* terhadap serangan yang sebelumnya sulit ditangani. Salah satu fitur unggulannya adalah kemampuannya dalam menentukan secara dinamis ukuran area *embedding* berdasarkan jarak dari pusat gambar. Hal ini berkontribusi pada peningkatan ketahanan terhadap serangan sekaligus menjaga kualitas visual citra yang baik [7].

Kekurangan dari metode ini adalah bertambahnya jumlah informasi kompensasi yang harus disimpan akibat kompleksitas sistem, yang pada akhirnya dapat menurunkan efisiensi, terutama dalam proses ekstraksi atau penyimpanan. Selain itu, strategi *embedding* dilakukan pada area lokal di sekitar tepi gambar yang memiliki ukuran relatif kecil. Pendekatan ini menjadikan *watermark* lebih rentan terhadap serangan yang menargetkan area kecil, seperti rotasi ekstrem atau pemotongan sebagian.

Keterbatasan metode ini terletak pada performanya terhadap skenario serangan yang lebih kompleks. Meskipun ketahanannya terhadap distorsi geometris dasar sudah cukup baik, efektivitasnya masih perlu ditingkatkan untuk menghadapi kombinasi serangan seperti *cropping* yang agresif dan penambahan *noise* secara bersamaan. Selain itu, keberhasilan metode ini sangat bergantung pada akurasi deteksi titik fitur lokal. Dalam kondisi citra dengan tekstur yang rendah atau ketika terkena serangan kuat, proses deteksi titik fitur bisa terganggu, sehingga berdampak langsung pada akurasi ekstraksi *watermark* [7].

1.3.4 Skema RRW Berbasis Ekstraksi Fitur Menggunakan Momen Zernike Dan Pergeseran Histogram (FRRW)

Keunggulan dari metode ini terletak pada kombinasi antara *Zernike moments* dan algoritma ekstraksi fitur seperti *Speeded-Up Robust Features* (SURF) dan *Oriented FAST and Rotated BRIEF* (ORB), yang memberikan ketahanan tinggi terhadap berbagai bentuk distorsi geometris seperti rotasi dan skala, serta serangan berbasis *noise* [8]. Dengan memanfaatkan titik-titik fitur yang stabil, *watermark* disisipkan pada area-area gambar yang relatif tahan terhadap modifikasi, sehingga tetap dapat dipertahankan meskipun citra mengalami serangan. Metode ini juga menggunakan *Zernike moments* tingkat rendah untuk menjaga agar *watermark* tetap tersembunyi (*imperceptible*), sehingga kualitas visual gambar hasil penyisipan tetap tinggi. Selain itu, fleksibilitas pemilihan titik fitur berdasarkan karakteristik masing-masing

gambar, yang didukung oleh kombinasi SURF dan ORB, menjadikan metode ini adaptif dan lebih kuat dalam menghadapi berbagai jenis serangan.

Kekurangan dari skema ini adalah kompleksitas komputasi yang tinggi akibat kombinasi beberapa algoritma sekaligus, yaitu SURF, ORB, *Zernike moments*, dan teknik pergeseran histogram. Kompleksitas ini dapat menjadi kendala terutama untuk aplikasi yang dijalankan pada perangkat dengan keterbatasan daya dan sumber daya komputasi. Selain itu, meskipun metode ini sangat kuat terhadap serangan geometris, ia masih menunjukkan kerentanan terhadap serangan berbasis noise seperti *Gaussian noise* dan *Speckle noise*, terutama pada level intensitas noise yang tinggi, yang ditunjukkan melalui peningkatan nilai *Bit Error Rate* (BER) dalam hasil pengujian [8].

Keterbatasan metode ini antara lain terletak pada sensitivitas terhadap pergeseran titik fitur akibat serangan yang kuat. Karena proses penyisipan dan ekstraksi sangat bergantung pada ketepatan lokasi titik-titik fitur, perpindahan titik akibat transformasi citra dapat menyebabkan kegagalan dalam ekstraksi *watermark* secara akurat. Selain itu, metode ini menghadapi dilema klasik dalam *Watermarking*, yaitu *trade-off* antara kapasitas penyisipan dan tingkat ketersembunyian. Menyisipkan *watermark* dalam jumlah besar dapat menurunkan kualitas visual citra secara signifikan. Terakhir, sebagian besar evaluasi yang dilakukan dalam penelitian ini masih berfokus pada serangan berbasis transformasi geometris dan *noise*, sehingga efektivitasnya dalam menghadapi jenis serangan lanjutan seperti kompresi ekstrem, *collage attack*, atau perusakan terstruktur belum diuji secara menyeluruh [8].

1.3.5 Skema RRW Dua Tahap Berbasis Domain Penyematan Independen

Keunggulan dari metode ini terletak pada pendekatannya yang membagi proses penyisipan *watermark* ke dalam dua domain frekuensi secara independen menggunakan Transformasi Haar. Transformasi ini memisahkan gambar ke dalam domain frekuensi rendah dan tinggi, di mana *watermark* yang bersifat *robust* disisipkan pada frekuensi rendah agar tahan terhadap kompresi dan gangguan umum, sedangkan *watermark* yang *reversible* disisipkan pada frekuensi tinggi untuk meminimalkan distorsi terhadap citra asli [8]. Pemisahan domain ini secara strategis menjaga kualitas *watermark robust* tetap optimal, bahkan setelah dilakukan penyisipan *reversible*, sehingga mengurangi potensi interferensi antar kedua jenis *watermark*. Metode ini juga menunjukkan performa yang baik, khususnya dalam menghadapi serangan seperti kompresi JPEG dan penambahan *noise*, menjadikannya cocok untuk aplikasi yang menuntut ketahanan tinggi terhadap serangan digital.

Kekurangan dari pendekatan dua tahap ini adalah peningkatan kompleksitas komputasi. Pemisahan domain frekuensi dan proses *embedding* yang terpisah menambah beban pemrosesan, terutama saat diterapkan pada gambar dengan resolusi tinggi. Selain itu, efektivitas metode ini dalam menghadapi serangan geometris seperti rotasi dan skala cenderung terbatas, karena *watermark* yang disisipkan sangat bergantung pada struktur frekuensi gambar yang sensitif terhadap perubahan geometris.

Keterbatasan dari metode ini berkaitan dengan karakteristik citra yang digunakan. Pada gambar yang memiliki banyak tekstur atau detail visual yang kompleks, performa metode dapat menurun karena area *embedding* di domain frekuensi tinggi lebih rentan terhadap distorsi visual. Selain itu, kapasitas penyisipan *watermark* juga bergantung pada struktur frekuensi citra. Artinya, jumlah data yang dapat disisipkan terutama di domain frekuensi tinggi menjadi terbatas, sehingga membatasi fleksibilitas metode dalam mengakomodasi *watermark* berukuran besar.

1.4 Tujuan Capstone Design

Tujuan dari *Capstone Design* ini adalah untuk merancang dan mengimplementasikan sebuah sistem *Watermarking* digital yang bersifat *robust* dan *reversible* guna melindungi citra digital dari penyalahgunaan dan manipulasi. Sistem yang dikembangkan menggabungkan dua pendekatan utama, yaitu *Spread Spectrum* berbasis *Slantlet Transform* (SLT) dan *Screen-Shooting Resilient Watermarking* berbasis *Scalling Factor embedding*, *Improved SIFT* (I-SIFT), dan *Discrete Cosine Transform* (DCT).

Dengan memanfaatkan dua pendekatan tersebut, sistem ini diharapkan mampu menyisipkan *watermark* secara tersembunyi tanpa menurunkan kualitas citra secara signifikan, serta mampu mengekstrak kembali *watermark* bahkan setelah citra mengalami berbagai bentuk serangan, termasuk *screen shooting*.

Adapun tujuan khusus dari proyek ini adalah sebagai berikut:

- Merancang sistem *Watermarking digital* yang tahan terhadap berbagai jenis serangan seperti *noise*, kompresi, dan transformasi geometris.
- Mengembangkan metode penyisipan *watermark* berbasis SLT yang mendukung pemulihan citra asli secara utuh (*reversible*).
- Menerapkan metode deteksi fitur I-SIFT dan *embedding* DCT untuk menghadapi serangan *screen shooting* secara *robust*.

- Membangun antarmuka pengguna berbasis MATLAB GUI untuk memudahkan proses *embedding*, transformasi perspektif, ekstraksi, dan evaluasi *watermark*.
- Mengevaluasi performa sistem dengan metrik kuantitatif seperti *Peak Signal-to-Noise Ratio* (PSNR), *Bit Error Rate* (BER), dan CRC (*Cyclic Redundancy Check*).
- Memberikan kontribusi akademik dan praktis dalam bidang keamanan data visual, khususnya pada perlindungan hak cipta citra digital.

1.5 Batasan *Capstone Design*

Dalam pelaksanaan proyek *Capstone Design* ini, terdapat beberapa batasan yang ditetapkan agar fokus pengembangan tetap terarah dan dapat diselesaikan dalam waktu yang tersedia. Batasan-batasan tersebut adalah sebagai berikut:

- Sistem hanya diujikan pada citra digital *grayscale* dengan resolusi tetap 512×512 piksel, sesuai standar pengujian citra digital *Watermarking*.
- Metode *Watermarking* yang digunakan terbatas pada dua pendekatan utama: *Spread Spectrum* berbasis SLT dan *Screen-Shooting Resilient Watermarking* menggunakan I-SIFT + DCT serta *embedding* adaptif berdasarkan parameter *Scalling Factor*.
- Implementasi dilakukan sepenuhnya di lingkungan MATLAB *Desktop*, tanpa integrasi ke platform *mobile*, *website*, atau *cloud*.
- Proses koreksi perspektif pada metode *Screen shooting* dilakukan secara manual melalui klik empat titik sudut oleh pengguna.
- Sistem belum mendukung *Watermarking* pada video.
- Evaluasi performa sistem dibatasi pada tiga metrik utama, yaitu PSNR untuk *imperceptibility*, BER untuk akurasi ekstraksi, dan CRC untuk validasi integritas data.
- Pengujian serangan terbatas pada jenis serangan digital umum seperti kompresi JPEG, *Gaussian Noise*, *Salt and Pepper Noise*, rotasi, *scaling*, dan *Screen shooting*, tanpa mencakup serangan lanjutan seperti *cropping* ekstrem atau manipulasi *mosaic*.