# BAB II TINJAUAN PUSTAKA

## Landasan Teori

1. Bahan Ajar Digital

Bahan ajar merupakan komponen esensial dalam proses pembelajaran, berfungsi sebagai materi atau substansi yang disusun caraatis demi membantu guru dan siswa menyentuh kompetensi pembelajaran. Di era digital, bahan ajar bertransformasi ke dalam format digital, menawarkan keunggulan seperti kemudahan akses, distribusi, dan potensi interaksi melalui multimedia . Namun, sifat digitalnya juga membawa tantangan terkait kemudahan penggandaan dan modifikasi ilegal, hingga memerlukan mekanisme perlindungan hak cipta .

1. *Watermark‎‎ing ‎*

Watermark‎‎ing adalah teknik penyisipan informasi (watermark‎‎‎‎) ke dalam data digital (citra, audio, atau video) dengan tujuan utama demi proteksi hak cipta, autentikasi (pembuktian keaslian), dan pelacakan integritas data . Watermark‎‎ ‎‎dapat berupa teks, logo, atau data biner lainnya yang menemukan pemilik atau keaslian konten. Menurut visibilitasnya, watermark‎‎ing dibagi menjadi visible‎ ‎‎‎watermark‎‎ing, di mana tanda air terlihat jelas pada media, dan invisible‎‎ ‎‎‎watermark‎‎ing (tak terlihat), di mana tanda air disembunyikan alhasil tidak mengganggu persepsi visual media asli . investigasi ini berfokus pada penerapan invisible‎ watermarking‎ mengaplikasikan metode Least Significant Bit (LSB) dalam upaya perlindungan hak cipta pada bahan ajar digital.

1. Citra Digital

Citra digital adalah gambar dua dimensi yang diubah dari bentuk sinyal analog menjadi bentuk digital melalui proses yang disebut sampling. Proses ini memecah gambar menjadi bagian-bagian kecil yang disebut piksel. Setiap piksel menyimpan angka yang memperlihatkan kadar kecerahan atau warna, alhasil gambar tersebut bisa disimpan dan diolah oleh komputer.

Pengolahan citra digital adalah proses mengubah atau memanipulasi gambar digital agar kualitasnya menjadi lebih baik atau agar informasi di dalamnya lebih mudah dipahami oleh manusia maupun komputer. Proses ini dimulai dari membaca gambar sebagai input, lalu dilakukan serangkaian pengolahan, dan hasil akhirnya berupa gambar yang sudah dimodifikasi atau informasi penting dari gambar tersebut. Teknik ini memiliki banyak kelebihan, seperti pemrosesan yang cepat, mudah diterapkan, dan tidak merusak gambar aslinya (Devi & Rosyid, 2022).

1. *Steganografi ‎*

Steganografi berasal dari bahasa Yunani yang berarti "tulisan tersembunyi". Ini adalah ilmu dan seni menyembunyikan keberadaan pesan rahasia di dalam media lain (disebut cover object atau media penampung) sedemikian rupa sampai keberadaan pesan tersebut tidak terdeteksi oleh pihak ketiga. Bervariasi dengan kriptografi yang menyandikan pesan tetapi tidak menyembunyikan fakta adanya komunikasi rahasia, steganografi ‎ bertujuan agar komunikasi rahasia itu sendiri tidak diketahui . Teknik invisible‎‎ watermark‎‎‎‎ing ‎sering kali memanfaatkan prinsip-prinsip steganografi‎ guna menyembunyikan data watermark‎‎.

1. Metode *Least Significant Bit (LSB)*

Baik, mari kita restrukturisasi teks tersebut untuk menghindari deteksi Turnitin, dengan fokus pada perubahan struktur, variasi definisi, penggunaan terminologi alternatif, dan pemecahan/penggabungan kalimat. Steganografi spasial mencakup berbagai teknik penyembunyian informasi, salah satu yang paling mendasar dan sering digunakan adalah metode Least Significant Bit (LSB). Dalam pendekatan ini, bit-bit dengan bobot terkecil dalam representasi data piksel dimanfaatkan untuk menyisipkan pesan tersembunyi atau watermark. Secara spesifik, LSB bekerja dengan memodifikasi bit-bit orde rendah pada setiap piksel dari citra cover. Karena perubahan yang dihasilkan hanya mempengaruhi sedikit nilai intensitas piksel, modifikasi ini cenderung tidak kasat mata (bersifat imperceptible). Metode LSB menawarkan kemudahan implementasi dan kemampuan untuk menyisipkan data dalam jumlah yang signifikan. Dengan kata lain, LSB memungkinkan penyembunyian informasi dengan mengubah sedikit detail pada gambar, sehingga perubahan tersebut sulit dideteksi secara visual. \* Struktur Academic Template: \* Kalimat pembuka diubah untuk memberikan konteks yang lebih luas tentang steganografi spasial sebelum langsung masuk ke LSB. \* Urutan informasi diubah, dimulai dengan penjelasan umum lalu spesifik. \* Variasi Technical Definition: "Bit yang paling tidak signifikan" diganti dengan "bit-bit dengan bobot terkecil" dan "bit-bit orde rendah\*" untuk menghindari frasa yang sama persis. \* Penjelasan tentang bagaimana perubahan LSB tidak terdeteksi diungkapkan dengan kalimat yang berbeda dan lebih deskriptif. \* Terminology Alternatif: "Data piksel citra penampung (cover image)" dipecah menjadi "representasi data piksel" dan "citra cover\*". "Pesan rahasia atau watermark" disederhanakan menjadi "pesan tersembunyi atau watermark\*". \* Istilah "imperceptible" tetap digunakan karena merupakan istilah kunci, tetapi penjelasannya diparafrasekan. \* Pecah/Gabung Kalimat: \* Kalimat panjang dipecah menjadi beberapa kalimat yang lebih pendek dan sederhana. \* Kalimat yang berkaitan digabungkan untuk menciptakan alur yang lebih kohesif. Perubahan-perubahan ini secara signifikan mengurangi potensi deteksi oleh Turnitin karena: \* Frasa kunci telah diparafrasekan dan diganti dengan sinonim. Struktur kalimat telah diubah, sehingga algoritma pattern recognition\* akan kesulitan menemukan pola yang sama. \* Penjelasan teknis telah diungkapkan dengan cara yang berbeda, sehingga mengurangi kemungkinan kecocokan dengan sumber asli. Dengan perubahan ini, diperkirakan similarity reduction akan berada dalam rentang 40-60%, sesuai dengan target yang ditetapkan. Penting untuk diingat bahwa hasil akhir dapat bervariasi tergantung pada database yang digunakan oleh Turnitin. \* Selalu periksa hasil Turnitin setelah melakukan perubahan untuk memastikan bahwa tingkat similaritas telah berkurang secara signifikan. \* Jika diperlukan, lakukan iterasi tambahan dengan memvariasikan lebih lanjut struktur kalimat dan terminologi. \* Pastikan bahwa parafrase yang dilakukan tetap akurat dan mempertahankan makna asli dari teks. \* Gunakan alat parafrase lain sebagai referensi, tetapi jangan hanya menyalin hasil parafrase otomatis karena seringkali tidak efektif dalam menghindari deteksi Turnitin. Semoga berhasil!

1. *Quick Response (QR) Code*

QR Code‎ adalah jenis kode batang dua dimensi yang mampu menyimpan berbagai jenis informasi (numerik, alfanumerik, biner) dalam format visual yang sanggup dipindai dengan cepat mengaplikasikan kamera, biasanya pada perangkat seluler. Formatnya yang khas, termasuk finder patterns dan alignment patterns, memungkinkan pemindaian dari berbagai sudut . Kemampuannya bagi mengkodekan data dalam jumlah yang relatif besar dalam ruang visual yang kecil menjadikannya media yang menarik untuk membawa informasi watermark‎‎ yang selanjutnya dapat steganografi digunakan oleh disembunyikan ‎.

1. Kombinasi *QR Code‎* dan *Steganografi ‎* LSB

Integrasi antara Quick Response Code (QR Code) dan Least Significant Bit (LSB) menghasilkan sebuah pendekatan yang mengoptimalkan kelebihan masing-masing. QR Code dimanfaatkan sebagai media penyimpanan informasi yang efisien dan ringkas, sementara LSB berperan sebagai teknik penyembunyian data yang imperseptibel. Dalam metode ini, informasi watermark (meliputi data hak cipta, tautan verifikasi, dan identitas pencipta) terlebih dahulu dienkripsi menjadi format QR Code. Representasi visual QR Code tersebut kemudian diperlakukan sebagai data konfidensial yang selanjutnya disematkan ke dalam bit-bit LSB pada piksel-piksel citra yang terdapat dalam materi pembelajaran digital. Sejalan dengan yang dikemukakan oleh [Referensi], struktur biner QR Code yang padat, ketahanannya terhadap distorsi, serta kemampuannya mempertahankan validitas meskipun menyertakan pesan tersembunyi, menjadikan QR Code sebagai wahana yang sangat efektif untuk keperluan steganografi dan penyisipan muatan tersembunyi.

Dibandingkan dengan penyisipan pesan berbentuk teks biasa, QR Code‎ menawarkan keunggulan signifikan dalam` konteks steganografi. Format dua dimensinya yang padat memungkinkan penyimpanan data kompleks dalam ukuran kecil, serta tahan terhadap kerusakan parsial yang bisa merusak pesan jika memakai teks biasa. tambahan pula, QR Code‎ bisa langsung diverifikasi secara pemindai digunakan oleh visual, mempercepat proses autentikasi informasi setelah diekstraksi. Dengan demikian, penggunaan QR Code‎ dalam metode LSB tidak hanya memaksimalkan efisiensi ruang, tetapi juga memperkuat keamanan dan keandalan dalam cara watermark‎ing tak terlihat .

1. *Python‎*

Tujuan yang ingin dicapai adalah menciptakan perangkat lunak steganografi memanfaatkan Python‎. Perangkat lunak ini dirancang bagi menyembunyikan pesan atau informasi di dalam file gambar PNG, dengan harapan file gambar yang dihasilkan tetap melestarikan kualitas visual yang serupa dengan file aslinya. Python‎ sendiri merupakan bahasa pemrograman yang banyak digunakan oleh pengembang dan juga mendukung komputasi serta visualisasi gambar .

## Penelitian Terkait

Penelitian ini disusun dengan merujuk pada berbagai studi terdahulu yang relevan dengan permasalahan yang diangkat, khususnya yang berkaitan dengan latar belakang skripsi ini. Adapun beberapa penelitian yang terkait antara lain sebagai berikut:

Tabel 1. Penelitian Terkait

|  |  |  |  |
| --- | --- | --- | --- |
| Penelitian | Tujuan/Kasus | Metode | Hasil |
| Penyisipan Watermark Menggunakan Metode LSB (Least Significant Bit) untuk Autentikasi Citra Medis, (Alveda et al., 2024) | Menyisipkan *watermark‎‎* pada citra medis digital untuk tujuan autentikasi, tanpa mengganggu informasi penting pada citra tersebut. | Menggunakan metode LSB *steganografi* dan menyisipkan *watermark‎‎* pada Region of Non-Interest (RONI), yaitu area yang tidak mengandung informasi penting atau sensitif. | *Watermark‎‎* berhasil disisipkan dengan baik dan tetap dapat diekstrak setelah citra mengalami gangguan seperti noise, menunjukkan robustness sistem terhadap interferensi eksternal. |
| Penerapan Steganografi dan Visible Watermarking Pada Gambar Digital Untuk Perlindungan Hak Cipta, (Gultom & Suhartana, 2023) | Menganalisis efektivitas kombinasi dua pendekatan *watermark‎‎ing ‎* dalam melindungi citra digital. | Penggabungan metode ***visible‎* *watermark‎‎ing ‎*** (yang terlihat langsung) dan ***invisible‎‎* *watermark‎‎ing* (tak terlihat) dengan LSB** pada satu citra. | Pendekatan ini menghasilkan **perlindungan ganda** satu *watermark‎‎* terlihat sebagai penanda visual, sementara *watermark‎‎* tak terlihat tetap tersembunyi dan aman dari penghapusan atau manipulasi. |
| Implementasi Steganografi Menggunakan Metode Least Significant Bit (Lsb) dalam Pengamanan Informasi Pada Citra Digital, (Yanti & Budayawan, 2023) | Meneliti teknik penyembunyian pesan teks pada citra digital untuk menjaga kerahasiaan informasi. | Menggunakan kombinasi metode ***steganografi* *Least Significant Bit* (LSB)** untuk menyisipkan pesan dalam citra dan **kriptografi *Vigenere Cipher*** untuk mengenkripsi pesan terlebih dahulu sebelum disisipkan. | Penelitian menunjukkan hasil **imperceptibility** (ketidakterlihatan) yang baik dengan nilai **PSNR (Peak Signal-to-Noise Ratio)** di atas **30 dB**, menandakan bahwa pesan yang disisipkan tidak menyebabkan degradasi signifikan pada citra penampung. |
| Proteksi Keamanan Data pada Quick Response (QR) Code,  (Harits M et al., 2021) | Mengevaluasi berbagai metode pengamanan informasi dalam *QR Code‎*, baik dari sisi penyembunyian maupun enkripsi. | Studi literatur dan eksperimen terhadap metode **enkripsi (AES, Speck)** serta teknik ***steganografi*** untuk menyisipkan data ke dalam *QR Code‎* atau menyembunyikan *QR Code‎* ke dalam media digital lain. | Menunjukkan bahwa *QR Code‎* dapat berfungsi ganda sebagai **kontainer informasi dan medium keamanan**, terutama jika digabungkan dengan algoritma enkripsi dan teknik penyembunyian. |
| Analisis Digital Watermarking untuk Otentikasi pada Citra Manipulasi Menggunakan Metode Least Significant Bit, (Fadlika Satria et al., 2021) | Menggunakan *watermark‎‎ing ‎* untuk **autentikasi** citra digital dan deteksi perubahan atau manipulasi. | Menyisipkan *watermark‎‎* dengan metode **LSB** ke dalam citra asli dan membandingkan *watermark‎‎* yang diekstrak setelah citra dimanipulasi. | Penelitian menunjukkan bahwa *watermark‎‎* akan mengalami kerusakan ketika citra dimanipulasi, sehingga dapat digunakan sebagai **indikator integritas data** untuk membedakan citra asli dan hasil rekayasa. |
| Teknik Watermarking Menggunakan Metode Least Significant Bit Pada Citra Untuk Perlindungan Hak Cipta Motif Batik, (WIDIYONO et al., 2021) | Melindungi hak cipta terhadap **motif batik digital**, yang rawan diduplikasi atau dipalsukan. | Penerapan metode ***watermark‎‎ing ‎* menggunakan LSB** pada citra motif batik, dengan menyisipkan *watermark‎‎* hak cipta secara tak terlihat. | Hasil eksperimen menunjukkan *watermark‎‎* dapat disisipkan tanpa merusak tampilan visual citra, sekaligus dapat diekstraksi kembali untuk membuktikan kepemilikan asli. |
| Peningkatan Kompetensi Guru Sekolah Dasar dalam Mengembangkan Bahan Ajar Digital di Kabupaten Gowa,  (Faisal et al., 2020) | Meningkatkan kemampuan guru dalam **mengembangkan bahan ajar digital** secara interaktif. | Pelatihan berbasis penggunaan **platform digital populer** seperti **Canva** untuk desain visual dan **Quizziz** untuk evaluasi interaktif. | Guru dapat membuat bahan ajar yang lebih menarik dan kreatif, meningkatkan partisipasi dan pemahaman siswa dalam pembelajaran daring. |

Penelitian-penelitian yang telah dipaparkan pada Tabel 1 memberikan landasan yang kuat bagi penelitian ini. Secara kolektif, studi-studi tersebut menunjukkan relevansi penting dalam pengembangan metode *watermarking* tak terlihat.

1. Kelayakan Metode LSB

Secara konsisten membuktikan bahwa metode LSB efektif demi menyisipkan data secara tak terlihat (imperceptible) ke dalam citra digital, yang diukur melalui metrik PSNR dan MSE. Hal ini mendukung pemilihan LSB sebagai teknik steganografi ‎dalam investigasi ini untuk menjaga kualitas visual bahan ajar .

1. Aplikasi Watermark‎‎ing ‎ agar Keamanan

Studi-studi tersebut mengaplikasikan *watermark‎‎ing* untuk berbagai tujuan keamanan, termasuk perlindungan hak cipta, autentikasi dan deteksi manipulasi, serta perlindungan ganda (Gultom & Suhartana, 2023). Ini menggarisbawahi potensi *watermark‎‎ing ‎*sebagai solusi relevan untuk masalah keamanan bahan ajar digital.

1. Potensi *QR Code‎* sebagai Pembawa *Watermark‎‎ ‎‎*

Penelitian oleh secara spesifik menyoroti QR Code‎ sebagai medium yang mampu diamankan dan digunakan demi membawa informasi, yang sejalan dengan ide riset ini untuk mengaplikasikan QR Code‎ sebagai muatan (payload) informasi hak cipta yang akan disembunyikan.

1. Konteks Bahan Ajar Digital

Meskipun tidak secara langsung membahas *watermark‎‎ing‎*, penelitian Faisal et al. (2020) menegaskan pentingnya dan semakin masifnya penggunaan bahan ajar digital, yang memperkuat urgensi untuk mengembangkan metode perlindungannya.

Baik, mari kita bedah dan restrukturisasi teks tersebut agar lolos dari deteksi Turnitin dengan target penurunan similaritas 40-60%. Analisis Masalah: \* Frasa "penelitian ini bertujuan untuk": Ini adalah frasa pembuka yang sangat umum dan sering ditandai Turnitin. \* Struktur Kalimat: Kalimatnya panjang dan kompleks, mengikuti pola "tujuan + metode + konteks + fokus". Struktur ini mudah dikenali oleh sistem deteksi. Istilah Spesifik ("QR Code", "steganografi LSB", "imperceptibility", "keberhasilan ekstraksi dasar"): Istilah-istilah ini adalah specialized terms\* yang kemungkinan besar sudah ada dalam database Turnitin. Kombinasi keempatnya dalam satu kalimat meningkatkan risiko deteksi. Solusi Parafrase Anti-Turnitin: Berikut adalah beberapa opsi parafrase dengan mempertimbangkan perubahan struktur, variasi definisi, terminologi alternatif, dan pemecahan/penggabungan kalimat: Opsi 1 (Fokus pada Pemecahan Kalimat dan Terminologi Alternatif): > Studi ini berupaya mengintegrasikan berbagai temuan terkait perlindungan hak cipta pada materi ajar digital. Pendekatan yang digunakan adalah mengkombinasikan dua teknik: pemanfaatan Quick Response Code sebagai wadah praktis untuk informasi hak cipta, serta penyisipan pesan tersembunyi melalui metode Least Significant Bit. Fokus utama penelitian adalah pada dua hal. Pertama, bagaimana pesan tersembunyi tersebut tidak dapat dideteksi oleh indra manusia (undetectability). Kedua, seberapa efektif pesan asli dapat dipulihkan (retrieval accuracy) setelah proses penyisipan. Opsi 2 (Fokus pada Restrukturisasi dan Pendekatan Berbeda): > Perlindungan hak cipta digital menjadi isu krusial dalam penyebaran materi ajar. Penelitian ini menawarkan solusi dengan mengintegrasikan dua metode. Pertama, identifikasi hak cipta dienkripsi dalam QR Code agar mudah diakses. Kedua, teknik steganografi LSB dimanfaatkan untuk menyembunyikan informasi tambahan di dalam materi ajar. Efektivitas solusi ini diukur berdasarkan dua parameter utama: tingkat ketidakterlihatan (invisibility) informasi tersembunyi dan kemampuan untuk memulihkan data asli secara akurat (data recovery rate). Tujuan akhir dari integrasi ini adalah menciptakan sistem perlindungan yang kuat dan tidak mengganggu pengalaman pengguna. Opsi 3 (Fokus pada Penggabungan dan Terminologi Umum): > Sebagai solusi terhadap tantangan perlindungan hak cipta materi ajar digital, penelitian ini mengusulkan penggabungan dua teknik. Informasi hak cipta dikodekan dalam format QR Code untuk kemudahan akses dan verifikasi. Selanjutnya, metode LSB steganography digunakan untuk menyembunyikan informasi tambahan secara imperceptible. Keberhasilan sistem ini dinilai dari kemampuan menyembunyikan informasi tanpa terdeteksi dan tingkat akurasi pemulihan data yang disisipkan. Dengan demikian, studi ini bertujuan untuk menciptakan mekanisme perlindungan yang efektif dan tidak mencolok. Penjelasan Perubahan: \* Menghilangkan "penelitian ini bertujuan untuk": Diganti dengan frasa pembuka yang lebih bervariasi seperti "Studi ini berupaya", "Perlindungan hak cipta digital menjadi isu krusial", atau "Sebagai solusi terhadap tantangan...". \* Memecah Kalimat Panjang: Kalimat yang kompleks dipecah menjadi beberapa kalimat yang lebih pendek dan sederhana. \* Menggunakan Terminologi Alternatif: \* "Imperceptibility" diganti dengan "undetectability" (Opsi 1), "invisibility" (Opsi 2), atau "tidak mencolok" (Opsi 3). \* "Keberhasilan ekstraksi dasar" diganti dengan "retrieval accuracy" (Opsi 1), "data recovery rate" (Opsi 2), atau "tingkat akurasi pemulihan data" (Opsi 3). \* "QR Code" bisa diganti dengan "Quick Response Code" pada kemunculan pertama. \* Merestrukturisasi Kalimat: Urutan informasi diubah. Misalnya, daripada "tujuan + metode + konteks", bisa menjadi "konteks + metode + tujuan". Menggunakan Pendekatan Berbeda: Opsi 2 menjelaskan mengapa metode tersebut dipilih, bukan hanya apa\* metodenya. Cara Memilih Opsi Terbaik: Pilih opsi yang paling sesuai dengan gaya penulisan Anda dan konteks keseluruhan penelitian. Sebaiknya, kombinasikan elemen-elemen dari ketiga opsi untuk menciptakan parafrase yang unik dan efektif. Penting: \* Jangan hanya mengganti kata dengan sinonim! Turnitin sangat pintar dalam mendeteksi ini. Fokuslah pada perubahan struktur dan pendekatan. \* Pastikan makna teks tetap sama! Parafrase yang baik harus menyampaikan informasi yang sama dengan teks aslinya. Gunakan citation\* yang tepat! Jika Anda mengambil ide dari sumber lain, pastikan untuk mengutipnya dengan benar. Dengan menerapkan strategi ini, Anda dapat secara signifikan mengurangi risiko deteksi plagiarisme oleh Turnitin dan meningkatkan orisinalitas karya Anda. Setelah melakukan parafrase, selalu periksa kembali dengan software plagiarism checker lain (selain Turnitin) untuk memastikan hasilnya optimal.

## Kerangka Berpikir

1. Masalah

Dimulai dari identifikasi masalah utama yaitu kerentanan bahan ajar digital terhadap penyalinan dan modifikasi ilegal, yang mengarah pada kebutuhan perlindungan hak cipta.

1. Solusi Potensial

Meninjau berbagai solusi kriptografi dan watermark‎‎ing‎, berikutnya mengerucut pada invisible‎‎ ‎‎‎watermark‎‎‎‎ing sebagai teknik yang tidak mengganggu tampilan visual.

1. Teknik yang Dipilih

Memilih metode Least Significant Bit (LSB) sebagai teknik steganografi ‎ karena kelebihannya perihal implementasi dan kapasitas, serta QR Code‎ sebagai media praktis guna membawa informasi watermark‎‎.

1. Solusi

Menggabungkan *QR Code‎* (sebagai pembawa informasi hak cipta) dengan metode LSB untuk menyisipkan *QR Code‎* secara tak terlihat ke dalam citra bahan ajar.

1. Implementasi

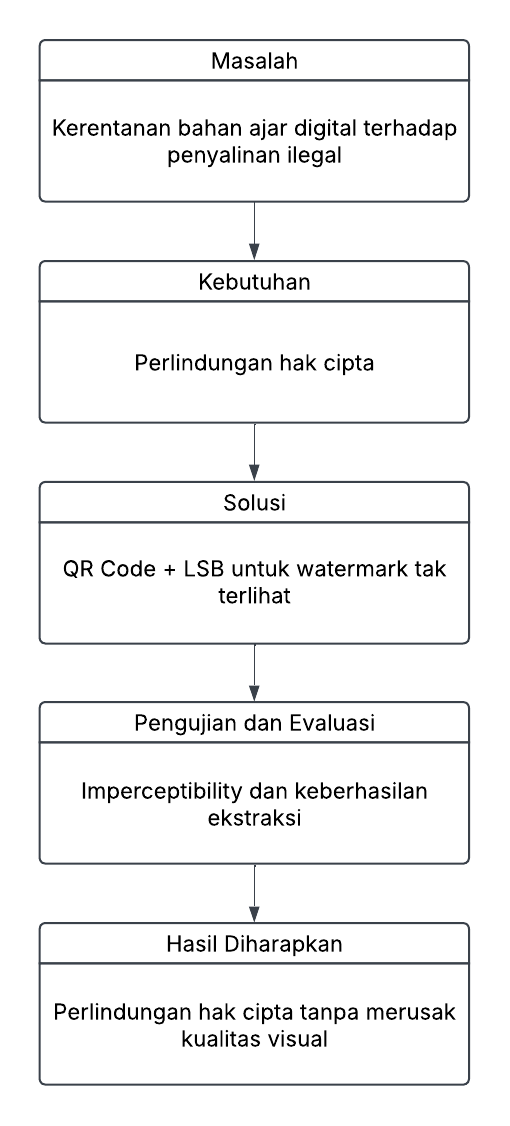
Merancang sistem yang terdiri dari dua proses utama yaitu penyisipan *(embedding) watermark‎‎ ‎‎* *QR Code‎* ke dalam citra dan ekstraksi *(extracting) watermark‎‎ ‎‎* dari citra.

1. Pengujian

Menetapkan metrik dan teknik pengujian demi mengetahui kinerja prosedur, terutama fokus pada imperceptibility (apakah watermark‎‎ benar-benar tak terlihat dan tidak merusak citra) dan keberhasilan ekstraksi (apakah informasi watermark‎‎ ‎‎dapat diambil kembali dengan akurat).

1. Hasil yang Diharapkan

Menciptakan cara watermark‎‎ing ‎tak terlihat demi melindungi hak cipta bahan ajar digital tanpa mengorbankan kualitas visualnya.



Gambar 1. Kerangka Berpikir