

**ANALISIS FORENSIK DIGITAL UNTUK VERIFIKASI KEASLIAN
BUKTI TRANSAKSI PEMBAYARAN QRIS MENGGUNAKAN
ALGORITMA HASH SHA-256 SEBAGAI
UPAYA DETEKSI MANIPULASI DOKUMEN DIGITAL**

SKRIPSI

DISUSUN OLEH

ADIBAH SALSABILAH

NPM. 2209010064



**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN
2026**

**ANALISIS FORENSIK DIGITAL UNTUK VERIFIKASI KEASLIAN
BUKTI TRANSAKSI PEMBAYARAN QRIS MENGGUNAKAN
ALGORITMA HASH SHA-256 SEBAGAI
UPAYA DETEKSI MANIPULASI DOKUMEN DIGITAL**

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Sistem
Informasi (S.I) dalam Program Studi Sistem Informasi pada Fakultas Ilmu
Komputer dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara**

ADIBAH SALSABILAH

2209010064

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA**

MEDAN

2026

LEMBAR PENGESAHAN

Judul Skripsi : ANALISIS FORENSIK DIGITAL UNTUK
VERIFIKASI KEASLIAN BUKTI TRANSAKSI
PEMBAYARAN QRIS MENGGUNAKAN
ALGORITMA HASH SHA-256 SEBAGAI
UPAYA DETEKSI MANIPULASI DOKUMEN
DIGITAL

Nama Mahasiswa : ADIBAH SALSABILLAH
NPM : 2209010064
Program Studi : SISTEM INFORMASI

Menyetujui
Komisi Pembimbing



(Mahardika Abdi Prawira Tanjung, M.Kom)
NIDN. 0117088902

Ketua Program Studi



(Mahardika Abdi Prawira Tanjung, S.Kom.,
M.Kom)
NIDN. 0117088902



(Dr. Al-Khadzraji, S.Kom., M.Kom.)
NIDN. 0120099201

PERNYATAAN ORISINALITAS

ANALISIS FORENSIK DIGITAL UNTUK VERIFIKASI KEASLIAN BUKTI TRANSAKSI PEMBAYARAN QRIS MENGGUNAKAN ALGORITMA HASH SHA-256 SEBAGAIUPAYA DETEKSI MANIPULASI DOKUMEN DIGITAL

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, 17 Mei 2026

Yang membuat pernyataan



Adibah Salsabilah

NPM. 2209010064

**PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN
AKADEMIS**

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Adibah Salsabilah
NPM	: 2209010064
Program Studi	: Sistem informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif (*Non-Exclusive Royalty free Right*) atas penelitian skripsi saya yang berjudul:

**ANALISIS FORENSIK DIGITAL UNTUK VERIFIKASI KEASLIAN
BUKTI TRANSAKSI PEMBAYARAN QRIS MENGGUNAKAN
ALGORITMA HASH SHA-256 SEBAGAIUPAYA DETEKSI
MANIPULASI DOKUMEN DIGITAL**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, 19 Mei 2026

Yang membuat pernyataan



Adibah Salsabilah

NPM. 2209010064

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap : Adibah Salsabilah
Tempat dan Tanggal Lahir : Bp.Mandoge, 01 Agustus 2004
Alamat Rumah : G2 Plasmen, Dusun X, Bp.Mandoge
Telepon/Faks/HP : 0821-8141-9395
E-mail : adibahsalsabilah0811@gmail.com
Instansi Tempat Kerja : -
Alamat Kantor : -

DATA PENDIDIKAN

SD	: SDN 016402 BANDAR PASIR MANDOG	TAMAT: 2016
SMP	: SMP SWASTA PTPN IV BP.MANDOG	TAMAT: 2019
SMA	: SMA SWASTA UMUM SENTOSA	TAMAT: 2022

KATA PENGANTAR



Puji syukur alhamdulillah penulis ucapkan kehadiran Allah SWT yang telah melimpahkan rahmat, hidayah, serta karunia-Nya kepada penulis sehingga penulis dapat menyelesaikan skripsi ini. Skripsi merupakan salah satu persyaratan bagi setiap mahasiswa yang ingin menyelesaikan studinya di Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara. Sehubungan dengan ini, disusun skripsi yang berjudul **“ANALISIS FORENSIK DIGITAL UNTUK VERIFIKASI KEASLIAN BUKTI TRANSAKSI PEMBAYARAN QRIS MENGGUNAKAN ALGORITMA HASH SHA-256 SEBAGAIUPAYA DETEKSI MANIPULASI DOKUMEN DIGITAL”**.

Dengan selesainya skripsi ini, penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. Akrim, M.Pd selaku Rektor Universitas Muhammadiyah Sumatera Utara.
2. Bapak Dr. Al - Khowarizmi, S.Kom., M.Kom selaku Dekan Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara.
3. Ibu Dr.Firahmi Rizky, S.Kom., M.Kom selaku Wakil Dekan I dan,
4. Bapak Mhd. Basri, S.Si, M.Kom selaku Wakil Dekan III Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera

Utara.

5. Bapak Mahardika Abdi Prawira Tanjung, S.Kom., M.Kom selaku Ketua Prodi Sistem Informasi dan selaku Dosen Pembimbing skripsi saya yang telah memberikan dorongan, bimbingan dan arahan sehingga skripsi ini selesai.
6. Bapak Mulkan Azhari, S.Kom, M.Kom selaku Sekretaris Prodi Sistem Informasi Universitas Muhammadiyah Sumatera Utara.
7. Teruntuk cinta pertamaku sekaligus penyemangat penulis Ayahanda tercinta, Suratman. Terimakasih atas segala doa, kasih sayang, dan cinta yang tulus, serta perjuangan ayah yang tidak pernah lelah demi putri sulungmu ini. Meskipun ayah tidak sempat merasakan bangku perkuliahan, namun dengan kerja keras, pengorbanan, dan ketulusan hati, ayah mampu mengantarkan putri sulungmu hingga merasakan pendidikan yang memadai sampai pada tahap ini. Setiap langkah yang penulis tempuh tidak lepas dari dukungan, dan doa ayah.
8. Teruntuk bidadari surgaku ibunda tercinta, Septiana Rezky. Terimakasih atas cinta yang tidak pernah putus, doa yang selalu mengiringi setiap langkah, serta pengorbanan yang begitu besar demi masa depan anak-anakmu. Ibu selalu menjadi tempat pulang yang paling menenangkan, sumber kekuatan, serta penyemangat ketika penulis merasa lelah dalam menjalani proses perkuliahan hingga penyusunan skripsi ini.
9. Teruntuk cinta kasihku adik-adikku, Alfiyah Hafizah dan Muhammad Oktri Haziq. Terimakasih sudah memberikan tawa dan canda yang begitu

hangat disaat penulis merasa lelah. Penulis sangat menyayangi kalian adik-adikku.

10. Teruntuk nenekku tersayang, Irianseh dan kakekku tersayang Selamat.

Terimakasih untuk setiap doa tulus yang dipanjatkan, dan perhatian kasih sayang yang tulus yang diberikan ke cucunya. Penulis sangat berharap nenek dan kakek diberi umur yang panjang agar kelak bisa melihat kesuksesan cucunya.Amin.

11. Teruntuk teman seperjuanganku, Nita Natalia dan Ayu Astuti Siregar.

Terima kasih atas kebersamaan, dukungan, serta semangat yang selalu diberikan selama menjalani masa perkuliahan hingga proses penyusunan skripsi ini. Banyak cerita, tawa, serta perjuangan yang telah kita lalui bersama, yang menjadi kenangan berharga dalam perjalanan ini. Semoga pertemanan ini, tetap terjaga, penuh kenangan indah, dan menjadi bagian berharga dalam perjalanan hidup kita kedepannya.

Sebagai manusia biasa penulis menyadari penyusunan skripsi ini jauh dari kata sempurna. Oleh karena itu, atas kesalahan kekurangan dalam penulisan skripsi ini, penulis memohon maaf dan bersedia menerima kritikan yang membangun.

Terakhir, harapan penulis, semoga skripsi ini dapat memberikan manfaat bagi siapa saja yang membacanya.

Medan,18 April 2026

Penyusun,

Adibah Salsabilah

ABSTRAK

Perkembangan sistem pembayaran digital melalui *Quick Response Code Indonesian Standard* (QRIS) memberikan kemudahan dalam transaksi non-tunai, namun juga menimbulkan potensi penyalahgunaan berupa manipulasi bukti transaksi digital. Manipulasi dapat terjadi pada elemen transaksi seperti nominal pembayaran, waktu transaksi, serta identitas pengirim dan penerima, yang sulit dideteksi secara visual. Di sisi lain, perubahan pada dokumen digital tidak selalu menunjukkan manipulasi karena dapat disebabkan oleh proses teknis seperti kompresi atau konversi format file. Permasalahan dalam penelitian ini meliputi bagaimana menganalisis elemen transaksi untuk mengidentifikasi perubahan, bagaimana perbedaan nilai hash SHA-256 antara file asli dan file yang telah dimanipulasi, serta bagaimana sistem menampilkan hasil verifikasi keaslian dokumen. Penelitian ini bertujuan untuk menganalisis elemen transaksi, menerapkan algoritma SHA-256 dalam mendeteksi perubahan dokumen, menentukan keaslian bukti transaksi, serta mengimplementasikan sistem yang mampu menampilkan hasil verifikasi. Metode yang digunakan adalah metode kuantitatif yang didukung dengan analisis elemen transaksi, di mana dilakukan perhitungan nilai hash SHA-256 terhadap file referensi dan file uji, serta perbandingan elemen transaksi yang meliputi nominal, waktu, identitas pengirim, dan penerima melalui input manual. Tahapan penelitian meliputi identifikasi masalah, pengumpulan data melalui wawancara, perancangan sistem, implementasi, dan pengujian. Hasil penelitian menunjukkan bahwa algoritma SHA-256 mampu mendeteksi perubahan pada dokumen digital melalui perbedaan nilai hash, namun tidak dapat mengidentifikasi bagian yang berubah. Oleh karena itu, analisis elemen transaksi digunakan sebagai metode pendukung untuk mengidentifikasi bagian yang mengalami perubahan. Sistem yang dikembangkan mampu menampilkan hasil verifikasi berupa informasi keaslian dokumen, apakah termasuk asli, mengalami perubahan teknis, atau manipulasi. Kesimpulan dari penelitian ini adalah bahwa kombinasi penggunaan algoritma SHA-256 dan analisis elemen transaksi dapat digunakan secara efektif dalam verifikasi keaslian bukti transaksi QRIS secara lebih akurat.

Kata Kunci: Forensik Digital, QRIS, SHA-256, Hashing, Verifikasi Dokumen, Manipulasi Digital

ABSTRACT

The development of digital payment systems through the Quick Response Code Indonesian Standard (QRIS) provides convenience in non-cash transactions, but also creates the potential for misuse in the form of manipulation of digital transaction evidence. Manipulation can occur in transaction elements such as the payment amount, transaction time, and the identity of the sender and recipient, which are difficult to detect visually. On the other hand, changes to digital documents do not always indicate manipulation because they can be caused by technical processes such as compression or file format conversion. The problems in this research include how to analyze transaction elements to identify changes, how the SHA-256 hash value differs between the original file and the manipulated file, and how the system displays the results of document authenticity verification. This research aims to analyze transaction elements, apply the SHA-256 algorithm in detecting document changes, determine the authenticity of transaction evidence, and implement a system capable of displaying verification results. The method used is a quantitative method supported by transaction element analysis, where the SHA-256 hash value is calculated for reference files and test files, and a comparison of transaction elements including the amount, time, sender and recipient identities through manual input. The research stages include problem identification, data collection through interviews, system design, implementation, and testing. The results of the study indicate that the SHA-256 algorithm is capable of detecting changes in digital documents through differences in hash values, but cannot identify the changed parts. Therefore, transaction element analysis is used as a supporting method to identify the changed parts. The developed system is able to display verification results in the form of information on the authenticity of the document, whether it is genuine, has undergone technical changes, or is manipulated. The conclusion of this study is that the combination of the SHA-256 algorithm and transaction element analysis can be used effectively to verify the authenticity of QRIS transaction evidence more accurately.

Keywords: *Digital Forensics, QRIS, SHA-256, Hashing, Document Verification, Digital Manipulation*

DAFTAR ISI

LEMBAR PENGESAHAN	i
PERNYATAAN ORISINALITAS.....	ii
PERNYATAAN PERSETUJUAN PUBLIKASI.....	iii
RIWAYAT HIDUP	iv
KATA PENGANTAR.....	v
ABSTRAK	viii
ABSTRACT	ix
DAFTAR ISI.....	x
DAFTAR TABEL	xii
DAFTAR GAMBAR.....	xiii
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	4
1.3 Batasan Masalah.....	5
1.4 Tujuan Penelitian	6
1.5 Manfaat Penelitian	6
BAB II LANDASAN TEORI	9
2.1 Forensik Digital	9
2.2 Sistem Pembayaran	9
2.3 Pembayaran Digital	11
2.4 Quick Response Code (QR Code).....	13
2.5 Algoritma Hash.....	15
2.6 Secure Hash Algorithm 256	17
2.7 Studi Terdahulu	21
2.8 UML	24
2.8.1 Use Case Diagram.....	24
2.8.2 Activity Diagram	26

2.8.3 Sequence Diagram	27
2.9 Metadata	28
2.9.1 Penerapan Metadata dalam Penelitian	28
2.10 <i>Optical Character Recognition</i> (OCR)	29
BAB III ANALISA DAN PERANCANGAN SISTEM.....	31
3.1 Analisis Permasalahan	31
3.2 Algoritma Sistem	33
3.3 Flowchart Sistem	35
3.4 Pemodelan dan Perancangan Sistem	39
3.4.1 Use Case Diagram.....	39
3.4.2 Activity Diagram	40
3.4.3 Sequence Diagram	42
3.5 Pengumpulan Data (<i>Collection</i>)	43
3.6 Rancangan UI/UX	45
BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM	51
4.1 Kebutuhan Sistem	51
4.1.1 Kebutuhan Perangkat Lunak (Software)	51
4.1.2 Kebutuhan Data	53
4.1.3 Kebutuhan Fungsional Sistem	53
4.1.4 Kebutuhan Non-Fungsional.....	54
4.2 Implementasi Sistem	54
4.3 Pengujian Sistem.....	62
4.3.1 Pengujian sistem dokumen yang terindikasi manipulasi.	62
4.3.2 Pengujian sistem dokumen yang identik/asli.....	66
4.3.3 Pengujian Blackbox Testing	70
BAB V PENUTUP	72
5.1 Kesimpulan	72
5.2 Saran.....	73
DAFTAR PUSTAKA	74
LAMPIRAN.....	78

DAFTAR TABEL

Tabel 2. 1 Inisialisasi nilai awal Hash SHA-256	18
Tabel 2. 2 Studi Terdahulu.....	21
Tabel 2. 3 Simbol-simbol Use Case Diagram.....	25
Tabel 2. 4 Simbol-simbol Activity Diagram.....	26
Tabel 2. 5 Simbol-simbol Sequence Diagram (Rusmawan, 2020).	27

DAFTAR GAMBAR

Gambar 3. 1 Tahapan penelitian.....	34
Gambar 3. 2 Flowchart Sistem SHA-256.....	35
Gambar 3. 3 Use Case Diagram	39
Gambar 3. 4 Activity Diagram Login.....	40
Gambar 3. 5 Activity Diagram Hapus Transaksi	41
Gambar 3. 6 Sequence Diagram	42
Gambar 3. 7 Teknik Pengumpulan Data	44
Gambar 3. 8 Halaman Login	45
Gambar 3. 9 Halaman Dashboard.....	46
Gambar 3. 10 Halaman Unggah Menggunakan QRIS	47
Gambar 3. 11 Hasil Verifikasi Dokumen	48
Gambar 3. 12 Riwayat Verifikasi	48
Gambar 3. 13 Hapus Dokumen	49
Gambar 4. 1 Halaman Login	55
Gambar 4. 2 Halaman Dashboard.....	55
Gambar 4. 3 Halaman Unggah Bukti QRIS	56
Gambar 4. 4 Halaman Hasil Verifikasi	57
Gambar 4. 5 Halaman Hasil Pembacaan Dokumen Referensi dan Detail Hasil Pembacaan Dokumen Uji	58
Gambar 4. 6 Halaman Detail Informasi Teknis Dokumen	59
Gambar 4. 7 Halaman Tampilan Bukti Transaksi QRIS	60
Gambar 4. 8 Halaman Riwayat Verifikasi.....	61

BAB 1

PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi pembayaran digital berbasis QRIS telah memberikan kemudahan dalam proses transaksi, khususnya pada usaha kecil seperti warung, kedai, dan kafe. Digitalisasi di sektor keuangan telah melahirkan berbagai inovasi layanan pembayaran non-tunai yang bertujuan untuk meningkatkan efisiensi, kecepatan, dan kemudahan transaksi (Davis, 2021). Salah satu bentuk inovasi tersebut adalah penerapan *Quick Response Code Indonesian Standard* (QRIS), yang dikembangkan oleh Bank Indonesia sebagai standar nasional pembayaran berbasis kode QR (Bank Indonesia, 2019). QRIS dirancang untuk menyatukan berbagai platform pembayaran digital agar dapat digunakan secara interoperabel, sehingga mempermudah masyarakat dan pelaku usaha dalam melakukan transaksi keuangan secara elektronik (Bank Indonesia, 2020).

Berdasarkan data statistik sistem pembayaran yang dirilis oleh Bank Indonesia dan Otoritas Jasa Keuangan, penggunaan QRIS menunjukkan pertumbuhan yang sangat pesat dari tahun ke tahun (Otoritas Jasa Keuangan, 2022). Peningkatan ini terlihat dari bertambahnya jumlah pengguna, merchant, volume transaksi, serta nilai transaksi QRIS secara nasional. Tingginya pertumbuhan tersebut menunjukkan bahwa QRIS telah menjadi salah satu instrumen pembayaran digital yang paling dominan dan dipercaya oleh masyarakat Indonesia (Bank Indonesia, 2023).

Metode pembayaran ini banyak digunakan dalam berbagai aktivitas sehari-hari, mulai dari transaksi di warung kecil hingga pusat perbelanjaan modern. Setiap transaksi QRIS umumnya menghasilkan bukti pembayaran dalam bentuk dokumen digital, seperti file gambar asli berbentuk JPG/PNG, yang digunakan sebagai alat verifikasi oleh penjual.

Namun, kemudahan dalam membuat dan menyebarkan bukti transaksi digital juga diiringi dengan potensi penyalahgunaan. Saat ini, berbagai aplikasi pengolah gambar memungkinkan seseorang untuk melakukan manipulasi terhadap bukti transaksi, seperti mengubah nominal pembayaran, waktu transaksi, atau identitas pengirim. Manipulasi tersebut sering kali sulit dideteksi secara kasat mata karena tampilan visual dokumen tetap terlihat meyakinkan.

Di sisi lain, tidak semua perubahan pada file digital menunjukkan adanya manipulasi isi. Perubahan dapat terjadi akibat proses teknis seperti kompresi file, atau pengiriman melalui aplikasi pesan, yang menyebabkan perbedaan pada struktur file tanpa mengubah isi informasi transaksi. Hal ini menimbulkan kesulitan dalam membedakan antara dokumen yang benar-benar dimanipulasi dengan dokumen yang hanya mengalami perubahan teknis.

Untuk mengatasi permasalahan tersebut, diperlukan suatu pendekatan berbasis forensik digital yang mampu mendeteksi keaslian dokumen secara lebih akurat. Salah satu metode yang dapat digunakan adalah algoritma hash kriptografi seperti SHA-256, yang memiliki kemampuan untuk mendeteksi perubahan sekecil apa pun pada file digital melalui perbedaan nilai hash. Namun, algoritma ini hanya dapat menunjukkan adanya perubahan pada file secara keseluruhan, tanpa dapat mengidentifikasi bagian spesifik yang mengalami perubahan. Oleh karena itu, dalam penelitian ini tidak hanya dilakukan perhitungan hash menggunakan SHA-256, tetapi juga dilakukan analisis terhadap elemen-elemen.

Transaksi seperti nominal pembayaran, waktu transaksi, serta identitas pengirim dan penerima. Proses analisis ini dilakukan melalui input manual untuk memastikan keakuratan data yang dibandingkan. Dengan menggunakan kedua pendekatan tersebut, diharapkan sistem dapat membedakan antara perubahan teknis file dan manipulasi isi transaksi secara lebih tepat.

Dalam praktik sehari-hari, penjual umumnya melakukan verifikasi pembayaran hanya dengan melihat bukti transaksi yang ditunjukkan oleh pembeli melalui perangkat ponsel. Proses ini sering dilakukan secara cepat, terutama dalam kondisi transaksi yang ramai, sehingga penjual tidak memiliki cukup waktu untuk memeriksa secara detail informasi yang terdapat pada bukti transaksi tersebut. Kondisi tersebut menyebabkan proses verifikasi hanya mengandalkan pengamatan visual yang berpotensi menimbulkan kesalahan.

Di sisi lain, bukti transaksi QRIS yang berbentuk dokumen digital memiliki potensi untuk dimodifikasi atau diedit menggunakan aplikasi pengolah gambar seperti Adobe Photoshop. Manipulasi tersebut dapat dilakukan dengan cara sederhana sehingga sulit dibedakan dari bukti asli jika hanya dilihat sekilas. Selain itu, penjual umumnya tidak menyimpan bukti transaksi sebagai arsip, sehingga tidak memiliki data pembandingan ketika terjadi ketidaksesuaian antara jumlah transaksi dan dana yang diterima. Oleh karena itu, diperlukan suatu sistem yang mampu menyimpan bukti transaksi serta menjaga integritasnya.

Penerapan algoritma hash SHA-256 dapat digunakan untuk menghasilkan nilai unik dari setiap dokumen, sehingga setiap perubahan pada bukti transaksi dapat dideteksi dan membantu proses verifikasi secara lebih akurat.

Kondisi ini berpotensi menimbulkan kerugian finansial, menurunkan kepercayaan dalam sistem pembayaran digital, serta memicu sengketa antara pihak yang terlibat dalam transaksi (Casey, 2011).

Algoritma Secure Hash Algorithm 256-bit (SHA- 256) merupakan salah satu algoritma hash yang memiliki tingkat keamanan tinggi dan banyak digunakan dalam berbagai sistem keamanan digital. SHA-256 memiliki sifat *collision resistant* dan *avalanche effect*, di mana perubahan satu bit data saja akan menghasilkan nilai hash yang berbeda secara signifikan (Stallings, 2017). Dengan karakteristik tersebut, SHA-256 sangat efektif digunakan untuk mendeteksi perubahan sekecil apa pun pada dokumen digital.

Berdasarkan latar belakang tersebut, penelitian ini berfokus pada penerapan analisis forensik digital untuk memverifikasi keaslian bukti transaksi pembayaran QRIS dengan memanfaatkan algoritma hash SHA-256. Data yang digunakan dalam penelitian ini meliputi file gambar bukti pembayaran QRIS dalam format JPG atau PNG.

Dengan membandingkan nilai hash file asli dan file hasil manipulasi, penelitian ini bertujuan untuk membuktikan bahwa setiap perubahan pada dokumen digital dapat terdeteksi secara objektif dan akurat sebagai indikasi manipulasi.

Melalui pendekatan ini, diharapkan penelitian dapat memberikan kontribusi dalam pengembangan metode verifikasi keaslian dokumen pembayaran digital, khususnya pada sistem QRIS. Selain itu, hasil penelitian ini diharapkan dapat meningkatkan kesadaran akan pentingnya penerapan forensik digital dalam menjaga keamanan transaksi elektronik serta menjadi referensi bagi pelaku usaha, dan pihak terkait dalam menghadapi potensi penyalahgunaan bukti transaksi digital.

1.2 Rumusan Masalah

Berdasarkan penjelasan latar belakang yang telah disampaikan rumusan masalah dalam penelitian ini dapat dirinci adalah sebagai berikut :

- a. Bagaimana menganalisis elemen transaksi (nominal, waktu transaksi, identitas pengirim, dan penerima) untuk mengidentifikasi bagian yang mengalami perubahan pada bukti transaksi QRIS?
- b. Bagaimana penerapan algoritma SHA-256 dalam mendeteksi perubahan pada dokumen bukti transaksi QRIS?
- c. Bagaimana cara melakukan verifikasi keaslian bukti transaksi pembayaran QRIS secara digital?
- d. Bagaimana sistem menampilkan bukti hasil transaksi pembayaran QRIS?

1.3 Batasan Masalah

Agar penelitian ini terfokus dan tidak menyimpang dari tujuan yang telah ditetapkan, maka diperlukan batasan masalah sebagai berikut:

- a. Dokumen yang dianalisis berupa file gambar (JPG/PNG).
- b. Bukti transaksi QRIS yang dianalisis dibatasi pada manipulasi visual dan data, meliputi perubahan nominal pembayaran, tanggal transaksi, dan identitas pengirim, tanpa membahas aspek keamanan sistem QRIS secara menyeluruh.
- c. Data yang digunakan dalam penelitian ini berupa file bukti pembayaran QRIS asli (yang disimpan dan dikirim langsung via wa oleh penjual) dan file yang telah dimanipulasi secara sengaja sebagai skenario pengujian.
- d. Algoritma kriptografi yang digunakan dalam penelitian ini dibatasi hanya pada algoritma hash SHA-256, tanpa melakukan perbandingan dengan algoritma hash lain seperti MD5, SHA-1, atau SHA-512.
- e. Analisis forensik digital dalam penelitian ini difokuskan pada Hash SHA-256 dan *Optical Character Recognition* (OCR).
- f. Bukti transaksi pembayaran QRIS yang digunakan pada penelitian ini yaitu hanya bukti transaksi QRIS dari Bank Syariah Indonesia (BSI),

karena memang data yang diuji peneliti hanya bukti QRIS dari Bank BSI.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut :

- a. Untuk menganalisis elemen-elemen transaksi yang meliputi nominal, waktu transaksi, identitas pengirim, dan penerima guna mengidentifikasi bagian yang mengalami perubahan pada bukti transaksi QRIS.
- b. Untuk menerapkan algoritma SHA-256 dalam mendeteksi adanya perubahan pada dokumen bukti transaksi QRIS.
- c. Untuk memverifikasi keaslian bukti transaksi pembayaran QRIS.
- d. Untuk mengimplementasikan sistem yang mampu menampilkan hasil transaksi pembayaran QRIS.

1.5 Manfaat Penelitian

Penelitian ini diharapkan memberikan berbagai manfaat, baik bagi pihak-pihak terkait lainnya.

1. Bagi Peneliti

- a. Memberikan kontribusi dalam pengembangan keilmuan di bidang forensik digital dan keamanan informasi, khususnya terkait verifikasi keaslian dokumen digital berbentuk gambar.
- b. Memperkaya kajian ilmiah mengenai penerapan algoritma hash SHA-256 dalam konteks transaksi pembayaran digital berbasis QR code.

2. Bagi Prodi

- a. Penelitian ini memberikan kontribusi pada pengembangan ilmu pengetahuan di bidang Sistem Informasi dan Keamanan Informasi, khususnya dalam kajian forensik digital dan verifikasi keaslian dokumen digital.

- b. Hasil penelitian ini dapat menjadi referensi akademik bagi penelitian selanjutnya yang ingin mengembangkan metode deteksi manipulasi dokumen digital, khususnya pada bukti transaksi pembayaran elektronik berbasis QR code.
- c. Penelitian ini dapat menjadi rujukan bagi pengembangan dan implementasi algoritma hash kriptografis, khususnya SHA-256, dalam berbagai konteks pengamanan data dan verifikasi integritas dokumen digital.
- d. Penelitian ini dapat menjadi acuan bagi peneliti lain yang tertarik mengembangkan teknologi serupa di bidang administrasi digital, keamanan sistem informasi yang melibatkan pengelolaan dan verifikasi dokumen digital.

3. Bagi Pelaku Usaha dan UMKM

- a. Penelitian ini dapat membantu pelaku usaha dan pihak penerima pembayaran dalam memverifikasi keaslian bukti transaksi QRIS secara lebih akurat dan objektif.
- b. Dengan penerapan analisis forensik digital dan algoritma hash SHA-256, potensi kerugian akibat manipulasi bukti pembayaran digital dapat diminimalkan.
- c. Penelitian ini dapat meningkatkan kepercayaan dan keamanan transaksi digital, khususnya dalam penggunaan QRIS sebagai sistem pembayaran non-tunai.
- d. Hasil penelitian ini dapat menjadi bahan pertimbangan teknis dalam pengembangan prosedur atau sistem verifikasi bukti transaksi pembayaran digital.

4. Bagi Universitas

- a. Penelitian ini dapat meningkatkan kualitas akademik dan lulusan melalui kegiatan penelitian yang aplikatif, relevan dengan perkembangan teknologi, dan sesuai dengan kebutuhan industri digital.
- b. Hasil penelitian ini dapat menjadi referensi ilmiah bagi civitas akademika dalam pengembangan penelitian di bidang forensik digital.

BAB II

LANDASAN TEORI

2.1 Forensik Digital

Forensik adalah cabang ilmu forensik yang berkaitan dengan pengumpulan, analisis, dan pelestarian bukti digital dari perangkat elektronik yang digunakan untuk investigasi hukum dan keamanan siber. Secara lebih spesifik, digital forensik bertujuan untuk mendapatkan bukti yang sah, menjamin integritas dan keaslian data, serta mengungkap motif pelaku, sehingga informasi yang di dapat tetap valid.

Menurut (Qodri, 2025) forensik digital dapat juga diartikan sebagai pengumpulan dan analisis data dari berbagai sumber daya komputer yang mencakup sistem komputer, jaringan komputer, jalur komunikasi, dan berbagai media penyimpanan yang layak untuk diajukan dalam sidang pengadilan. Forensik digital memiliki fungsi yang krusial dalam menjaga keaslian, integritas, dan validitas informasi transaksi yang tersimpan di dalam sistem elektronik.

Bukti digital yang didapat dari alat seperti komputer, telepon pintar, jaringan, dan tempat penyimpanan memiliki kekuatan hukum apabila dapat dibuktikan keaslian dan integritasnya. Dalam situasi transaksi finansial elektronik, khususnya melalui Kode Respons Cepat Standar Indonesia (QRIS), forensik digital memainkan peran krusial untuk memastikan keabsahan dan keutuhan bukti pembayaran yang tercatat dalam sistem digital.

2.2 Sistem Pembayaran

Secara terminologis, istilah *sistem pembayaran* tersusun atas dua kata, yaitu *sistem* dan *pembayaran*.

Menurut Kamus Umum Bahasa Indonesia, sistem diartikan sebagai sekelompok bagian atau unsur yang saling berkaitan dan bekerja sama untuk mencapai suatu tujuan tertentu. Menurut Kamus Umum Bahasa Indonesia, sistem diartikan sebagai sekelompok bagian atau unsur yang saling berkaitan dan bekerja sama untuk mencapai suatu tujuan tertentu. Dalam konteks ilmu sistem, sistem dapat dipahami sebagai suatu tatanan atau susunan yang terstruktur, terdiri atas komponen-komponen yang saling berinteraksi secara teratur dan terencana guna mencapai tujuan yang telah ditetapkan. Setiap komponen dalam sistem memiliki fungsi masing-masing, namun tetap saling bergantung satu sama lain (Jogiyanto, 2017).

Sementara itu, pembayaran secara umum diartikan sebagai proses perpindahan nilai dari satu pihak ke pihak lain sebagai konsekuensi dari adanya transaksi ekonomi. Pihak-pihak yang terlibat dalam proses pembayaran umumnya adalah penjual dan pembeli. Dalam setiap aktivitas ekonomi yang melibatkan pertukaran barang atau jasa, proses pembayaran menjadi elemen yang tidak terpisahkan karena berfungsi sebagai sarana penyelesaian kewajiban finansial antara kedua belah pihak (Mishkin, 2019).

Berdasarkan definisi terminologis dan yuridis tersebut, dapat disimpulkan bahwa sistem pembayaran merupakan suatu mekanisme terstruktur yang bekerja secara sistematis dalam memfasilitasi perpindahan nilai ekonomi antar pihak yang bertransaksi. Dalam perkembangannya, sistem pembayaran tidak lagi terbatas pada pembayaran tunai, tetapi telah berkembang ke arah sistem pembayaran non-tunai berbasis teknologi digital. Transformasi ini bertujuan untuk meningkatkan efisiensi, kecepatan, dan keamanan transaksi, sekaligus mengurangi risiko yang melekat pada penggunaan uang tunai (Bank Indonesia, 2020).

Seiring dengan digitalisasi sistem pembayaran, muncul tantangan baru terkait keamanan dan keaslian bukti transaksi digital. Bukti pembayaran yang sebelumnya berbentuk fisik kini beralih menjadi dokumen digital yang rentan terhadap manipulasi. Oleh karena itu, sistem pembayaran modern menuntut adanya mekanisme verifikasi dan pengamanan tambahan untuk menjaga integritas transaksi. Dalam konteks ini, penerapan teknologi forensik digital dan kriptografi menjadi penting untuk memastikan bahwa bukti pembayaran digital benar-benar autentik dan tidak mengalami perubahan yang dapat merugikan pihak-pihak yang terlibat dalam transaksi (Casey, 2011).

2.3 Pembayaran Digital

Digital payment atau pembayaran digital merupakan metode pembayaran yang memanfaatkan media elektronik sebagai sarana utama dalam proses transaksi keuangan. Pembayaran digital umumnya dilakukan melalui berbagai platform berbasis teknologi informasi, seperti *Short Message Service* (SMS), *internet banking*, *mobile banking*, serta dompet elektronik (*e-wallet*). Menurut Dahlberg et al. (2015), pembayaran digital adalah sistem pembayaran yang memungkinkan perpindahan nilai secara elektronik dengan dukungan infrastruktur teknologi, sehingga transaksi dapat dilakukan tanpa penggunaan uang tunai secara langsung.

Pembayaran digital saat ini menjadi salah satu layanan keuangan ritel yang paling banyak digunakan dalam aktivitas sehari-hari. Hal ini disebabkan oleh meningkatnya kebutuhan masyarakat akan sistem pembayaran yang cepat, mudah, dan fleksibel. Layanan pembayaran digital mampu meningkatkan pengalaman pengguna (*customer experience*).

Karena memberikan efisiensi dari sisi kecepatan transaksi, kenyamanan penggunaan, serta aksesibilitas melalui berbagai saluran (*multi-channel accessibility*), seperti perangkat mobile dan jaringan internet (Khiaonarong & Humphrey, 2019).

Dalam praktiknya, penggunaan digital payment menawarkan berbagai keuntungan bagi penggunanya. Pertama, transaksi menjadi lebih mudah dan praktis karena dapat dilakukan kapan saja dan di mana saja tanpa harus membawa uang tunai. Kedua, pembayaran digital dinilai lebih aman karena dilengkapi dengan sistem keamanan berlapis, seperti autentikasi pengguna, enkripsi data, dan pencatatan transaksi secara otomatis. Ketiga, digital payment memberikan kenyamanan dalam bertransaksi karena proses pembayaran dapat diselesaikan dalam waktu singkat tanpa interaksi fisik. Keempat, kecepatan transaksi menjadi salah satu keunggulan utama, terutama dalam aktivitas ekonomi dengan frekuensi transaksi tinggi. Kelima, pembayaran digital dapat digunakan untuk berbagai layanan, mulai dari pembelian barang dan jasa, pembayaran tagihan, hingga transaksi transportasi dan hiburan digital (Ozili, 2018).

Berdasarkan laporan yang dimuat oleh Liputan6, GoPay tercatat sebagai dompet digital yang paling banyak digunakan di Indonesia dengan tingkat penggunaan mencapai sekitar 81%. Tingginya tingkat adopsi dompet digital ini menunjukkan bahwa masyarakat Indonesia semakin terbiasa dengan transaksi non-tunai dan menaruh kepercayaan besar terhadap sistem pembayaran digital. Namun demikian, tingginya penggunaan pembayaran digital juga menimbulkan tantangan baru, terutama terkait keamanan transaksi dan keaslian bukti pembayaran digital yang dihasilkan dari sistem tersebut.

2.4 Quick Response Code (QR Code)

QR Code (*Quick Response Code*) merupakan kode dua dimensi yang dikembangkan untuk menyimpan dan menyajikan informasi secara cepat melalui proses pemindaian. Secara teknis, QR Code terdiri atas pola persegi pada tiga sudut utama, yaitu sudut kiri atas, sudut kanan atas, dan sudut kiri bawah, yang berfungsi sebagai *finder pattern* untuk membantu perangkat pemindai mengenali orientasi dan posisi kode. Selain itu, QR Code tersusun atas modul-modul hitam berbentuk titik atau piksel persegi yang merepresentasikan data dalam bentuk biner. Struktur ini memungkinkan QR Code menyimpan data alfanumerik, karakter, maupun simbol dalam jumlah yang relatif besar dibandingkan dengan kode batang satu dimensi (*barcode*) (Denso Wave, 2020).

Salah satu keunggulan utama QR Code adalah kemampuannya dalam menyimpan informasi secara horizontal dan vertikal, sehingga kapasitas penyimpanan data menjadi lebih besar dan proses pembacaan data menjadi lebih cepat. Karakteristik ini menjadikan QR Code sangat sesuai untuk digunakan dalam sistem pembayaran digital, khususnya pada transaksi nirsentuh (*contactless payment*). Melalui proses pemindaian menggunakan perangkat seluler, informasi pembayaran dapat dikirimkan secara instan dari pengguna kepada sistem pembayaran tanpa memerlukan kontak fisik atau penggunaan uang tunai (Roussos & Kostakos, 2009). Dalam konteks sistem pembayaran, QR Code telah banyak diterbitkan dan digunakan oleh lembaga perbankan maupun lembaga non-perbankan, termasuk penyedia layanan dompet digital dan *financial technology* (fintech).

QR Code pembayaran umumnya terhubung dengan sistem berbasis server, di mana data transaksi akan diproses secara real time melalui jaringan internet. Penerapan QR Code dalam sistem pembayaran ini bertujuan untuk meningkatkan efisiensi transaksi, mengurangi penggunaan uang tunai, serta mendukung ekosistem pembayaran digital yang lebih inklusif (Bank Indonesia, 2020).

Penggunaan QR Code pembayaran banyak diterapkan oleh para pedagang, khususnya pada sektor ritel dan Usaha Mikro, Kecil, dan Menengah (UMKM). Para pedagang biasanya menyediakan QR Code di tempat usaha mereka agar pelanggan dapat dengan mudah melakukan pembayaran menggunakan aplikasi pembayaran digital yang dimiliki. Dengan memindai QR Code yang tersedia, pelanggan dapat langsung melakukan transaksi secara non-tunai tanpa perlu interaksi fisik dengan kasir. Hal ini tidak hanya mempercepat proses pembayaran, tetapi juga meningkatkan kenyamanan dan keamanan transaksi bagi kedua belah pihak (Khiaonarong & Humphrey, 2019).

Meskipun QR Code pembayaran menawarkan berbagai kemudahan dan keunggulan, penggunaan kode ini juga menimbulkan tantangan tersendiri, terutama terkait keamanan transaksi dan keaslian bukti pembayaran digital yang dihasilkan. Bukti pembayaran berbasis QR Code umumnya ditampilkan dalam bentuk dokumen digital, sehingga rentan terhadap manipulasi apabila tidak dilengkapi dengan mekanisme verifikasi yang memadai. Oleh karena itu, diperlukan pendekatan tambahan, seperti analisis forensik digital dan penggunaan teknik kriptografi, untuk memastikan integritas dan keaslian bukti transaksi pembayaran berbasis QR Code.

2.5 Algoritma Hash

Algoritma hash atau fungsi hash merupakan suatu fungsi matematis yang menerima masukan berupa pesan atau data dengan panjang sembarang (*variable length input*) dan mengubahnya menjadi keluaran berupa nilai tetap (*fixed length output*). Proses ini dikenal sebagai proses *hashing*, sedangkan hasil keluarannya disebut sebagai *message digest* atau nilai hash. Nilai hash bersifat unik terhadap data asalnya, sehingga perubahan sekecil apa pun pada data masukan akan menghasilkan nilai hash yang berbeda secara signifikan (Dermawan Ikhsan, 2021).

Nilai hash yang dihasilkan oleh suatu algoritma hash memiliki panjang yang berbeda-beda tergantung pada jenis algoritma yang digunakan. Sebagai contoh, algoritma MD5 menghasilkan nilai hash sepanjang 128 bit, SHA-1 menghasilkan 160 bit, sedangkan algoritma SHA-256 menghasilkan nilai hash sepanjang 256 bit. Perbedaan panjang nilai hash ini berpengaruh terhadap tingkat keamanan dan ketahanan algoritma hash terhadap serangan kriptografi, seperti *collision attack* dan *preimage attack* (Stallings, 2017).

Secara umum, algoritma hash kriptografis memiliki beberapa karakteristik utama, yaitu bersifat satu arah (*one-way function*), deterministik, dan sensitif terhadap perubahan input. Bersifat satu arah berarti nilai hash tidak dapat dikembalikan ke data asli dengan mudah. Deterministik berarti data masukan yang sama akan selalu menghasilkan nilai hash yang sama. Sementara itu, sifat sensitivitas perubahan data dikenal sebagai *avalanche effect*, di mana perubahan satu bit pada data masukan akan menghasilkan perubahan besar pada nilai hash yang dihasilkan (Menezes et al., 2018).

Skema proses hashing pada suatu algoritma hash umumnya diawali dengan memasukkan data atau pesan asli (*plaintext*) ke dalam fungsi hash. Selanjutnya, fungsi hash akan melakukan proses kompresi dan transformasi data melalui serangkaian operasi matematis hingga menghasilkan nilai hash dengan panjang tetap. Skema ini menggambarkan bahwa fungsi hash tidak menyimpan informasi panjang asli data, melainkan hanya merepresentasikan data tersebut dalam bentuk nilai ringkas yang bersifat unik. Oleh karena itu, algoritma hash banyak digunakan untuk tujuan verifikasi integritas data, autentikasi, dan pendeteksian perubahan data pada sistem digital.

Dalam konteks keamanan dokumen digital dan forensik digital, algoritma hash berperan penting sebagai alat untuk memastikan integritas data. Dengan membandingkan nilai hash dari suatu dokumen sebelum dan sesudah dilakukan pemeriksaan, dapat diketahui apakah dokumen tersebut mengalami perubahan atau manipulasi. Jika nilai hash berbeda, maka dapat disimpulkan bahwa dokumen telah mengalami perubahan, baik disengaja maupun tidak disengaja. Prinsip inilah yang menjadikan algoritma hash sangat relevan dalam penelitian ini, khususnya dalam verifikasi keaslian bukti transaksi pembayaran QRIS.

2.6 Secure Hash Algorithm 256

Secure Hash Algorithm 256 (SHA-256) merupakan salah satu algoritma hash kriptografis yang termasuk ke dalam keluarga algoritma SHA (*Secure Hash Algorithm*). Hash adalah fungsi yang secara efisien mengubah string input dengan panjang berhingga menjadi string output dengan panjang tetap yang disebut nilai hash, sedangkan fungsi hash kriptografis adalah fungsi hash yang memiliki beberapa sifat keamanan tambahan sehingga dapat dipakai untuk tujuan keamanan data. Algoritma SHA-256 digunakan karena memiliki sifat satu arah (*one-way function*), deterministik, dan sensitif terhadap perubahan data (*avalanche effect*), di mana perubahan satu bit data akan menghasilkan nilai hash yang berbeda secara signifikan (Stallings, 2017). Nilai hash yang dihasilkan berfungsi sebagai *fingerprint* digital dari dokumen tersebut. Umumnya digunakan pada keperluan autentikasi dan integritas data. Menurut (Rivest & Adleman, 2022) SHA-256 adalah fungsi hash kriptografi dengan panjang message digest keluaran 256 bit, merupakan fungsi hash yang tak membutuhkan kunci. Pesan diproses oleh blok $512 = 16 \times 32 \text{ bit}$, tiap blok membutuhkan 64 putaran. Algoritma ini dirancang oleh *United States National Security Agency* (NSA) pada tahun 2001 dan distandarkan oleh *National Institute of Standards and Technology* (NIST). SHA-256 dipatenkan di bawah paten Amerika Serikat dengan nomor US Patent 6829355 (Bhargav et al., 2015). SHA-256 dirancang sebagai pengembangan dari algoritma hash sebelumnya untuk menghasilkan tingkat keamanan yang lebih tinggi terhadap serangan kriptografi.

SHA-256 menghasilkan nilai hash dengan panjang tetap sebesar **256 bit**, yang umumnya direpresentasikan dalam format heksadesimal (*hexadecimal*) agar lebih mudah dibaca dan diimplementasikan pada sistem digital (Endelina, 2021). Panjang hash yang relatif besar ini membuat SHA-256 memiliki tingkat ketahanan yang tinggi terhadap serangan *collision*, *preimage*, dan *second preimage*, sehingga banyak digunakan dalam sistem keamanan informasi, tanda tangan digital, blockchain, dan verifikasi integritas data.

Adapun nilai hash awal dari pada fungsi SHA-256 adalah sebagai berikut:

Tabel 2. 1Inisialisasi nilai awal Hash SHA-256

Variabel	Nilai
H ₀	6A09E667
H ₁	BB67AE85
H ₂	3C6EF372
H ₃	A54FF53A
H ₄	510E527F
H ₅	9B05688C
H ₆	1F83D9AB
H ₇	5BE0CD19

Fungsi SHA-256 memiliki 8 langkah kerja dan rumus sebagai berikut:

1. Tambahkan bit padding, yaitu pesan diisi sehingga panjangnya kongruen dengan 448, modulus 512. Padding 1 bit ditambahkan di akhir pesan, diikuti oleh banyak nol yang diperlukan sehingga panjang bit sama dengan 448 modulus 512.
2. Panjang append, yaitu representasi panjang pesan 64 bit ditambahkan pada hasil akhirnya, langkah untuk membuat panjang pesan kelipatan 512 bit.
3. Parsing pesan, yaitu pesan padding diuraikan menjadi N blok pesan 512 bit, $M(1), M(2), \dots, M(N)$, dengan menambahkan blok 64 bit.
4. Inisialisasi nilai hash, yaitu nilai hash awal, (0) diatur, terdiri dari delapan kata 32 bit, dalam bentuk heksadesimal.

5. Mempersiapkan jadwal pesan, yaitu SHA-256 menggunakan jadwal pesan enam puluh empat kata 32 bit, kata-kata dari jadwal pesan diberi label $W_0, 1, \dots, W_{63}, wd$.

$$W_t = \begin{cases} M_t^{(t)}, & 0 \leq t \leq 15 \\ \sigma_1^{256}(W_{t-2}) + (W_{t-7}) + \sigma_0^{256}(W_{t-15}) + (W_{t-16}), & 16 \leq t \leq 63 \end{cases} \quad (1)$$

Dimana :

$$\sigma_1^{256}(W_{t-2}) = ((W_{t-2})ROTR 17) \oplus ((W_{t-2})ROTR 19) \oplus ((W_{t-2})SHR 10) \quad (2)$$

$$\sigma_0^{256}(W_{t-15}) = ((W_{t-15})ROTR 17) \oplus ((W_{t-15})ROTR 18) \oplus ((W_{t-15})SHR 3) \quad (3)$$

6. Inisialisasi, yaitu inisialisasi delapan variable kerja a, b, c, d, e, f, g dan h dengan nilai *hash*.

$$\begin{aligned} & (i-1) \text{ for } t = 0 \text{ to } 63 \\ & \{ T_1 = h + \sum_1^{(256)}(e) + Ch(e, f, g) + K_1^{(256)} + W_t \} \end{aligned} \quad (4)$$

$$\begin{aligned} T_2 &= \sum_0^{256}(a) + Maj(a, b, c) \\ h &= g \\ f &= e \\ e &= d + T_1 \\ d &= c \\ c &= b \\ b &= a \\ a &= T_1 + T_2 \end{aligned}$$

Dimana :

$$\sum_1^{(256)}(e) = (eROTR6) \oplus (eROTR11) \oplus (eROTR25) \quad (5)$$

$$\sum_0^{(256)}(a) = (aROTR2) \oplus (aROTR13) \oplus (aROTR22) \quad (6)$$

$$Ch(e, f, g) = (e \wedge f) \oplus (e \wedge g) \quad (7)$$

$$Maj(a, b, c) = (a \wedge b) \oplus (a \wedge c) \oplus (b \wedge c) \quad (8)$$

$$\begin{aligned} ROTR &= \text{Rotate Right} \\ \oplus &= \text{fungsi XOR} \\ \wedge &= \text{fungsi AND} \end{aligned}$$

7. Value nilai akhir hash, yaitu setelah seluruh iterasi selesai, diperoleh delapan variabel akhir a, b, c, d, e, f, g, h . Dengan menjumlahkan hasil akhir a, b, c, d, e, f, g dan h dengan inisial hash value $H(i)$.

$$H0 = H0 + a$$

$$H1 = H1 + b$$

$$H2 = H2 + c$$

$$H3 = H3 + d$$

$$H4 = H4 + e$$

$$H5 = H5 + f$$

$$H6 = H6 + g$$

$$H7 = H7 + h$$

2.7 Studi Terdahulu

Tabel 2. 2 Studi Terdahulu

No	Penulis	Judul	Metode	Hasil
1	Fachrul et al., 2022	Penerapan Konsep Digital Signature Terhadap Verifikasi Keaslian Dokumen Transkrip Nilai Mahasiswa Menggunakan Enkripsi Rivest Shamir Adleman (RSA) dan SHA-256	RSA dan SHA-256	Tanda tangan digital yang dibuat menggunakan algoritma RSA dan SHA-256 dapat digunakan untuk memverifikasi keaslian dokumen digital seperti PDF.
2	Andika et al., 2021	Aplikasi Enterprise Document Digital Signature Menggunakan RSA dan SHA-256 untuk WFH di Era Pandemi COVID-19	RSA dan SHA-256	Hasil penelitian menunjukkan bahwa melalui uji integritas, verifikasi dapat mendeteksi apabila dokumen PDF atau tanda tangan telah dipalsukan.
3	Arisandi et al., 2020	Pemeriksaan Integritas Dokumen dengan Digital Signature Algorithm	Digital Signature Algorithm (DSA)	Hasil penelitian menunjukkan bahwa algoritma DSA berhasil mengidentifikasi perubahan dari key yang digunakan.
4	Cahyo Prabowo & Afrianto, 2017	Penerapan Digital Signature dan Kriptografi pada Otentikasi Sertifikat Tanah Digital	RSA dan SHA-256	Penelitian menunjukkan tanda tangan digital mampu melacak perubahan yang terjadi apabila dokumen PDF diubah.
5	Hutagalung et al., 2023	Keamanan Data Menggunakan Secure Hashing Algorithm (SHA)-256 dan Rivest Shamir Adleman (RSA) pada Digital Signature	RSA dan SHA-256	Tanda tangan digital yang dibuat menggunakan algoritma RSA dan SHA-256 mampu memverifikasi keaslian Surat Keterangan Lulus (SKL).
6	Rangkuti et al., 2019	Implementasi Digital Signature pada E-Invoice di Uniq Digital Invitation Menggunakan Algoritma SHA-256 dan RSA	RSA dan SHA-256	Penelitian menyimpulkan bahwa algoritma SHA-256 dan RSA dapat diterapkan untuk menjaga keaslian data e-invoice dengan menghasilkan kode digital signature yang kompleks dan acak.
7	Endelina, 2021	Implementasi Digital Signature pada File Audio Menerapkan Metode SHA-256	SHA-256	Penelitian menghasilkan bahwa metode SHA-256 dapat mendeteksi keaslian file audio yang digunakan.

8	Az-Zahra et al., 2024	Implementasi QR Code dengan Algoritma SHA-256 dan RSA yang Ditingkatkan untuk Autentikasi Dokumen Digital	RSA dan SHA-256	Hasil penelitian menunjukkan algoritma RSA dan SHA-256 dapat dimanfaatkan untuk proses autentikasi dokumen digital menggunakan QR Code.
9	Saputra & Nasution, 2022	Perbandingan Performa Algoritma MD5 dan SHA-256 dalam Membangkitkan Identitas File	MD5 dan SHA-256	Algoritma MD5 memiliki performa lebih unggul dibandingkan SHA-256 dalam penggunaan prosesor, memori, dan waktu pemrosesan identitas file.
10	Nuraeni et al., 2018	Implementasi Tanda Tangan Digital Menggunakan RSA dan SHA-512 pada Proses Legalisasi Ijazah	RSA dan SHA-512	Penerapan RSA dan SHA-512 terbukti aman, ditunjukkan melalui pengujian modifikasi data pada dokumen legalisasi yang berhasil terdeteksi oleh sistem.

2.7.1 Research Gap Penelitian

Berdasarkan kajian terhadap penelitian terdahulu, diketahui bahwa sebagian besar penelitian memanfaatkan algoritma kriptografi seperti RSA dan SHA-256 dalam konteks tanda tangan digital untuk memverifikasi keaslian dokumen digital formal, seperti ijazah, transkrip nilai, sertifikat, e-invoice, dan dokumen PDF lainnya. Penelitian-penelitian tersebut berfokus pada pencegahan pemalsuan dokumen melalui mekanisme digital signature dalam sistem yang terstruktur dan terkontrol.

Namun, hingga saat ini masih terbatas penelitian yang membahas verifikasi keaslian bukti transaksi pembayaran QRIS, khususnya bukti transaksi yang disajikan dalam bentuk dokumen digital berupa file gambar JPG atau PNG. Bukti transaksi QRIS memiliki karakteristik berbeda karena umumnya berupa hasil unduhan dari aplikasi pembayaran digital yang tidak

dilengkapi tanda tangan digital dan sangat mudah untuk dimanipulasi secara visual. Selain itu, penelitian terdahulu belum banyak mengkaji pendekatan forensik digital yang menitikberatkan pada analisis struktur file, metadata gambar, serta perubahan integritas dokumen sebagai dasar verifikasi keaslian. Penggunaan algoritma hash SHA-256 sebagai alat analisis forensik untuk mendeteksi manipulasi pada bukti transaksi QRIS juga belum menjadi fokus utama dalam penelitian sebelumnya.

Oleh karena itu, penelitian ini menawarkan pembaruan dengan menerapkan analisis forensik digital berbasis algoritma hash SHA-256 untuk memverifikasi keaslian bukti transaksi pembayaran QRIS. Penelitian ini diharapkan dapat mengisi celah penelitian yang ada serta memberikan kontribusi dalam pengembangan metode verifikasi keaslian dokumen digital pada sistem pembayaran berbasis QR Code.

Namun, perbedaan utama terletak pada objek penelitian, yaitu bukti transaksi pembayaran QRIS yang berbentuk file gambar digital (JPG/PNG). Penelitian ini mengembangkan skenario pengujian dengan melakukan manipulasi pada elemen-elemen tertentu dalam bukti pembayaran QRIS, seperti nominal transaksi, tanggal pembayaran, dan identitas pengirim, yang secara visual sulit dibedakan dari bukti pembayaran asli. Setiap bukti transaksi kemudian dianalisis melalui pemeriksaan struktur file dan metadata sebagai bagian dari analisis forensik digital. Pengujian lanjutan dalam penelitian ini difokuskan pada perbandingan nilai hash SHA-256 antara bukti pembayaran QRIS asli dan bukti pembayaran yang telah dimanipulasi. Perbandingan ini dilakukan untuk mengukur kemampuan algoritma SHA-256 dalam mendeteksi perbedaan sekecil apa pun

pada dokumen digital secara konsisten dan objektif. Melalui pendekatan ini, penelitian diharapkan dapat membuktikan bahwa kombinasi analisis forensik digital dan algoritma hash SHA-256 efektif digunakan sebagai metode verifikasi keaslian bukti transaksi pembayaran QRIS serta sebagai upaya deteksi manipulasi dokumen digital.

2.8 UML

Perangkat Lunak semakin berkembang dan semakin canggih. Perangkat lunak didesain dengan memperhatikan hal – hal seperti skalabilitas, keamanan serta eksekusi yang kokoh walaupun dalam kondisi sulit. *Unified Modeling Language* merupakan bahasa visual untuk pemodelan dan komunikasi mengenai sebuah sistem dengan menggunakan diagram dan teks-teks pendukung. *UML* hanya berfungsi untuk melakukan pemodelan. Jadi penggunaan *UML* tidak terbatas pada metodologi tertentu, meskipun pada kenyataannya *UML* paling banyak digunakan pada metodologi berorientasi objek (Putra, 2023). *UML* adalah bahasa grafis untuk mendefinisikan, mendokumentasikan, dan membuat suatu sistem.

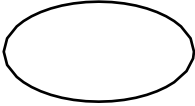
2.8.1 Use Case Diagram

Use Case Diagram menjelaskan manfaat dari aplikasi jika dilihat dari sudut pandang orang yang berada diluar sistem (aktor). *Diagram* ini menunjukkan fungsionalitas suatu sistem atau kelas dan bagaimana sistem berinteraksi dengan dunia luar. *Use Case Diagram* dapat digunakan selama proses analisa untuk menangkap *requirements* atau permintaan terhadap sistem dan untuk memahami bagaimana sistem tersebut harus bekerja (Putra,

2023). *Use case* diagram yang menggambarkan hubungan antara sistem dan actor.

Aktor adalah ilustrasi dari entitas manusia atau sebuah sistem yang beroperasi pada sistem. *Use case* merupakan deskripsi dari fungsionalitas yang dibutuhkan dari sebuah sistem (Prihandoyo, 2022). *Use case* digunakan untuk menentukan fungsi apa saja yang tersedia dalam sistem informasi serta yang berhak untuk menggunakan fungsi tersebut. Simbol-simbol yang digunakan dalam *Use Case* Diagram yaitu:

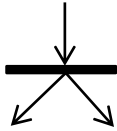
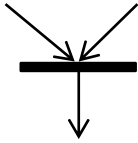
Tabel 2. 3 Simbol-simbol Use Case Diagram

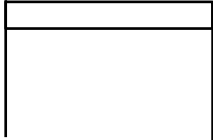
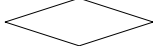
Gambar	Nama	Keterangan
		Fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau sektor
	Aktor	Orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi itu sendiri
	Asosiasi	Komunikasi antara actor dan yang berpartisipasi pada use case atau memiliki interaksi dengan aktor
	Generalisasi	Dimana fungsi yang satu adalah fungsi yang umum dari lainnya
	<<Include>>	Relasi dimana proses bersangkutan akan dilanjutkan ke proses yang dituju
	<<Extends>>	Menunjukkan bahwa satu use case dapat diperluas dengan use case lain

2.8.2 Activity Diagram

Activity Diagram menggambarkan aktivitas sistem bukan apa yang dilakukan oleh aktor, jadi aktivitas dapat dilakukan oleh sistem. Sebuah aktivitas dapat direalisasikan oleh satu *use case* atau lebih. Aktivitas menggambarkan proses yang berjalan, sementara *use case* menggambarkan bagaimana aktor menggunakan sistem untuk melakukan aktivitas (Putra, 2023). *Activity diagram* umumnya lebih menggambarkan proses dan jalur aktivitas dari tingkat ke-atas secara umum. Simbol-simbol yang digunakan untuk menggambarkan *activity diagram* dapat dilihat pada tabel 2.4

Tabel 2. 4 Simbol-simbol Activity Diagram

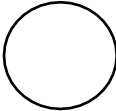
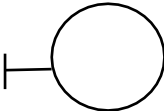
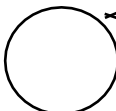
No.	Simbol	Nama	Keterangan
1.	 <i>Initial State</i>	 Awal (<i>Start</i>)	Diletakkan pada pojok kiri atas dan merupakan awal aktivitas.
2.	 <i>Final State</i>	Akhir (<i>End</i>)	Diletakkan di akhir berfungsi memberi tanda akhir aktivitas.
3.	 <i>Activity</i>	Aktivitas	Merupakan gambaran untuk sebuah proses/ kegiatan.
4.		<i>Fork/</i> Percabangan	<i>Fork/</i> percabangan digunakan untuk menunjukkan aktivitas yang berjalan secara paralel atau untuk menggabungkan dua aktivitas paralel menjadi satu.
5.		<i>Join/</i> Penggabungan	<i>Join /</i> penggabungan digunakan untuk menunjukkan adanya dekomposisi.

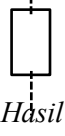
6.		<i>Swimlane</i>	Pembagian <i>activity</i> diagram untuk menunjukkan siapa melakukan apa.
7.	 <i>Decision Point</i>	Keputusan	Menggambarkan pilihan untuk pengambilan keputusan, <i>true</i> atau <i>false</i>

2.8.3 Sequence Diagram

Sequence Diagram adalah salah satu diagram pada *UML* yang disusun dalam urutan kronologis. Setiap diagram sekuensial mempresentasikan satu *flow* dari beberapa *flow* di dalam *use case* (Rusmawan, 2020). Berikut ini yang termasuk simbol dari *sequence diagram* adalah seperti sebagai berikut:

Tabel 2. 5 Simbol-simbol Sequence Diagram (Rusmawan, 2020).

No.	Simbol	Keterangan
1.	<i>Entity Class</i> 	Menjelaskan interaksi dari aktivitas yang dilakukan.
2.	<i>Boundary Class</i> 	Menjelaskan hubungan antara satu atau lebih aktor dengan sistem, seperti tampilan dari sebuah <i>form</i> .
3.	<i>Control Class</i> 	Menjelaskan hubungan antara perbatasan dengan tabel.
4.	<i>Message</i> 	Menjelaskan simbol pengiriman pesan.

5.	<i>Recursive</i> 	Menjelaskan pengiriman pesan yang dikirim kepada diri sendiri.
6.	<i>Activation</i>  <i>Hasil</i>	Sebuah eksekusi operasi dari objek, panjang kotak ini sebanding dengan durasi aktivitas suatu operasi.
7.	<i>Lifeline</i> 	Garis putus-putus yang terhubung ke objek, sepanjang <i>lifeline</i> terdapat <i>activation</i> .

2.9 Metadata

Metadata merupakan data yang memberikan informasi tentang data lain. Dalam konteks file digital, metadata berfungsi sebagai informasi tambahan yang menjelaskan karakteristik suatu file, seperti waktu pembuatan, ukuran file, format, dan informasi teknis lainnya (Park, J., & Tosaka, Y. 2010).

Metadata tambahan yang tersimpan dalam suatu file digital yang berfungsi untuk memberikan informasi mengenai file tersebut. Pada file gambar seperti JPG atau PNG, metadata umumnya dikenal sebagai EXIF (Exchangeable Image File Format). Namun demikian, metadata tidak selalu dijadikan sebagai bukti utama dalam menentukan keaslian suatu file, karena metadata dapat diubah atau dihapus oleh pengguna. Oleh karena itu, dalam penelitian ini metadata digunakan sebagai informasi pendukung untuk memperkuat analisis, sedangkan penentuan utama keaslian dokumen dilakukan menggunakan algoritma hash SHA-256.

2.9.1 Penerapan Metadata dalam Penelitian

Dalam penelitian ini, metadata digunakan sebagai salah satu parameter dalam analisis forensik digital terhadap bukti transaksi QRIS.

Metadata yang dianalisis meliputi:

1. Nama file
2. Ukuran file
3. Resolusi gambar

Metadata dari dokumen referensi dan dokumen uji dibandingkan untuk mengidentifikasi adanya perbedaan. Perbedaan metadata, seperti perubahan ukuran file atau resolusi, dapat menjadi indikasi bahwa dokumen telah mengalami manipulasi atau proses pengolahan ulang.

2.10 Optical Character Recognition (OCR)

OCR merupakan teknologi yang digunakan untuk mengubah teks yang terdapat dalam gambar menjadi bentuk data digital yang dapat dibaca dan diolah oleh (komputer Smith, R. 2007). OCR memungkinkan sistem untuk mengenali karakter huruf, angka. Menurut beberapa literatur, OCR merupakan bagian dari bidang pengolahan citra (image processing) dan kecerdasan buatan yang bertujuan untuk mengekstraksi informasi tekstual dari objek visual. Dengan adanya OCR, informasi yang sebelumnya hanya dapat dibaca oleh manusia dapat diolah lebih lanjut secara otomatis oleh sistem komputer.

Dengan memanfaatkan OCR, sistem tidak hanya mampu mendeteksi perubahan pada tingkat file melalui hash, tetapi juga dapat memahami isi dokumen secara langsung. Hal ini memberikan keunggulan dalam mengidentifikasi manipulasi spesifik yang tidak dapat diketahui hanya melalui analisis hash.

Peran OCR dalam Forensik Digital yaitu: Dalam konteks forensik digital, OCR memiliki peran penting dalam proses analisis bukti digital, khususnya pada

dokumen berbasis gambar. OCR memungkinkan sistem untuk: Mengubah bukti visual menjadi data terstruktur

Dengan demikian, OCR menjadi salah satu komponen penting dalam pendekatan multi-analisis yang digunakan dalam penelitian ini, bersama dengan algoritma hash SHA-256, analisis metadata, dan analisis struktur file.

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1 Analisis Permasalahan

Perkembangan sistem pembayaran digital berbasis QR Code, khususnya QRIS, telah menjadikan bukti transaksi dalam bentuk dokumen digital sebagai elemen krusial dalam proses validasi pembayaran. Bukti transaksi QRIS umumnya berupa file gambar berformat JPG atau PNG yang berisi informasi penting, seperti nominal transaksi, tanggal dan waktu pembayaran, serta identitas pengirim dan penerima. Dalam praktiknya, dokumen digital tersebut sering dijadikan satu-satunya acuan oleh pelaku usaha atau pihak penerima untuk memastikan bahwa transaksi telah benar-benar dilakukan. Kondisi ini menempatkan bukti pembayaran digital sebagai objek yang memiliki nilai penting sekaligus rentan terhadap penyalahgunaan.

Permasalahan utama yang ditemukan adalah seringnya manipulasi bukti transaksi pembayaran QRIS dengan memanfaatkan aplikasi pengeditan gambar yang mudah diakses dan digunakan. Manipulasi dapat dilakukan dengan mengubah nominal pembayaran, tanggal transaksi, maupun identitas pengirim tanpa meninggalkan jejak yang mudah dikenali secara visual. Menurut Casey (2011), dokumen digital berbentuk gambar sangat rentan terhadap pemalsuan karena perubahan konten visual dapat dilakukan tanpa merusak struktur file secara kasat mata. Hal ini menyebabkan proses verifikasi berbasis pengamatan visual menjadi tidak andal dan berpotensi menimbulkan kerugian finansial, terutama bagi pelaku usaha yang menerima transaksi dalam jumlah besar.

Di sisi lain, tidak semua perubahan pada file digital menunjukkan adanya manipulasi isi. Perubahan dapat terjadi akibat proses teknis seperti kompresi file, konversi format gambar (misalnya dari JPG ke PNG), atau pengiriman melalui aplikasi pesan, yang menyebabkan perbedaan pada struktur file tanpa mengubah isi informasi transaksi. Hal ini menimbulkan kesulitan dalam membedakan antara dokumen yang benar-benar dimanipulasi dengan dokumen yang hanya mengalami perubahan teknis.

Untuk mengatasi permasalahan tersebut, diperlukan suatu pendekatan berbasis forensik digital yang mampu mendeteksi keaslian dokumen secara lebih akurat. Salah satu metode yang dapat digunakan adalah algoritma hash kriptografi seperti SHA-256, yang memiliki kemampuan untuk mendeteksi perubahan sekecil apa pun pada file digital melalui perbedaan nilai hash. Namun, algoritma ini hanya dapat menunjukkan adanya perubahan pada file secara keseluruhan, tanpa dapat mengidentifikasi bagian spesifik yang mengalami perubahan.

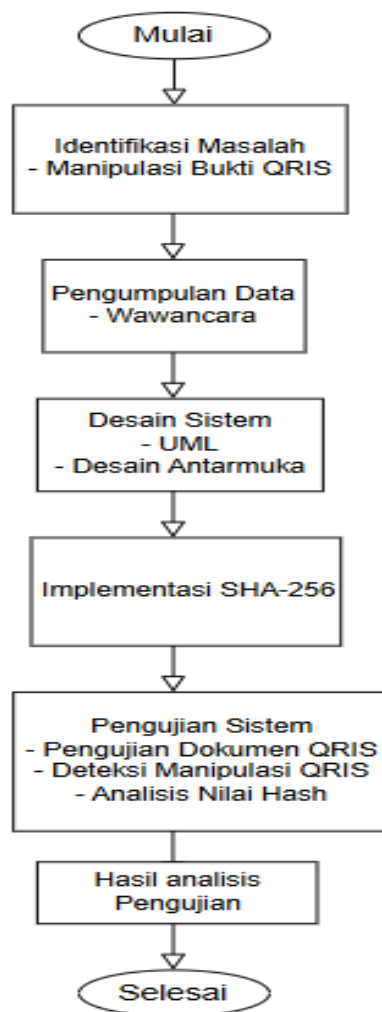
Oleh karena itu, dalam penelitian ini tidak hanya dilakukan perhitungan hash menggunakan SHA-256, tetapi juga dilakukan analisis terhadap elemen transaksi seperti nominal pembayaran, waktu transaksi, serta identitas pengirim dan penerima. Proses analisis ini dilakukan melalui input manual untuk memastikan keakuratan data yang dibandingkan. Dengan menggunakan kedua pendekatan tersebut, diharapkan sistem dapat membedakan antara perubahan teknis file dan manipulasi isi transaksi secara lebih tepat.

3.2 Algoritma Sistem

Algoritma sistem yang dirancang dalam penelitian ini bertujuan untuk memverifikasi keaslian bukti transaksi pembayaran QRIS secara objektif melalui kombinasi analisis forensik digital dan perhitungan nilai hash SHA-256. Algoritma ini dirancang agar mampu mendeteksi perubahan sekecil apa pun pada dokumen digital, baik perubahan yang tampak secara visual maupun perubahan yang hanya terjadi pada struktur file dan metadata. Pendekatan ini sejalan dengan prinsip dasar forensik digital yang menekankan keakuratan, konsistensi, dan dapat dipertanggung jawabkannya hasil analisis (Casey, 2011).

Metode yang digunakan dalam penelitian ini adalah metode eksperimen dengan pendekatan analisis forensik digital. Dalam penelitian ini, algoritma hash SHA-256 digunakan sebagai metode utama untuk mendeteksi perubahan pada dokumen digital.

Selain itu, digunakan metode pendukung berupa analisis metadata, struktur file, dan Optical Character Recognition (OCR) untuk memperkuat proses identifikasi manipulasi serta menentukan bagian spesifik yang mengalami perubahan. Tahapan penelitian diawali dengan identifikasi masalah dan potensi, yaitu ditemukannya potensi manipulasi pada bukti transaksi pembayaran QRIS dalam bentuk dokumen digital. Permasalahan tersebut menimbulkan kebutuhan akan suatu sistem yang mampu melakukan verifikasi keaslian dokumen secara digital. Tahap selanjutnya adalah pengumpulan data atau sampel, yang dilakukan untuk memperoleh informasi utama dalam perancangan sistem. Teknik pengumpulan data yang digunakan meliputi wawancara, yang dilakukan dengan pihak terkait untuk mendapatkan data kebutuhan sistem.



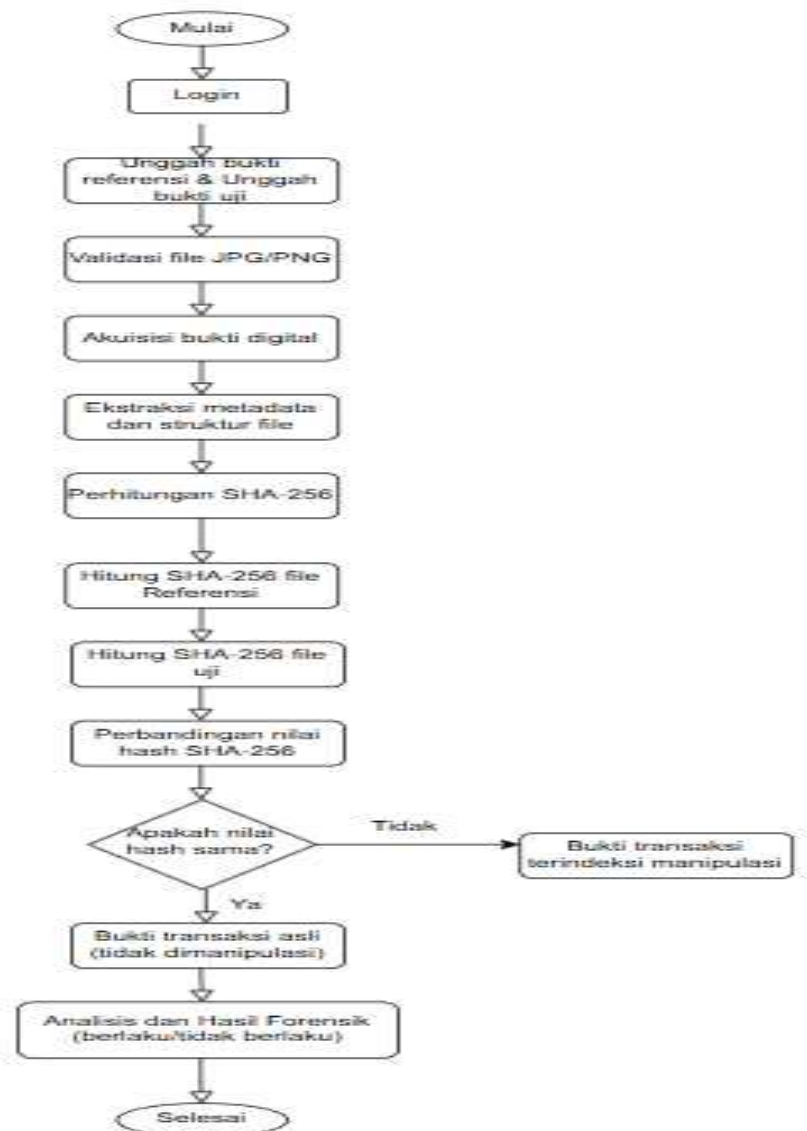
Gambar 3. 1 Tahapan penelitian

Kemudian dilakukan Desain Sistem yaitu UML, yaitu desain antarmuka. Setelah desain sistem selesai, penelitian dilanjutkan ke tahap implementasi sistem yang dilakukan sesuai dengan desain yang telah dirancang, termasuk penerapan algoritma hash SHA-256 untuk menghasilkan nilai hash dari dokumen transaksi QRIS. Sistem dibuat untuk memproses unggahan dokumen, melakukan perhitungan hash, dan menampilkan hasil verifikasi keaslian dokumen.

Tahap selanjutnya adalah pengujian sistem, yang dilakukan untuk memastikan sistem berfungsi sesuai dengan tujuan penelitian. Pengujian dilakukan dengan menggunakan dokumen transaksi QRIS asli dan dokumen yang

telah dimanipulasi. Hasil pengujian dianalisis berdasarkan perbedaan nilai hash SHA-256 untuk membuktikan kemampuan sistem dalam mendeteksi perubahan atau manipulasi pada dokumen digital.

3.3 Flowchart Sistem



Gambar 3. 2 Flowchart Sistem SHA-256

Flowchart tersebut menggambarkan alur kerja sistem dalam melakukan verifikasi keaslian bukti transaksi digital. Proses dimulai dari tahap “Mulai”, kemudian pengguna melakukan “login” ke dalam sistem sebagai bentuk

otentikasi. Setelah berhasil masuk, pengguna diminta untuk mengunggah dua file, yaitu “bukti referensi” (sebagai data pembanding) dan “bukti uji” (data yang akan diperiksa).

Selanjutnya, sistem melakukan “validasi format file” untuk memastikan bahwa file yang diunggah sesuai dengan ketentuan, yaitu berformat JPG atau PNG. Apabila file valid, proses dilanjutkan ke tahap “akuisisi bukti digital”, yaitu pengambilan dan persiapan data file untuk dianalisis. Pada tahap berikutnya, sistem melakukan “ekstraksi metadata dan struktur file”, seperti ukuran file dan informasi pendukung lainnya. Setelah itu, sistem menghitung “nilai hash menggunakan algoritma SHA-256” untuk masing-masing file, baik file referensi maupun file uji. Nilai hash yang dihasilkan kemudian “dibandingkan” untuk mengetahui kesamaan antara kedua file tersebut. Jika nilai hash yang dihasilkan “sama”, maka dapat disimpulkan bahwa bukti transaksi tersebut “asli dan tidak mengalami manipulasi”. Namun, jika nilai hash “berbeda”, maka bukti transaksi dinyatakan “terindikasi telah dimanipulasi”. Sebagai tahap akhir, sistem menampilkan “hasil analisis forensik digital” yang menyatakan status keaslian bukti transaksi, apakah valid atau tidak. Setelah seluruh proses selesai dilakukan, sistem mencapai tahap “Selesai” sebagai penutup dari alur kerja.

Alur penelitian atau pola algoritma hash SHA-256 yaitu, sebagai berikut:

1. Unggah bukti referensi & unggah bukti uji

Pengguna mengunggah dua file, yaitu:

- Bukti referensi (file asli sebagai

pembandingan)

- Bukti uji (file yang ingin diperiksa keasliannya)

2. Validasi file JPG/PNG

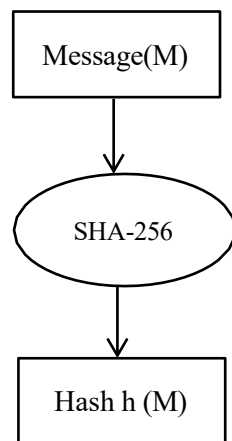
Sistem memeriksa apakah file yang diunggah memiliki format yang sesuai (JPG atau PNG). Jika tidak sesuai, maka proses tidak dapat dilanjutkan.

3. Akuisisi Bukti Digital, yaitu Sistem mengambil data dari file yang telah diunggah untuk diproses lebih lanjut dalam analisis forensik.

4. Selanjutnya, sistem melakukan ekstraksi metadata dan memeriksa struktur file. Metadata seperti tanggal transaksi, nominal pembayaran dan identitas pengirim yang digunakan dianalisis untuk menemukan indikasi ketidakwajaran yang dapat mengarah pada manipulasi dokumen.

5. Tahap berikutnya adalah perhitungan nilai hash SHA-256. Kemudian menghitung hash bukti transaksi pembayaran QRIS yang asli dan bukti transaksi pembayaran QRIS yang disalin kemudian diedit secara sengaja oleh peneliti. Setiap file bukti transaksi dihitung nilai hash-nya menggunakan fungsi hash SHA-256.

Secara matematis, proses hash dinyatakan sebagai:



Dimana:

H = nilai hash 256-bit

M = file bukti transaksi (JPG/PNG)

Nilai hash yang diperoleh pada tahap ini dijadikan sebagai nilai hash referensi (baseline) untuk proses verifikasi.

6. Tahap selanjutnya adalah Proses Perbandingan
Nilai Hash nilai hash file asli dibandingkan dengan nilai hash file hasil manipulasi. Kriteria verifikasi:
 - Jika $H_1 = H_2 \rightarrow$ Dokumen dinyatakan asli
(tidak mengalami perubahan)
 - Jika $H_1 \neq H_2 \rightarrow$ Dokumen terindikasi manipulasi

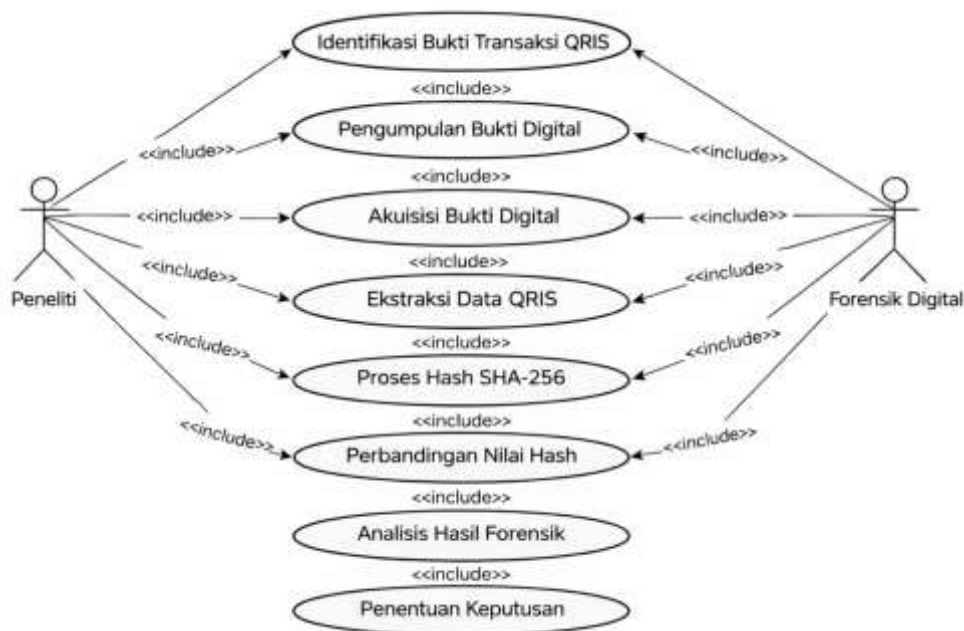
Perbedaan nilai hash menunjukkan adanya perubahan data, sesuai dengan sifat avalanche effect pada algoritma SHA-256 yang telah dijelaskan pada Bab II.

7. Analisis yaitu hasil verifikasi keaslian bukti

transaksi pembayaran QRIS, apakah dokumen Valid (hasil hash awal dan dokumen uji) identik. Atau apakah dokumen terindikasi mengalami perubahan atau manipulasi).

3.4 Pemodelan dan Perancangan Sistem

3.4.1 Use Case Diagram



Gambar 3. 3 Use Case Diagram

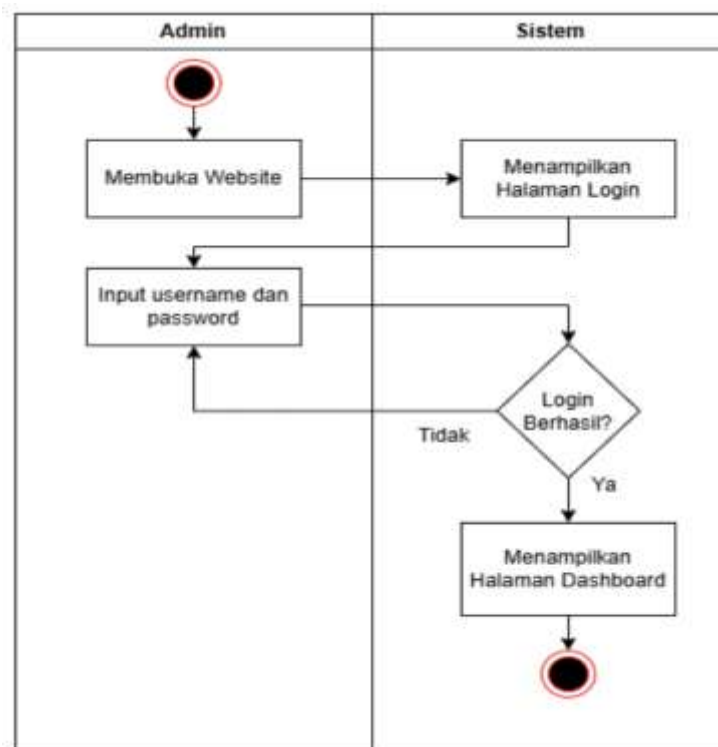
Diagram *use case* menggambarkan aktivitas yang dilakukan oleh aktor dalam sistem analisis forensik digital untuk verifikasi keaslian bukti transaksi pembayaran QRIS. Dalam hal ini, aktor yang terlibat yaitu peneliti atau analis forensik sebagai pengguna sistem. Proses diawali dengan identifikasi bukti transaksi QRIS yang akan diperiksa, kemudian dilanjutkan dengan pengumpulan dan akuisisi bukti digital guna menjamin keutuhan serta keaslian data. Setelah bukti digital diamankan, sistem melakukan ekstraksi data transaksi QRIS yang

terdapat pada dokumen digital.

Selanjutnya, peneliti menjalankan proses perhitungan nilai hash menggunakan algoritma SHA-256 terhadap dokumen digital yang diuji. Sistem kemudian membandingkan nilai hash yang dihasilkan untuk mendeteksi adanya perubahan atau manipulasi pada dokumen. Setelah proses perbandingan selesai, sistem akan menampilkan hasil analisis forensik yang menunjukkan status keaslian bukti transaksi QRIS. Pada tahap akhir, peneliti memperoleh informasi berupa keputusan akhir mengenai validitas bukti transaksi pembayaran QRIS yang telah dianalisis.

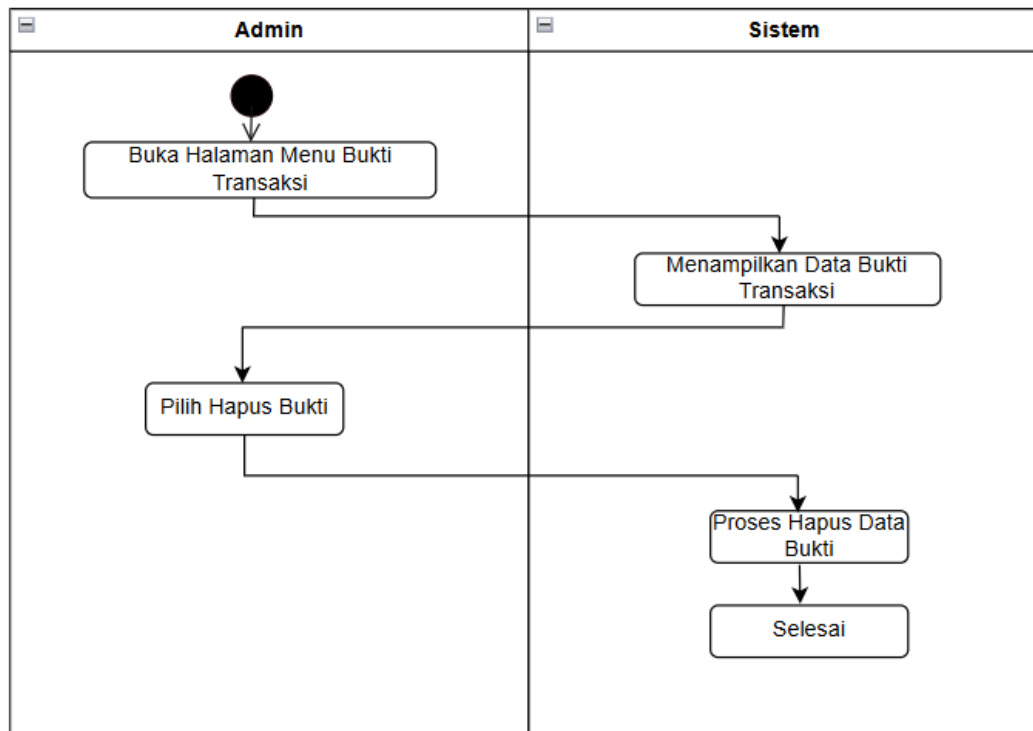
3.4.2 Activity Diagram

Admin akan masuk ke sistem dengan memasukkan username dan password, kemudian jika login berhasil, admin akan diarahkan ke halaman dashboard utama system.



Gambar 3. 4 Activity Diagram Login

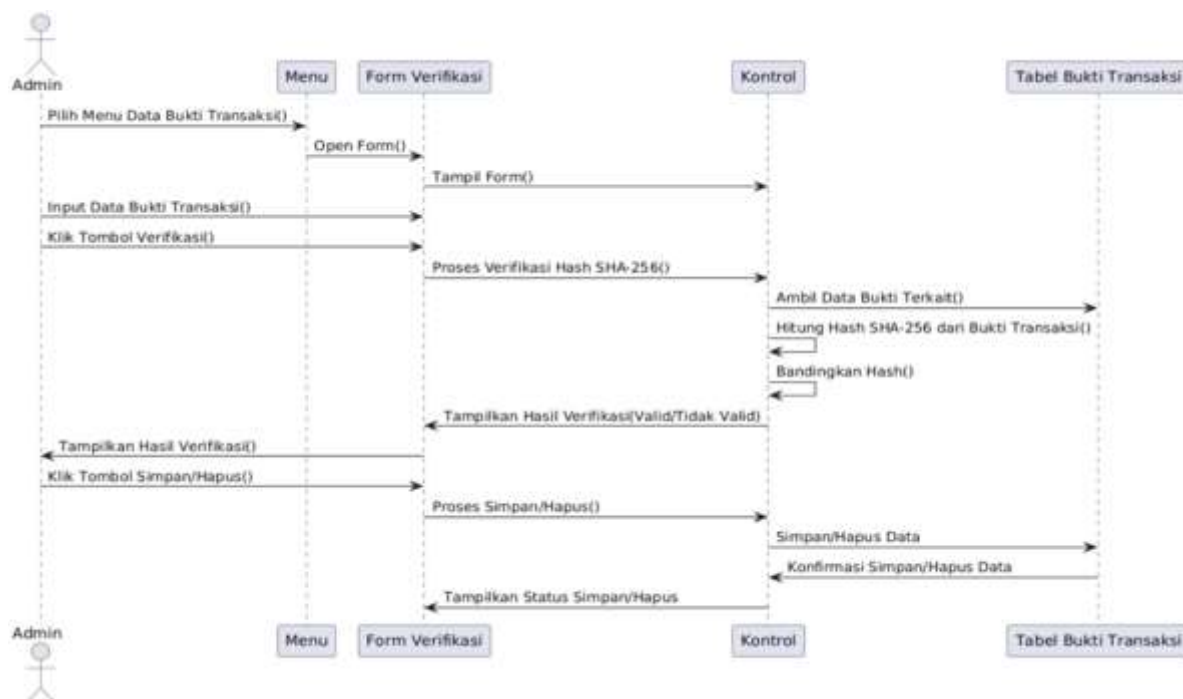
Gambar diatas menjelaskan alur proses login untuk seorang admin pada sebuah sistem. Proses dimulai ketika admin membuka website, yang kemudian diikuti oleh sistem menampilkan halaman login. Admin kemudian memasukkan username dan password pada halaman login tersebut. Sistem memeriksa apakah login berhasil atau tidak. Jika login berhasil, sistem akan menampilkan halaman dashboard.



Gambar 3. 5 Activity Diagram Hapus Transaksi

Proses dimulai ketika Admin membuka halaman menu bukti transaksi. Setelah itu, sistem menampilkan seluruh data bukti transaksi yang tersimpan di dalam basis data. Selanjutnya, admin memilih menghapus data dan sistem akan menjalankan proses penghapusan data bukti transaksi dari sistem.

3.4.3 Sequence Diagram



Gambar 3. 6 Sequence Diagram

Sequence diagram tersebut menggambarkan alur kerja sistem verifikasi keaslian bukti transaksi QRIS yang melibatkan Admin, Menu, Form Verifikasi, Kontrol, dan Tabel Bukti Transaksi. Proses dimulai ketika Admin memilih menu data bukti transaksi, kemudian sistem menampilkan Form Verifikasi untuk memasukkan data dan file bukti transaksi. Setelah Admin menekan tombol verifikasi, sistem melakukan proses analisis forensik melalui Kontrol dengan menghitung nilai hash SHA-256 dari bukti transaksi dan membandingkannya dengan data hash yang tersimpan. Hasil perbandingan hash tersebut menentukan status keaslian bukti transaksi, yaitu valid atau tidak valid.

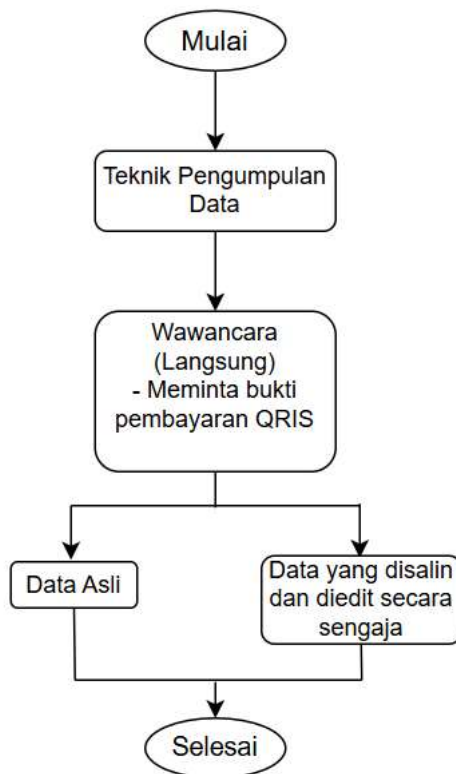
Hasil verifikasi kemudian ditampilkan kepada Admin. Selanjutnya, Admin dapat memilih untuk menyimpan atau menghapus data bukti transaksi. Sistem akan memproses permintaan tersebut dan memberikan konfirmasi status

penyimpanan atau penghapusan data. Dengan alur ini, sequence diagram menunjukkan bagaimana algoritma hash SHA-256 digunakan untuk mendeteksi manipulasi dokumen digital pada transaksi QRIS secara sistematis dan terstruktur.

3.5 Pengumpulan Data (*Collection*)

Tahap collection merupakan fase awal yang berfokus pada penghimpunan bukti digital yang akan diproses pada tahap berikutnya. Objek penelitian ini adalah bukti transaksi pembayaran QRIS dalam format JPG/PNG. Pengumpulan dilakukan dengan mengunduh bukti transaksi pembayaran QRIS secara langsung dari halaman produk sebagai bukti asli, kemudian disimpan. Dan dari bukti transaksi pembayaran QRIS asli tadi, kemudian di salin dan di edit secara sengaja oleh penulis sebagai upaya pengujian sistem.

Dalam penelitian ini, pengumpulan data dilakukan melalui wawancara terhadap teman atau pembeli untuk meminta sample data bukti transaksi pembayaran QRIS yang asli, yang bertujuan untuk memperoleh data yang relevan dengan topik penelitian. Teknik-teknik tersebut digunakan secara terintegrasi agar data yang diperoleh bersifat komprehensif dan mendukung proses analisis serta perancangan sistem verifikasi bukti transaksi pembayaran QRIS.



Gambar 3. 7 Teknik Pengumpulan Data

Data yang digunakan dalam penelitian ini terdiri dari:

1. Data Asli

File bukti transaksi QRIS hasil transaksi sah dalam format JPG/PNG.

2. Data Manipulasi

Salinan file asli yang telah dimodifikasi secara sengaja menggunakan pengedit gambar pada bagian nominal, tanggal transaksi, atau identitas pengirim untuk keperluan skenario pengujian.

3.6 Rancangan UI/UX

Rancangan layar dari Aplikasi Analisis Forensik Digital untuk Verifikasi Keaslian Bukti Transaksi Pembayaran QRIS Menggunakan Algoritma Hash SHA-256. Perancangan antarmuka pengguna (*User Interface*) dan pengalaman pengguna (*User Experience*) bertujuan untuk menghasilkan sistem yang mudah digunakan, informatif, dan mampu menyajikan hasil analisis forensik digital secara jelas dan akurat. Desain antarmuka difokuskan pada kesederhanaan tampilan, kemudahan navigasi, serta efisiensi proses verifikasi dokumen transaksi QRIS.

3.6.1 Rancangan Layar Halaman Login



Analisis Forensik Digital Untuk Verifikasi Keaslian Bukti Transaksi Pembayaran QRIS Menggunakan Algoritma Hash SHA-256 Sebagai Upaya Deteksi Manipulasi Dokumen Digital

Username / Email

Password Show

☐ Ingat Saya

LOGIN

[Lupa Password?](#)

Gambar 3. 8 Halaman Login

Halaman login merupakan tampilan awal aplikasi yang berfungsi sebagai pengaman akses sistem. Pengguna diharuskan memasukkan username dan kata sandi yang valid sebelum dapat mengakses fitur utama sistem. Rancangan UI dibuat sederhana dengan penempatan form login yang jelas, sehingga pengguna dapat melakukan autentikasi dengan cepat dan aman.

3.6.2 Rancangan Layar Dashboard



Gambar 3. 9 Halaman Dashboard

Halaman dashboard berfungsi sebagai pusat informasi utama setelah pengguna berhasil masuk ke sistem. Dashboard menampilkan ringkasan aktivitas sistem, seperti jumlah dokumen QRIS yang telah diverifikasi, status hasil verifikasi, serta notifikasi proses analisis. Rancangan UX pada halaman ini menekankan keterbacaan informasi dan kemudahan akses ke menu utama system.

3.6.3 Rancangan Layar Unggah QRIS

Sistem Forensik Digital Verifikasi QRIS

Dashboard
Unggah Bukti
Analisis Forensik
Data Bukti

Unggah Bukti

Unggah Bukti Transaksi QRIS

Pilih File Bukti

Nama File: Tanggal Transaksi:

Bukti harus format jpg, png.

UNGGAH BUKTI

Gambar 3. 10 Halaman Unggah Menggunakan QRIS

Halaman unggah dokumen dirancang untuk memudahkan pengguna dalam menginput bukti transaksi QRIS dalam bentuk file digital. Pengguna dapat memilih dan mengunggah dokumen transaksi yang akan dianalisis. Antarmuka dilengkapi dengan informasi format file yang diperbolehkan dan indikator proses unggah untuk meningkatkan pengalaman pengguna.

3.6.4 Rancangan Layar Hasil Verifikasi Keaslian Dokumen

Sistem Forensik Digital Verifikasi QRIS

[Dashboard](#)
[Unggah Bukti](#)
[Analisis Forensik](#)
[Data Bukti](#)

Hasil Verifikasi Transaksi QRIS

Detail Bukti Transaksi QRIS

Tanggal Transaksi:
Pengirim:
Penerima:

Nama **File Upload** Unduh

Hasil Verifikasi Keaslian Dokumen

Status:
Hash SHA-256 Asli:
Hash SHA-256 Terhitung:

[Analisis Forensik](#)

Gambar 3. 11 Hasil Verifikasi Dokumen

Halaman hasil verifikasi menampilkan informasi mengenai keaslian dokumen transaksi QRIS. Informasi yang ditampilkan meliputi nilai hash dokumen, status keaslian dokumen (asli atau terindikasi manipulasi), serta keterangan hasil analisis. Rancangan UX dibuat dengan visualisasi hasil yang jelas agar pengguna dapat dengan mudah memahami hasil verifikasi.

3.6.5 Rancangan Riwayat Verifikasi Dokumen

Sistem Forensik Digital Verifikasi QRIS

[Dashboard](#)
[Unggah Bukti](#)
[Analisis Forensik](#)
[Bukti Unggah](#)

Riwayat Verifikasi Dokumen

Riwayat Verifikasi QRIS

Tanggal:

No	Nama File	Tanggal	Pengirim/Penerima	Status
----	-----------	---------	-------------------	--------

Gambar 3. 12 Riwayat Verifikasi

Halaman riwayat verifikasi berfungsi untuk menampilkan daftar dokumen QRIS yang telah dianalisis sebelumnya. Informasi yang ditampilkan meliputi tanggal analisis, nama file, nilai hash, dan status verifikasi. Rancangan antarmuka dibuat dalam bentuk tabel yang terstruktur untuk memudahkan pencarian dan penelusuran data.

3.6.6 Rancangan Hapus Dokumen



Gambar 3. 13 Hapus Dokumen

Rancangan layar hapus dokumen digunakan untuk mendukung pengelolaan data pada sistem Analisis Forensik Digital untuk Verifikasi Keaslian Bukti Transaksi Pembayaran QRIS menggunakan Algoritma Hash SHA-256. Fitur ini dirancang sebagai mekanisme pengendalian data agar administrator dapat menghapus riwayat verifikasi dokumen pembayaran QRIS yang sudah tidak diperlukan, duplikat, atau tidak relevan, dengan tetap menjaga aspek keamanan dan kehati-hatian.

Pada tampilan ini, sistem menampilkan jendela konfirmasi (confirmation dialog) yang muncul ketika pengguna memilih aksi hapus pada data riwayat

verifikasi. Dialog konfirmasi dilengkapi dengan ikon peringatan berwarna merah yang berfungsi sebagai penanda visual bahwa tindakan yang akan dilakukan bersifat penting dan berisiko. Hal ini bertujuan untuk mencegah penghapusan data secara tidak sengaja. Pesan konfirmasi pada layar hapus dokumen dirancang menggunakan bahasa yang jelas dan tegas, yang menjelaskan bahwa penghapusan riwayat verifikasi bersifat permanen dan tidak dapat dibatalkan. Informasi ini sangat penting dalam konteks forensik digital, karena data verifikasi dapat menjadi bagian dari bukti atau arsip audit system.

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Kebutuhan Sistem

Kebutuhan sistem dalam penelitian ini disusun berdasarkan hasil analisis permasalahan serta perancangan sistem yang telah dijelaskan pada Bab III. Sistem yang dikembangkan bertujuan untuk mendukung proses analisis forensik digital dalam memverifikasi keaslian bukti transaksi pembayaran QRIS berbasis dokumen digital. Pendekatan yang digunakan dalam sistem ini adalah dengan menggunakan algoritma hash SHA-256 untuk mendeteksi adanya perubahan atau manipulasi pada file. Sistem harus mampu menerima input berupa file bukti transaksi, melakukan proses analisis terhadap file tersebut, serta menghasilkan output berupa status keaslian dokumen.

4.1.1 Kebutuhan Perangkat Lunak (*Software*)

Perangkat lunak yang digunakan dalam pengembangan sistem ini berfungsi sebagai platform untuk menjalankan aplikasi serta mendukung proses pengolahan data. Adapun perangkat lunak yang digunakan adalah:

1. Sistem operasi Windows

Sistem operasi ini berfungsi sebagai lingkungan utama untuk menjalankan seluruh perangkat lunak pendukung, termasuk web server dan database.

2. Visual Studio Code

Visual Studio Code digunakan sebagai perangkat lunak editor kode sumber dalam proses pengembangan sistem.

3. Python

Python digunakan sebagai bahasa pemrograman utama dalam membangun sistem.

4. SQLite

SQLite digunakan sebagai sistem manajemen basis data untuk menyimpan data yang digunakan.

5. Tesseract OCR

Tesseract OCR digunakan sebagai engine pembacaan teks otomatis dari dokumen gambar.

6. Pytesseract

Pytesseract merupakan library Python yang digunakan sebagai penghubung antara aplikasi Python dengan Tesseract OCR. Library ini digunakan agar sistem dapat memanggil engine OCR langsung dari kode program Python, lalu memproses hasil pembacaan teks untuk analisis lebih lanjut.

7. HTML

HTML digunakan untuk membangun struktur halaman antarmuka pengguna pada sistem.

8. Web Browser (Google Chrome / Microsoft Edge)

Browser digunakan untuk mengakses dan menjalankan aplikasi berbasis web yang dibangun.

9. PowerShell / Terminal

PowerShell atau terminal digunakan untuk menjalankan perintah-perintah pengembangan dan eksekusi sistem.

10. Alat pengedit gambar

Disini dibutuhkan alat pengedit gambar untuk dokumen uji seperti: Adobe Photo Photoshop.

4.1.2 Kebutuhan Data

Data yang digunakan dalam penelitian ini merupakan elemen penting dalam proses pengujian sistem. Data yang digunakan terdiri dari dua jenis, yaitu:

1. **Data asli**, yaitu file bukti transaksi QRIS asli yang tidak mengalami perubahan atau manipulasi. Data asli inilah yang dijadikan sebagai referensi, yang dihitung dengan SHA-256 untuk mendapatkan hash awal (asli). Data ini digunakan oleh peneliti dalam penelitian sebanyak 34 bukti transaksi pembayaran QRIS yang asli.
2. **Data manipulasi**, yaitu salinan dari file asli yang dimodifikasi atau diedit secara sengaja oleh peneliti, baik pada bagian nominal transaksi, tanggal, atau identitas pengirim. Data ini juga digunakan oleh peneliti dalam penelitian sebanyak 34 sampel.

Data manipulasi dibuat secara sengaja untuk menguji kemampuan sistem dalam mendeteksi perubahan yang terjadi pada dokumen digital. Perbandingan antara kedua jenis data tersebut akan menunjukkan efektivitas algoritma SHA-256 dalam menjaga integritas data.

4.1.3 Kebutuhan Fungsional Sistem

Kebutuhan fungsional merupakan kebutuhan yang berkaitan langsung dengan fungsi utama sistem. Sistem yang dibangun dalam penelitian ini harus mampu menjalankan beberapa fungsi berikut:

1. Melakukan proses autentikasi pengguna melalui halaman login.
2. Mengunggah file bukti transaksi QRIS dalam format gambar (JPG/PNG).
3. Melakukan ekstraksi metadata sebagai informasi pendukung analisis.
4. Menghitung nilai hash SHA-256 dari file yang diunggah.
5. Menyimpan data file dan nilai hash ke dalam database.
6. Membandingkan nilai hash antara dokumen yang diuji dengan dokumen referensi.
7. Menampilkan hasil verifikasi berupa status keaslian dokumen.

4.1.4 Kebutuhan Non-Fungsional

Selain kebutuhan fungsional, sistem juga harus memenuhi kebutuhan non-fungsional, yaitu:

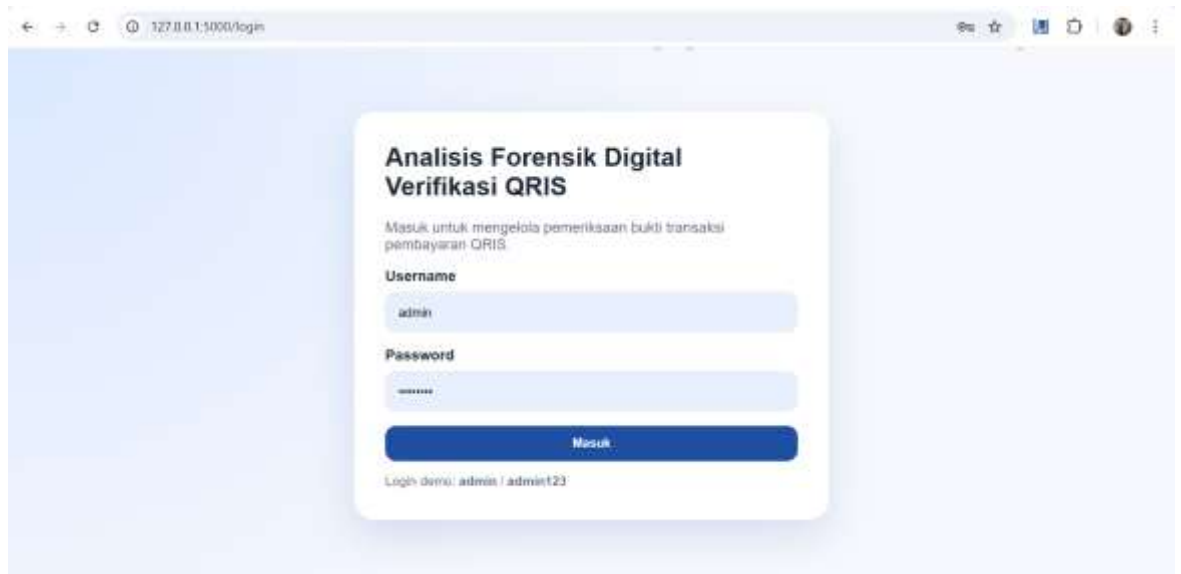
1. Sistem memiliki tampilan antarmuka yang sederhana dan mudah digunakan oleh pengguna.
2. Proses pengolahan data dilakukan secara cepat dan efisien.
3. Sistem mampu menjaga keamanan data melalui mekanisme login.
4. Sistem dapat berjalan secara stabil tanpa mengalami error yang signifikan.

Dengan terpenuhinya kebutuhan non-fungsional tersebut, sistem diharapkan dapat memberikan pengalaman penggunaan yang baik serta hasil analisis yang akurat.

4.2 Implementasi Sistem

Implementasi sistem merupakan tahap penerapan hasil perancangan sistem ke dalam bentuk aplikasi yang dapat digunakan secara langsung. Sistem yang dikembangkan dalam penelitian ini berbasis web, sehingga dapat diakses melalui browser tanpa memerlukan instalasi tambahan pada sisi pengguna.

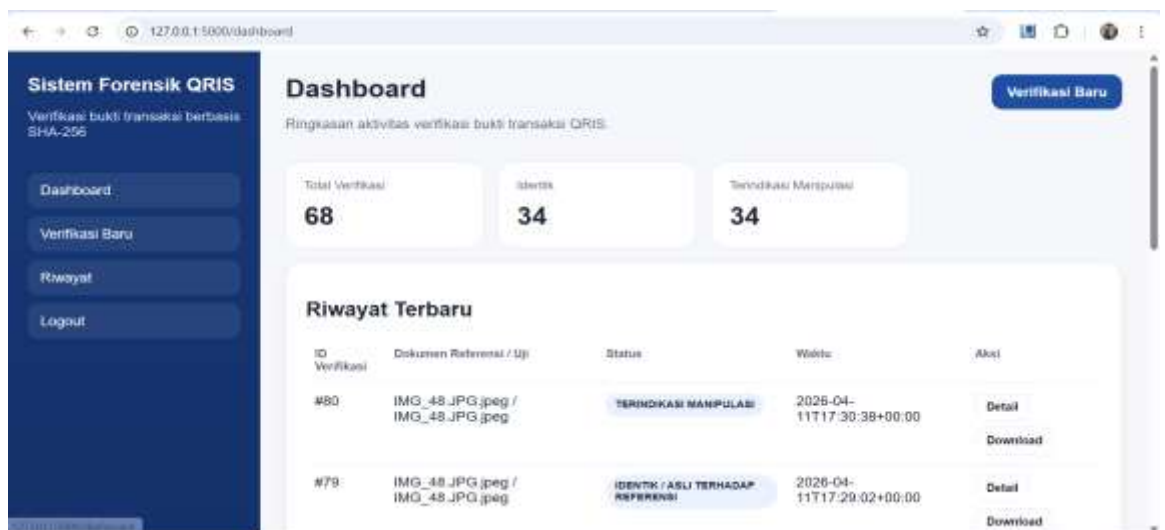
a. Halaman Login



Gambar 4. 1 Halaman Login

Halaman login digunakan sebagai awal untuk mengakses sistem. Pengguna diharuskan memasukkan username dan password yang valid. Seperti diatas Username: admin, dan Password: admin123. Kemudian pilih menu “Masuk ke Sistem”, setelah itu akan di arahkan ke tampilan Dashboard. Tujuan dari halaman ini adalah untuk menjaga keamanan sistem agar hanya dapat diakses oleh pihak yang berwenang.

b. Halaman Dashboard



Gambar 4. 2 Halaman Dashboard

Halaman Dashboard pada Sistem Forensik QRIS berfungsi sebagai pusat informasi utama yang menampilkan ringkasan aktivitas verifikasi bukti transaksi secara cepat dan terstruktur. Pada halaman ini, pengguna dapat melihat jumlah keseluruhan proses verifikasi yang telah dilakukan, yaitu 68 verifikasi, dengan rincian 34 dokumen dinyatakan identik atau asli terhadap referensi dan 34 dokumen terindikasi manipulasi. Selain itu, dashboard juga menyediakan bagian Riwayat Terbaru yang menampilkan data verifikasi terkini, meliputi ID verifikasi, nama dokumen referensi dan dokumen uji, status hasil pemeriksaan, waktu verifikasi, serta aksi lanjutan berupa tombol detail dan unduh hasil. Dengan tampilan ini, dashboard memudahkan pengguna dalam memantau hasil analisis, mengevaluasi kondisi dokumen yang diperiksa, serta mengakses riwayat verifikasi secara efisien.

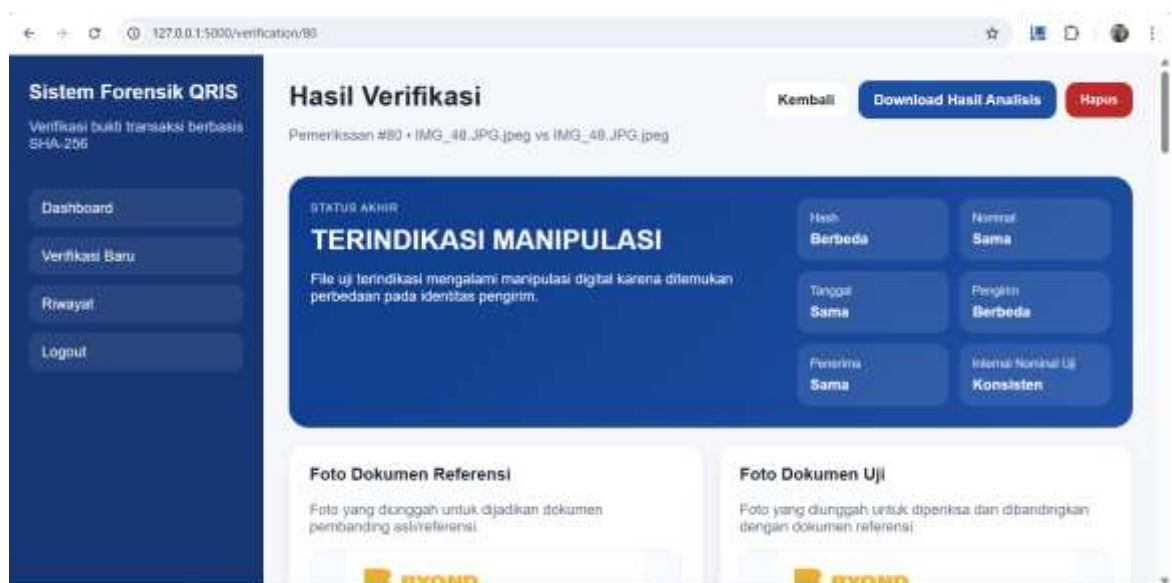
c. Halaman Unggah Bukti



Gambar 4. 3 Halaman Unggah Bukti QRIS

Halaman Unggah Bukti QRIS merupakan halaman input yang digunakan untuk melakukan proses verifikasi baru terhadap bukti transaksi QRIS. Pada halaman ini, pengguna diminta mengunggah dua jenis dokumen, yaitu Dokumen Referensi sebagai data pembanding dan Dokumen Uji sebagai data yang akan diperiksa keasliannya. Sedangkan tombol Proses Verifikasi di bagian bawah berfungsi untuk memulai analisis dan menentukan apakah bukti transaksi yang diuji identik dengan referensi atau terindikasi mengalami manipulasi.

d. Halaman Hasil Verifikasi



Gambar 4. 4 Halaman Hasil Verifikasi

Halaman Hasil Verifikasi merupakan halaman yang menampilkan keluaran akhir dari proses pemeriksaan bukti transaksi QRIS setelah data referensi dan dokumen uji dianalisis oleh sistem. Pada halaman ini, pengguna dapat melihat status akhir verifikasi secara ringkas, disertai indikator perbandingan beberapa komponen data untuk menunjukkan bagian mana yang sesuai atau berbeda antara kedua dokumen. Selain itu, halaman ini juga menyediakan tampilan foto dokumen referensi dan dokumen uji agar pengguna dapat melakukan peninjauan visual

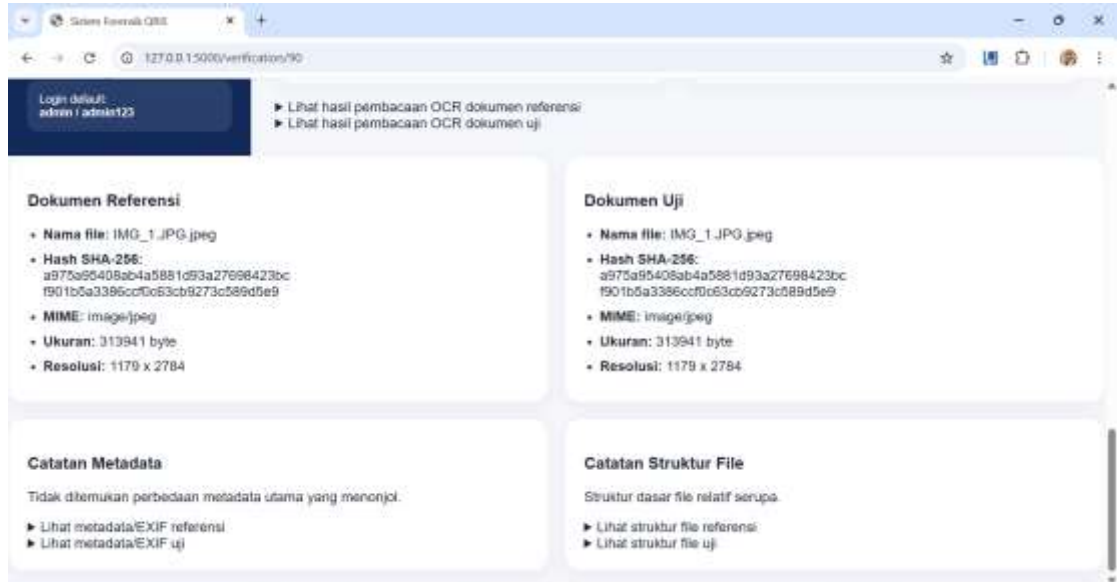
terhadap hasil pemeriksaan. Di bagian atas tersedia tombol aksi seperti kembali, mengunduh hasil analisis, dan menghapus data verifikasi, sehingga pengguna dapat mengelola hasil pemeriksaan dengan lebih mudah. Secara keseluruhan, halaman ini berfungsi sebagai pusat informasi akhir yang membantu pengguna memahami hasil verifikasi secara cepat, jelas, dan terstruktur.



Gambar 4. 5 Halaman Hasil Pembacaan Dokumen Referensi dan Detail Hasil Pembacaan Dokumen Uji

Pada tahap lanjutan proses verifikasi, sistem menampilkan hasil pembacaan teks dari dokumen referensi dan dokumen uji menggunakan OCR, yang berfungsi untuk mengekstraksi dan menampilkan isi informasi pada gambar seperti detail transaksi, waktu, dan identitas terkait secara visual. Hasil ini digunakan sebagai bahan pendukung agar pengguna dapat melihat isi dokumen secara lebih jelas dan melakukan perbandingan secara kasat mata antara kedua file. Namun demikian, proses penentuan keaslian dokumen tidak didasarkan pada hasil OCR, melainkan tetap mengacu pada perbandingan nilai hash menggunakan algoritma SHA-256 serta analisis struktur file seperti ukuran file, sehingga OCR

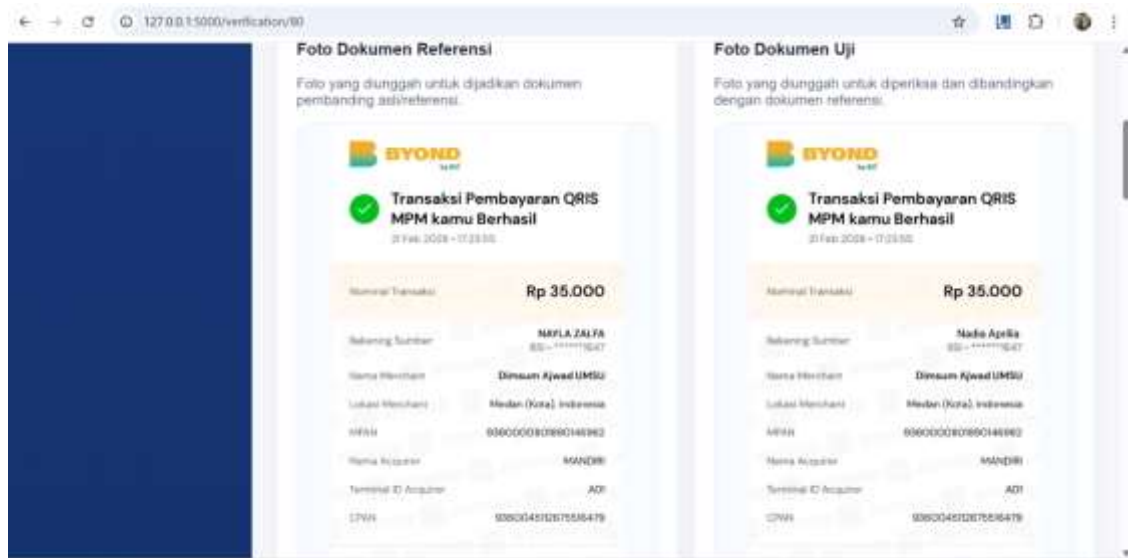
hanya berperan sebagai alat bantu pembacaan informasi, bukan sebagai metode utama dalam verifikasi integritas dokumen digital.



Gambar 4. 6 Halaman Detail Informasi Teknis Dokumen

Lanjutan hasil verifikasi, terdapat pula rincian teknis file seperti nama file, hash SHA-256, tipe file, ukuran, resolusi, metadata, dan struktur file, yang berfungsi untuk memperkuat proses verifikasi secara digital. Dengan demikian, lanjutan halaman ini memberikan gambaran analisis yang lebih menyeluruh dan mendukung pengguna dalam memahami dasar penentuan hasil verifikasi oleh sistem.

e. Halaman Bukti Transaksi QRIS



Gambar 4. 7 Halaman Tampilan Bukti Transaksi QRIS

Tampilan hasil bukti transaksi pembayaran QRIS pada halaman ini berfungsi untuk menyajikan perbandingan visual antara dokumen referensi dan dokumen uji secara berdampingan. Melalui tampilan ini, pengguna dapat melihat secara langsung informasi yang tercantum pada masing-masing bukti transaksi, seperti status transaksi, tanggal dan waktu, nominal pembayaran, identitas pengirim, nama merchant, lokasi merchant, serta data pendukung lainnya. Bagian ini juga mendukung hasil analisis sistem, karena tidak hanya menampilkan keputusan verifikasi secara otomatis, tetapi juga memberikan bukti visual yang membantu pengguna memahami dasar perbandingan yang dilakukan. Dengan demikian, halaman ini berperan penting dalam meningkatkan kejelasan, kemudahan pemeriksaan, dan kepercayaan pengguna terhadap hasil verifikasi yang ditampilkan.

f. Halaman Riwayat Verifikasi



Sistem Forensik QRIS
Verifikasi bukti transaksi berbasis SHA-256

Dashboard
Verifikasi Baru
Riwayat
Logout

Riwayat Verifikasi

Cari nama file atau status

Daftar seluruh pemeriksaan yang telah dilakukan.

ID	Dokumen	Status	Waktu	Aksi
#80	IMG_48.JPG.jpeg / IMG_48.JPG.jpeg	TERINCIKASI MANIPULASI	2026-04-11T17:30:36+00:00	Detail Download
#79	IMG_48.JPG.jpeg / IMG_48.JPG.jpeg	IDENTIK / ASLI TERHADAP REFERENSI	2026-04-11T17:29:02+00:00	Detail Download
#78	IMG_44.JPG.jpeg / IMG_44.JPG.jpeg	IDENTIK / ASLI TERHADAP REFERENSI	2026-04-11T17:27:12+00:00	Detail Download
#77	IMG_43.JPG.jpeg / IMG_43.JPG.jpeg	IDENTIK / ASLI TERHADAP REFERENSI	2026-04-11T17:25:37+00:00	Detail Download

Gambar 4. 8 Halaman Riwayat Verifikasi

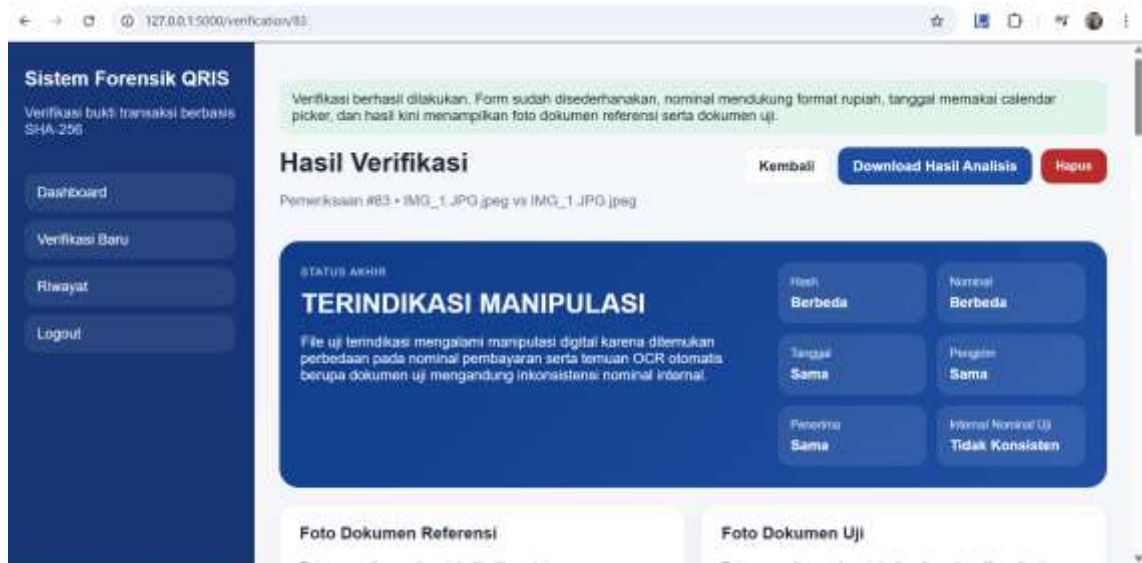
Halaman Riwayat Verifikasi berfungsi untuk menampilkan daftar seluruh hasil pemeriksaan bukti transaksi QRIS yang telah dilakukan oleh sistem. Pada halaman ini, pengguna dapat melihat informasi secara ringkas, meliputi ID verifikasi, nama dokumen, status hasil verifikasi, waktu pemeriksaan, serta aksi yang dapat dilakukan, seperti melihat detail hasil atau mengunduh laporan. Selain itu, tersedia fitur pencarian untuk memudahkan pengguna menemukan data verifikasi tertentu berdasarkan nama file atau status. Secara keseluruhan, halaman ini membantu pengguna dalam menelusuri, memantau, dan mengelola riwayat hasil verifikasi secara cepat, jelas, dan terstruktur.

4.3 Pengujian Sistem

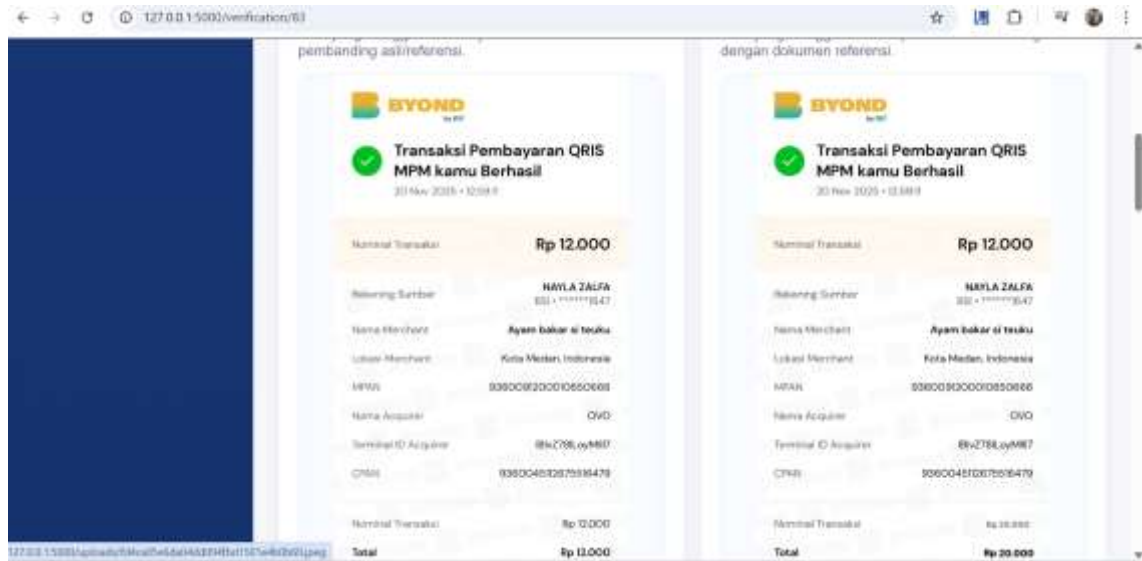
4.3.1 Pengujian sistem dokumen yang terindikasi manipulasi.



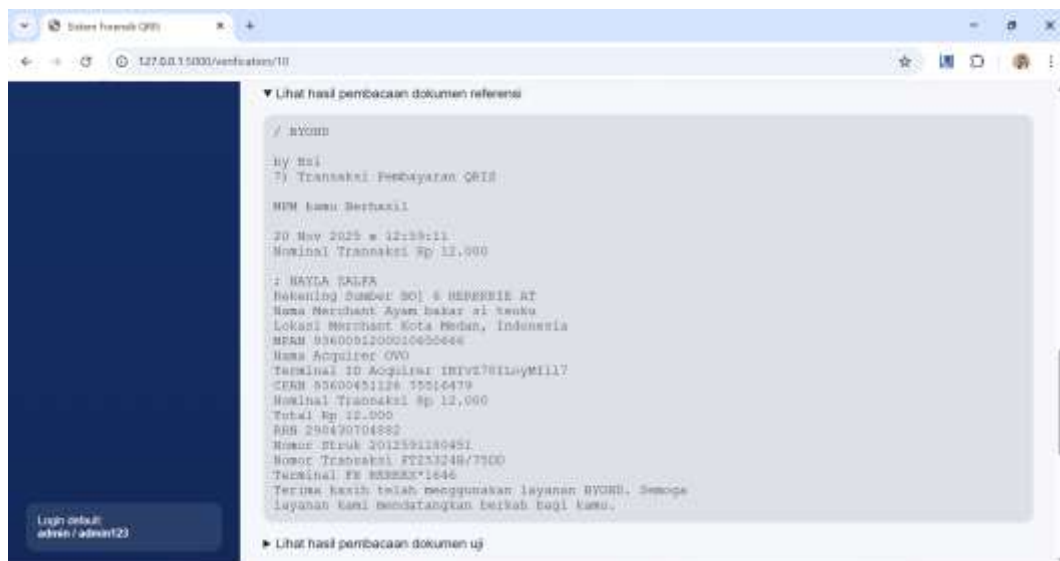
Halaman Unggah Bukti QRIS digunakan untuk memasukkan data yang akan diverifikasi oleh sistem. Terdapat dua bagian utama, yaitu Dokumen Referensi dan Dokumen Uji. Pada contoh ini, kedua file yang diunggah memiliki nama yang sama, yaitu IMG_1.JPG.jpeg. Halaman ini menunjukkan bahwa sebelum proses verifikasi dilakukan, sistem menerima masukan dokumen dan data transaksi yang akan dibandingkan.



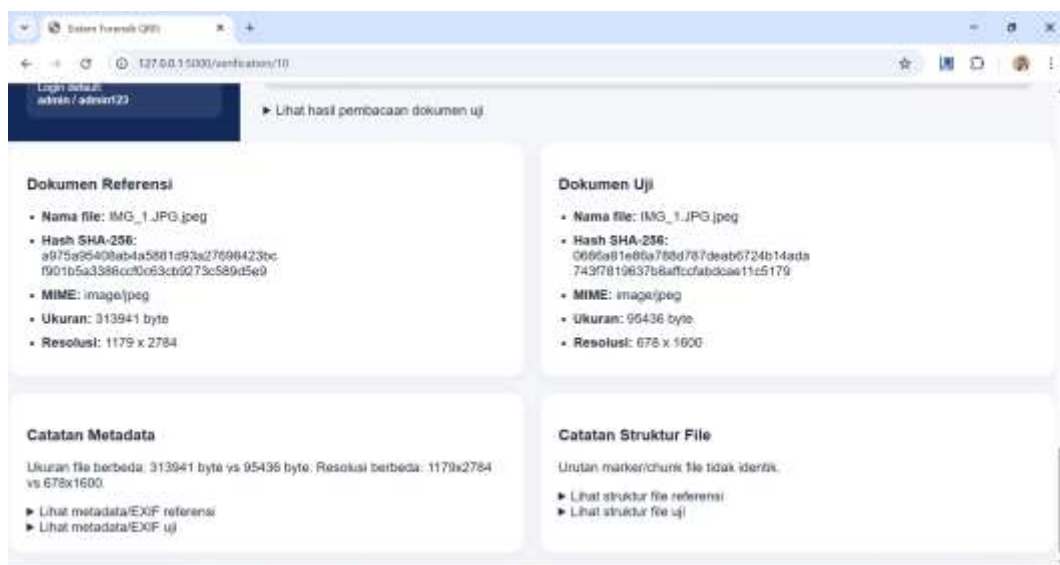
Sistem menampilkan hasil akhir pemeriksaan pada halaman Hasil Verifikasi. Status akhir yang ditunjukkan adalah “Terindikasi Manipulasi”. Kesimpulan ini diberikan karena sistem menemukan adanya perbedaan pada nominal pembayaran, meskipun beberapa komponen lain seperti tanggal, pengirim, dan penerima dinyatakan sama. Selain itu, bagian Hash juga dinyatakan berbeda, yang menunjukkan bahwa file referensi dan file uji tidak identik secara digital. Pada bagian Internal Nominal Uji, sistem menyatakan “Tidak Konsisten”, yang berarti terdapat ketidaksesuaian nilai nominal di dalam dokumen uji itu sendiri. Tampilan ini menegaskan bahwa sistem tidak hanya membandingkan data input, tetapi juga melakukan analisis isi dokumen dan karakteristik file.



Sistem menampilkan foto dokumen referensi dan foto dokumen uji secara berdampingan. Secara visual, kedua bukti transaksi tampak hampir sama dalam susunan dan format tampilannya. Namun, apabila diperhatikan lebih lanjut, terdapat perbedaan pada bagian nominal transaksi. Pada dokumen referensi, nominal yang terlihat adalah Rp12.000, sedangkan pada dokumen uji terdapat perubahan sehingga bagian bawah dokumen menunjukkan nilai Rp20.000. Tampilan ini berfungsi sebagai pembandingan visual agar pengguna dapat melihat secara langsung perbedaan yang menjadi dasar penilaian sistem.



Sistem menampilkan hasil pembacaan teks dari dokumen referensi dan dokumen uji menggunakan OCR, yang berfungsi untuk mengekstraksi dan menampilkan isi informasi pada gambar seperti detail transaksi, waktu, dan identitas terkait secara visual. Hasil ini digunakan sebagai bahan pendukung agar pengguna dapat melihat isi dokumen secara lebih jelas dan melakukan perbandingan secara kasat mata antara kedua file. Namun demikian, proses penentuan keaslian dokumen tidak didasarkan pada hasil OCR.



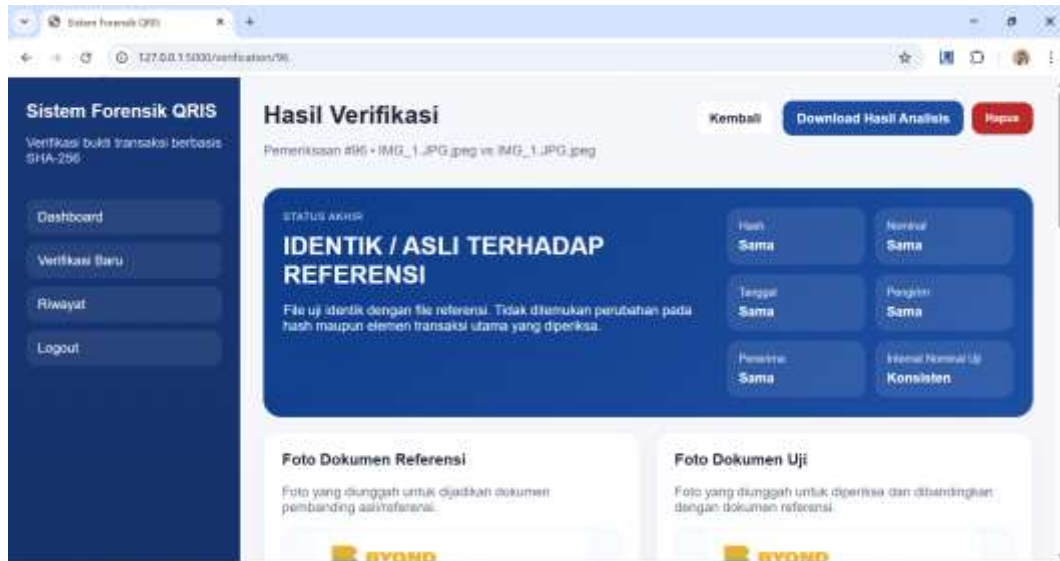
Sistem menampilkan rincian teknis dari kedua file. Untuk dokumen referensi, ukuran file adalah 313.914 byte dengan resolusi 1179 x 2784, sedangkan dokumen uji memiliki ukuran 95.436 byte dengan resolusi 678 x 1600. Nilai hash SHA-256 keduanya juga berbeda. Selain itu, data efektif yang terbaca menunjukkan bahwa nominal efektif dokumen referensi adalah Rp12.000, sedangkan nominal efektif dokumen uji adalah Rp20.000. Pada bagian bawah juga terdapat Catatan Metadata yang menyatakan adanya perbedaan ukuran file dan resolusi, serta Catatan Struktur File yang menunjukkan bahwa urutan marker atau chunk file tidak identik. Informasi ini memperkuat hasil analisis bahwa

dokumen uji memiliki perbedaan teknis dan isi dibandingkan dokumen referensi. Secara keseluruhan, sistem menyimpulkan bahwa dokumen uji terindikasi mengalami manipulasi, terutama karena terdapat perubahan nominal transaksi, inkonsistensi nominal internal, serta perbedaan hash, ukuran, resolusi, metadata, dan struktur file, meskipun beberapa informasi lain seperti tanggal, pengirim, dan penerima masih tetap sama.

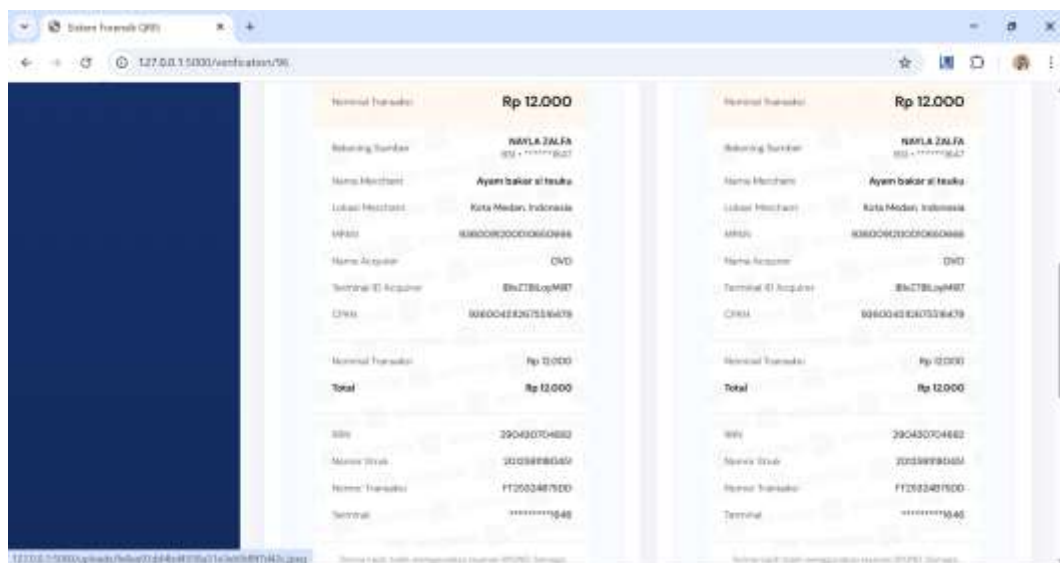
4.3.2 Pengujian sistem dokumen yang identik/asli.



Sistem menampilkan halaman Unggah Bukti QRIS yang digunakan untuk memasukkan data sebelum proses verifikasi dilakukan. Pada halaman ini, pengguna mengunggah dokumen referensi dan dokumen uji yang sama-sama menggunakan file IMG_1.JPG.jpeg. Tampilan ini menunjukkan bahwa sistem menerima dua dokumen dengan data yang identik untuk kemudian diproses lebih lanjut dalam tahap verifikasi.



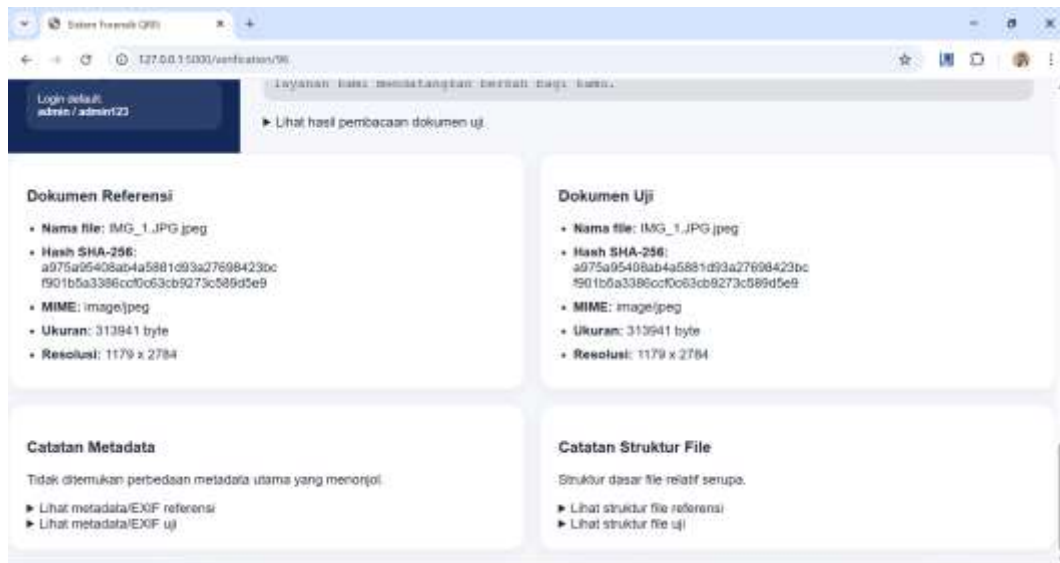
Sistem menampilkan halaman Hasil Verifikasi dengan status akhir “Identik / Asli terhadap Referensi”. Hasil ini menunjukkan bahwa dokumen uji dinyatakan sama dengan dokumen referensi dan tidak ditemukan perubahan pada komponen utama yang diperiksa. Hal ini diperkuat oleh indikator di sisi kanan yang seluruhnya menunjukkan hasil sama, yaitu pada hash, nominal, tanggal, pengirim, dan penerima, serta status konsistensi nominal internal dokumen uji yang dinyatakan konsisten. Dengan demikian, sistem menyimpulkan bahwa dokumen uji tidak terindikasi mengalami manipulasi.



Sistem menampilkan foto dokumen referensi dan foto dokumen uji secara berdampingan. Dari tampilan visual tersebut, kedua bukti transaksi memiliki isi yang sama, termasuk nominal transaksi Rp12.000, tanggal transaksi, nama pengirim, nama merchant, dan elemen informasi lainnya. Penyajian ini berfungsi sebagai pembandingan visual agar pengguna dapat melihat secara langsung bahwa dokumen referensi dan dokumen uji memiliki tampilan serta informasi transaksi yang identik.



Sistem menampilkan hasil pembacaan teks dari dokumen referensi dan dokumen uji menggunakan OCR, yang berfungsi untuk mengekstraksi dan menampilkan isi informasi pada gambar seperti detail transaksi, waktu, dan identitas terkait secara visual. Hasil ini digunakan sebagai bahan pendukung agar pengguna dapat melihat isi dokumen secara lebih jelas dan melakukan perbandingan secara kasat mata antara kedua file. Namun demikian, proses penentuan keaslian dokumen tidak didasarkan pada hasil OCR.



Sistem menampilkan rincian teknis dari dokumen referensi dan dokumen uji. Pada kedua dokumen, sistem menampilkan informasi yang sama, yaitu nama file IMG_1.JPG.jpeg, hash SHA-256 yang identik, MIME type image/jpeg, ukuran file 313.941 byte, resolusi 1179 x 2784. Pada bagian Catatan Metadata, sistem menyatakan bahwa tidak ditemukan perbedaan metadata utama yang menonjol, sedangkan pada Catatan Struktur File dijelaskan bahwa struktur dasar file relatif serupa. Halaman ini semakin memperkuat hasil verifikasi bahwa kedua dokumen memiliki karakteristik teknis yang sama dan tidak menunjukkan indikasi manipulasi.

Secara keseluruhan, sistem menyimpulkan bahwa dokumen uji identik dengan dokumen referensi. Kesimpulan ini didasarkan pada kesamaan hash SHA-256, nominal transaksi, tanggal transaksi, identitas pengirim, identitas penerima, konsistensi nominal internal, metadata, serta struktur file, sehingga dokumen dinyatakan asli terhadap referensi dan tidak terindikasi mengalami manipulasi.

4.3.3 Pengujian Blackbox Testing

Tabel 4. 1 Pengujian Blackbox Testing

No	Fitur	Skenario Pengujian	Data Uji / Input	Hasil yang Diharapkan	Hasil Pengujian	Status
1	Dashboard	Membuka halaman dashboard	Pengguna mengakses halaman dashboard	Sistem menampilkan total verifikasi, jumlah identik, jumlah manipulasi, dan riwayat terbaru	Halaman dashboard tampil dengan informasi ringkasan verifikasi	Berhasil
2	Verifikasi Baru	Membuka halaman verifikasi baru	Klik menu Verifikasi Baru	Sistem menampilkan form unggah bukti QRIS	Form unggah dokumen referensi dan dokumen uji berhasil ditampilkan	Berhasil
3	Upload dokumen referensi	Mengunggah file referensi	File IMG_1.JPG.jpg	File referensi berhasil diunggah ke sistem	File referensi berhasil dimuat pada form	Berhasil
4	Upload dokumen uji	Mengunggah file uji	File IMG_1.JPG.jpg	File uji berhasil diunggah ke sistem	File uji berhasil dimuat pada form	Berhasil
5	Proses verifikasi	Menjalankan verifikasi dokumen	Klik tombol Proses Verifikasi	Sistem memproses dokumen dan menampilkan hasil verifikasi	Hasil verifikasi berhasil ditampilkan	Berhasil
6	Status akhir verifikasi	Membandingkan dokumen referensi dan uji	Referensi Rp12.000, uji Rp20.000	Sistem menampilkan status Terindikasi Manipulasi	Status akhir tampil Terindikasi Manipulasi	Berhasil
7	Perbandingan hash	Membandingkan hash SHA-256 kedua file	Dokumen referensi dan dokumen uji	Sistem mendeteksi hash file berbeda	Hasil hash tampil Berbeda	Berhasil
8	Perbandingan nominal	Membandingkan nominal	Referensi Rp12.000, uji Rp20.000	Sistem mendeteksi nominal	Hasil nominal tampil	Berhasil

		transaksi		berbeda	Berbeda	
9	Perbandingan visual dokumen	Menampilkan gambar referensi dan uji	Dua gambar bukti transaksi	Sistem menampilkan kedua gambar secara berdampingan	Gambar dokumen referensi dan uji tampil	Berhasil
10	Tabel perbandingan hasil analisis	Menampilkan hasil analisis per komponen	Data hasil verifikasi	Sistem menampilkan tabel perbandingan	Tabel analisis tampil dengan status sama/berbeda	Berhasil
11	Metadata file	Membandingkan data teknis file	Ukuran, resolusi, hash	Sistem menampilkan perbedaan metadata	Metadata menunjukkan ukuran dan resolusi berbeda	Berhasil
12	Struktur file	Membandingkan struktur internal file	Marker/chunk file	Sistem menampilkan hasil struktur file	Struktur file ditampilkan tidak identik	Berhasil
13	Riwayat verifikasi	Membuka halaman riwayat	Klik menu Riwayat	Sistem menampilkan seluruh data riwayat verifikasi	Halaman riwayat berhasil ditampilkan	Berhasil
14	Detail verifikasi	Membuka hasil detail verifikasi	Klik tombol Detail	Sistem menampilkan halaman detail hasil verifikasi	Halaman detail berhasil dibuka	Berhasil
15	Download hasil	Mengunduh hasil analisis	Klik tombol Download Hasil Analisis	Sistem mengunduh hasil analisis	Tombol download tersedia dan dapat digunakan	Berhasil

BAB V PENUTUP

5.1 Kesimpulan

Berdasarkan hasil analisis, perancangan, implementasi, dan pengujian sistem, penelitian ini berhasil membangun sistem analisis forensik digital untuk memverifikasi keaslian bukti transaksi pembayaran QRIS menggunakan algoritma hash SHA-256. Sistem yang dikembangkan mampu menganalisis elemen transaksi seperti nominal, waktu transaksi, identitas pengirim, dan identitas penerima untuk mengidentifikasi bagian yang mengalami perubahan pada dokumen bukti transaksi QRIS. Selain itu, penerapan algoritma SHA-256 terbukti mampu mendeteksi adanya perubahan pada dokumen digital melalui perbedaan nilai hash antara dokumen referensi dan dokumen uji, sehingga dapat digunakan sebagai dasar dalam proses verifikasi keaslian dokumen.

Sistem yang dibangun juga telah mampu menampilkan hasil verifikasi secara jelas dan terstruktur melalui informasi status dokumen, hasil perbandingan elemen transaksi, tampilan visual dokumen, metadata, dan struktur file. Berdasarkan hasil pengujian blackbox, seluruh fungsi utama sistem berjalan sesuai dengan yang diharapkan, sehingga dapat disimpulkan bahwa tujuan penelitian telah tercapai dan permasalahan yang dibahas pada Bab 1 mengenai verifikasi keaslian bukti transaksi QRIS yang rentan dimanipulasi telah berhasil dijawab melalui sistem yang dibangun. Dengan demikian, kombinasi algoritma SHA-256 dan analisis elemen transaksi dapat digunakan secara efektif untuk membantu

mendeteksi indikasi manipulasi pada bukti transaksi pembayaran QRIS secara digital.

5.2 Saran

Sistem yang telah dibangun masih dibatasi pada bukti transaksi QRIS dalam format gambar JPG dan PNG, sehingga pada penelitian selanjutnya disarankan agar sistem dapat dikembangkan untuk mendukung format dokumen lain, seperti PDF atau tangkapan layar dari berbagai aplikasi pembayaran digital. Selain itu, penelitian berikutnya juga dapat menambahkan perbandingan dengan algoritma hash lain atau metode analisis tambahan untuk mengetahui efektivitas dan akurasi sistem dalam mendeteksi perubahan dokumen digital.

Perlu dilakukan peningkatan pada teknik ekstraksi teks agar informasi transaksi dapat dibaca dengan lebih akurat. Di samping itu, sistem juga dapat dikembangkan dengan menambahkan fitur keamanan yang lebih baik, manajemen pengguna, serta integrasi dengan data transaksi digital yang lebih luas agar proses verifikasi dapat dilakukan secara lebih otomatis dan optimal. Dengan pengembangan tersebut, sistem diharapkan tidak hanya bermanfaat sebagai media penelitian, tetapi juga dapat diterapkan secara lebih nyata untuk membantu meminimalkan risiko manipulasi bukti transaksi pembayaran QRIS.

DAFTAR PUSTAKA

- Abdulloh, R. (2022). *7 Materi Pemrograman Web untuk Pemula*. Jakarta: PT Elex Media Komputindo.
- Albar, M. A. (2022). Implementasi Restful API Pada Sistem Informasi Tracer Study Universitas Mataram Berbasis Mobile. *Prosiding SAINTEK LPPM Universitas Mataram, Vol. 4 (2022)*, 27.
- Anamisa, D. R. (2020). *DASAR PEMROGRAMAN WEB Teori & Implementasi (HTML, CSS, Javascript, Bootstrap, Codeigniter)*. Malang: Media Nusa Creative.
- Bank Indonesia. (2020). *QRIS: Quick Response Code Indonesian Standard*. Jakarta: Bank Indonesia.
- Bank Indonesia. (2022). *Statistik Sistem Pembayaran Indonesia*. Jakarta: Bank Indonesia.
- Bhargav, A., Mathur, A., & Gupta, R. (2015). Secure hash algorithm: Review and analysis. *International Journal of Computer Applications*, 115(11), 20–24. <https://doi.org/10.5120/20206-2471>
- Carrier, B. (2005). *File system forensic analysis*. Upper Saddle River, NJ: Addison-Wesley.
- Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers and the internet* (3rd ed.). London: Academic Press.
- Dahlberg, T., Guo, J., & Ondrus, J. (2015). A critical review of mobile payment research. *Electronic Commerce Research and Applications*, 14(5), 265–284. <https://doi.org/10.1016/j.elerap.2015.07.006>
- Denso Wave. (2020). *QR code essentials*. Tokyo: Denso Corporation.

- Endelina. (2021). Implementasi algoritma SHA-256 dalam pengamanan data digital. *Jurnal Teknologi Informasi*, 5(2), 45–52.
- Hafiz Maulana Siagian, Nasution, M. I. P., & Triase. (2022). Implementasi Framework Bootstrap Pada Sistem Kerja Praktek Berbasis Web Responsive. *JSiI (Jurnal Sistem Informasi)*, 9(1), 6–11.
<https://doi.org/10.30656/jsii.v9i1.3922>
- Hutapea, B. T. (2022). Lot Sizing Material Requirement Planning Pada Produk Kipas Angin Portable dengan Metode Period Order Quantity (POQ). *Talenta Conference Series: Energy and Engineering (EE)*, 5(2), 718–722
- Ikhsan, D. (2021). *Pengantar kriptografi dan keamanan informasi*. Jakarta: Informatika.
- Jogiyanto, H. M. (2017). *Analisis dan desain sistem informasi*. Yogyakarta: Andi Offset.
- Kahn Academy, & Rivest, R. (2018). Public key cryptography concepts and applications. *MIT OpenCourseWare*.
- Khiaonarong, T., & Humphrey, D. (2019). Cash use across countries and the demand for central bank digital currency. *IMF Working Paper*, WP/19/46.
- Liputan6. (2022). GoPay jadi dompet digital paling banyak digunakan di Indonesia. Diakses dari <https://www.liputan6.com>
- Maqsood, F., Zahid, M., & Abbas, S. (2017). Public key cryptography: Applications and challenges. *International Journal of Computer Science and Information Security*, 15(3), 98–105.
- Menezes, A. J., Van Oorschot, P. C., & Vanstone, S. A. (2018). *Handbook of applied cryptography*. Boca Raton, FL: CRC Press.

- Mishkin, F. S. (2019). *The economics of money, banking, and financial markets* (12th ed.). Boston, MA: Pearson Education.
- NIST. (2015). *Secure hash standard (SHS)* (FIPS PUB 180-4). Gaithersburg, MD: National Institute of Standards and Technology.
- Otoritas Jasa Keuangan. (2022). *Statistik fintech lending dan sistem pembayaran digital*. Jakarta: OJK.
- Ozili, P. K. (2018). Impact of digital finance on financial inclusion and stability. *Borsa Istanbul Review*, 18(4), 329–340. <https://doi.org/10.1016/j.bir.2017.12.003>
- Pressman, R. S. (2014). *Software engineering: A practitioner's approach* (8th ed.). New York, NY: McGraw-Hill.
- Rahmadanoor, R., & Normajatun. (2020). *Metodologi penelitian*. Banjarmasin: STIA Bina Banua Press.
- Roussos, G., & Kostakos, V. (2009). RFID in pervasive computing: State-of-the-art and outlook. *Pervasive and Mobile Computing*, 5(1), 110–131. <https://doi.org/10.1016/j.pmcj.2008.03.004>
- Rukin. (2022). *Metodologi penelitian kualitatif*. Yogyakarta: Zahir Publishing.
- Sitohang, N. (2019). Penerapan Customer Relationship Management Pada Sistem Informasi Penjualan (Studi Kasus Lavas Kopi Kisaran). *Ready Star -2*, 2(1), 224–234.
- Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Boston, MA: Pearson Education.
- Suendri. (2022). Implementasi Diagram UML (Unified Modelling Language) Pada Perancangan Sistem Informasi Remunerasi Dosen Dengan Database

- Oracle (Studi Kasus: UIN Sumatera Utara Medan). *Jurnal Ilmu Komputer Dan Informatika*.
- Sugiyono. (2019). *Metode penelitian dan pengembangan (research and development)*. Bandung: Alfabeta.
- Tanjung, M. A. P., & rekan. (2019). Klasifikasi kategori citra digital menggunakan metode bag of visual words. *Jurnal Teknologi Informasi*, 7(2), 85–92.
- Tanjung, M. A. P., & rekan. (2020). Kian Santang game: Digital storytelling untuk edukasi sejarah. *Jurnal Media Informatika*, 6(1), 11–18.
- Tanjung, M. A. P., & rekan. (2020). Lamp control system through android and WiFi. *Journal of Computer Engineering and Applications*, 5(1), 45–52.
- Tanjung, M. A. P., & rekan. (2022). Numerical analysis of variations distance formulas on k-nearest neighbors in classifying malaria parasite blood cells. *Journal of Informatics and Telecommunication Engineering*, 6(1), 120–128.
- Tanjung, M. A. P., & rekan. (2024). Implementasi natural language processing dalam perancangan aplikasi chatbot pada FIKTI UMSU. *Jurnal Mahasiswa Teknik Informatika (JATI)*, 8(1), 33–40.
- Tanjung, M. A. P., & rekan. (2024). Implementasi sistem monitoring kos berbasis Internet of Things (IoT) dengan sensor PIR. *Jurnal Mahasiswa Teknik Informatika (JATI)*, 8(2), 55–62.
- Undang-Undang Republik Indonesia Nomor 23 Tahun 1999 tentang Bank Indonesia. Qodri, A. Al. (2025). *ANALISIS FORENSIK DIGITAL TERHADAP PERDAGANGAN DATA PRIBADI DI DARK WEB MENGGUNAKAN OSINT & THREAT INTELLIGENCE*.
- Rivest, E., & Adleman, S. (2022). Penerapan konsep digital signature terhadap verifikasi keaslian dokumen transkrip nilai mahasiswa menggunakan enkripsi rivest shamir adleman. 8(1), 45–52.
<https://doi.org/10.55679/semantik.v8i1.21608>

LAMPIRAN

Lampiran 1. Form Revisi Sidang



UMSU
Unggul | Cerdas | Terpercaya

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi Unggul Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 174/SK/BDAN-PT/IA-P/PT/2024
 Pusat Administrasi: Jalan Muktihar Basri No. 3 Medan 20238 Telp. (061) 6623480 - 66224567 Fax. (061) 6625474 - 6631003

www.umsu.ac.id
 Email: info@umsu.ac.id
 [umsu.medan](https://www.facebook.com/umsu.medan)
 [umsu.medan](https://www.instagram.com/umsu.medan)
 [umsu.medan](https://www.youtube.com/channel/UC...)

FORMULIR PERBAIKAN UJIAN SKRIPSI

Pada hari ini, Sabtu 18 April 2026 telah dilaksanakan Ujian Skripsi bagi mahasiswa Fakultas Ilmu Komputer Dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara. Sbb:

Nama Mahasiswa : Adibah Salsabilah
 NPM : 2209010064
 Program Studi : Sistem Informasi
 Judul Proposal : Analisis Forensik Digital Untuk Verifikasi Keaslian Bukti Transaksi Pembayaran Qris Menggunakan Algoritma Hash SHA-256 Sebagai Upaya Deteksi Manipulasi Dokumen Digital

Materi/Point yang Diperbaiki :

		Paraf
Mahardika Prawira Tanjung, S.Kom., M.Kom.	—	
Rizaldy Khair, M.Kom	- Bukti dibatasi maksimal pakai OCR - Bagian ujungah bukti (input manual dihapus aja).	OK ✓  Rizaldy Khair J. Kom. M.Kom
Indah Purnama Sari, S.T., M.Kom	—	

Berita acara ini ditandatangani setelah skripsi diperbaiki sesuai petunjuk/arahan dari Pembimbing dan Penguji/Pembahas.

Lampiran 2. Turnitin Max 30%

ANALISIS FORENSIK DIGITAL UNTUK VERIFIKASI KEASLIAN BUKTI TRANSAKSI PEMBAYARAN QRIS MENGGUNAKAN ALGORITMA HASH SHA-256 SEBAGAI UPAYA DETEKSI MANIPULASI DOKUMEN DIGITAL

ORIGINALITY REPORT

28%	27%	12%	16%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	repository.umsu.ac.id Internet Source	5%
2	ojs.uho.ac.id Internet Source	2%
3	Submitted to Universitas Muhammadiyah Sumatera Utara Student Paper	1%
4	openjournal.unpam.ac.id Internet Source	1%
5	Submitted to Universitas Pamulang Student Paper	<1%
6	Submitted to Universitas Putera Batam Student Paper	<1%
7	repository.sar.ac.id Internet Source	<1%
8	jurusan.tik.pnj.ac.id Internet Source	<1%
9	Submitted to Universitas Putera Indonesia YPTK Padang Student Paper	<1%
10	eprints.pancabudi.ac.id Internet Source	

11	ejournal.unis.ac.id Internet Source	<1 %
12	Submitted to UIN Ar-Raniry Student Paper	<1 %
13	eprints.amikom.ac.id Internet Source	<1 %
14	repositori.uma.ac.id Internet Source	<1 %
15	text-id.123dok.com Internet Source	<1 %
16	ejurnal.umri.ac.id Internet Source	<1 %
17	repository.uinsu.ac.id Internet Source	<1 %
18	eprints.polsri.ac.id Internet Source	<1 %
19	journals.lcu.edu.ng Internet Source	<1 %
20	Submitted to KEDGE Business Schools Student Paper	<1 %
21	journal.unnes.ac.id Internet Source	<1 %
22	Submitted to King's Own Institute Student Paper	<1 %
23	grokipedia.com Internet Source	<1 %

repository.upi.edu

24	Internet Source	<1 %
25	www.scribd.com Internet Source	<1 %
26	digilib.uinsgd.ac.id Internet Source	<1 %
27	garuda.ristekbrin.go.id Internet Source	<1 %
28	ojs.trigunadharma.ac.id Internet Source	<1 %
29	repository.upiypk.ac.id Internet Source	<1 %
30	repository.upnvj.ac.id Internet Source	<1 %
31	journals.usm.ac.id Internet Source	<1 %
32	docplayer.com.br Internet Source	<1 %
33	e proceeding.undiksha.ac.id Internet Source	<1 %
34	ojs.uma.ac.id Internet Source	<1 %
35	repository.ar-raniry.ac.id Internet Source	<1 %
36	repository.mercubuana.ac.id Internet Source	<1 %
37	repository.untag-sby.ac.id Internet Source	<1 %
	digilib.unila.ac.id	

38	Internet Source	<1 %
39	pkm.lpkd.or.id Internet Source	<1 %
40	Submitted to Universitas Islam Riau Student Paper	<1 %
41	repository.ipb.ac.id Internet Source	<1 %
42	www.bundesbank.de Internet Source	<1 %
43	Submitted to Sharda University Student Paper	<1 %
44	Submitted to Universitas Sumatera Utara Student Paper	<1 %
45	docplayer.info Internet Source	<1 %
46	ejurnal.stmik-budidarma.ac.id Internet Source	<1 %
47	repository.ulb.ac.id Internet Source	<1 %
48	Submitted to Universitat Oberta de Catalunya Student Paper	<1 %
49	digilib.uinkhas.ac.id Internet Source	<1 %
50	hostjournals.com Internet Source	<1 %
51	repository.upnjatim.ac.id Internet Source	<1 %
	Submitted to Universitas Dharmawangsa	

52	Student Paper	<1 %
53	Submitted to Universitas Negeri Manado Student Paper	<1 %
54	etd.repository.ugm.ac.id Internet Source	<1 %
55	journal.eng.unila.ac.id Internet Source	<1 %
56	www.frontiersin.org Internet Source	<1 %
57	M Choirul Amri, Muhammad Farros Atiqi, Friza Talita, Ilka Zufria. "Implementasi Algoritma Naïve Bayes Untuk Klasifikasi Berita Online Terhadap Program Prioritas Pemerintah Kota Medan", DEVICE : JOURNAL OF INFORMATION SYSTEM, COMPUTER SCIENCE AND INFORMATION TECHNOLOGY, 2025 Publication	<1 %
58	Submitted to Universitas Sangga Buana YPKP Student Paper	<1 %
59	library.uis.ac.id Internet Source	<1 %
60	bogordaily.net Internet Source	<1 %
61	de.scribd.com Internet Source	<1 %
62	repository.uin-suska.ac.id Internet Source	<1 %
63	repository.wicida.ac.id	

	Internet Source	<1 %
64	www.researchgate.net Internet Source	<1 %
65	Submitted to Universitas Atma Jaya Yogyakarta Student Paper	<1 %
66	e-journal.kemensos.go.id Internet Source	<1 %
67	etheses.uin-malang.ac.id Internet Source	<1 %
68	lib.unnes.ac.id Internet Source	<1 %
69	www.sciencepubco.com Internet Source	<1 %
70	Submitted to Universitas Muhammadiyah Palembang Student Paper	<1 %
71	Submitted to Universitas Negeri Jakarta Student Paper	<1 %
72	files.eric.ed.gov Internet Source	<1 %
73	prin.or.id Internet Source	<1 %
74	tunasbangsa.ac.id Internet Source	<1 %
75	123dok.com Internet Source	<1 %
76	Submitted to Deptford Township High School Student Paper	<1 %

77	Submitted to Abdullah Gul University Student Paper	<1 %
78	Submitted to Saint Mary's University Student Paper	<1 %
79	Submitted to Universitas Islam Bandung Student Paper	<1 %
80	Submitted to Universitas Muhammadiyah Purwokerto Student Paper	<1 %
81	adaddanuarta.blogspot.com Internet Source	<1 %
82	digilib.esaunggul.ac.id Internet Source	<1 %
83	jogodebola.net Internet Source	<1 %
84	jurnal.atmaluhur.ac.id Internet Source	<1 %
85	jurnaluniv45sby.ac.id Internet Source	<1 %
86	repo.ukitoraja.ac.id Internet Source	<1 %
87	repository.uinjkt.ac.id Internet Source	<1 %
88	technoherbon.blogspot.com Internet Source	<1 %
89	Anton Sukma Wijaya, Gusmelia Testiana. "Perancangan UI/UX Website Menggunakan Figma di Politeknik Pariwisata Palembang",	<1 %

**RIGGS: Journal of Artificial Intelligence and
Digital Business, 2026**

Publication

90	Mega Chrstin Morys Lase, Vrenty Sri Berlian Nehe. "Sistem Grafic User Interface Aplikasi Berbasis Dekstop Penjualan Sederhana Menggunakan Java Netbeans", RIGGS: Journal of Artificial Intelligence and Digital Business, 2025 Publication	<1 %
91	Submitted to SDM Universitas Gadjah Mada Student Paper	<1 %
92	Submitted to Universitas Buana Perjuangan Karawang Student Paper	<1 %
93	barakati.id Internet Source	<1 %
94	elibrary.unikom.ac.id Internet Source	<1 %
95	epdf.pub Internet Source	<1 %
96	eprints.akakom.ac.id Internet Source	<1 %
97	indojurnal.com Internet Source	<1 %
98	repositori.usu.ac.id Internet Source	<1 %
99	repository.pnj.ac.id Internet Source	<1 %
100	www.rumahjurnal.or.id Internet Source	<1 %

		<1 %
101	Duni Paliling, Geris Siswanto, Innes Innes, Natalia Paranoan, Muliani Mangngalla. "Analisis Implementasi QRIS sebagai Sistem Pembayaran Digital pada Usaha Mikro, Kecil dan Menengah (UMKM) di Kelurahan Kapasa, Kota Makassar", RIGGS: Journal of Artificial Intelligence and Digital Business, 2026 Publication	<1 %
102	Submitted to Universitas Jenderal Achmad Yani Student Paper	<1 %
103	blog.unmaha.ac.id Internet Source	<1 %
104	ejournal.uin-suska.ac.id Internet Source	<1 %
105	id.123dok.com Internet Source	<1 %
106	repository.iainbengkulu.ac.id Internet Source	<1 %
107	repository.president.ac.id Internet Source	<1 %
108	smart.stmikplk.ac.id Internet Source	<1 %
109	teguh8581.wordpress.com Internet Source	<1 %
110	Delgio Liem Sorongan, Quido C Kainde, Sondy C Kumajas. "Web-Based Decision Support System for Determining the Best Employee Using the Simple Additive Weighting Method",	<1 %

Indonesian Journal of Innovation Studies,
2025

Publication

111	Dita Septasari. "ANALISIS ASOSIASI PILIHAN PROGRAM STUDI PENDAFTAR UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA JALUR MANDIRI MENGGUNAKAN ALGORITMA APRIORI", Aisyah Journal Of Informatics and Electrical Engineering (A.J.I.E.E), 2020 Publication	<1 %
112	docobook.com Internet Source	<1 %
113	dspace.uui.ac.id Internet Source	<1 %
114	journal.uwgm.ac.id Internet Source	<1 %
115	openlibrarypublications.telkomuniversity.ac.id Internet Source	<1 %
116	repository.unbari.ac.id Internet Source	<1 %
117	repository.unib.ac.id Internet Source	<1 %
118	Submitted to Universitas Muria Kudus Student Paper	<1 %
119	Submitted to Universitas Musamus Merauke Student Paper	<1 %
120	anzdoc.com Internet Source	<1 %
121	bkmattaqwa.uma.ac.id Internet Source	<1 %

Publication		
133	e-campus.lainbukittinggi.ac.id Internet Source	<1 %
134	ejurnal.seminar-id.com Internet Source	<1 %
135	ekonomi.uma.ac.id Internet Source	<1 %
136	ijaers.com Internet Source	<1 %
137	johannessimatupang.wordpress.com Internet Source	<1 %
138	jtiik.ub.ac.id Internet Source	<1 %
139	jurnal.pancabudi.ac.id Internet Source	<1 %
140	m.kaskus.co.id Internet Source	<1 %
141	ojs.stmik-banjarbaru.ac.id Internet Source	<1 %
142	repository.uinsaizu.ac.id Internet Source	<1 %
143	repository.unissula.ac.id Internet Source	<1 %
144	repository.unp.ac.id Internet Source	<1 %
145	Chycik Ayu Winata, Retno Mumpuni, Firza Prima Aditiawan. "PERANCANGAN SISTEM KLINIK KESEHATAN DAN INVENTORI OBAT DI KLINIK KESEHATAN GRATIS AL-MUHAJIRIN",	<1 %

Jurnal Informatika dan Teknik Elektro
Terapan, 2024

Publication

- | | | |
|-----|--|------|
| 146 | Vincent A. Dodd, Patrick M. Grace.
"Agricultural Engineering - Proceedings of the
Eleventh International Congress on
Agricultural Engineering, Dublin, 4-8
September 1989", CRC Press, 2026
Publication | <1 % |
| 147 | e-journal.uajy.ac.id
Internet Source | <1 % |
| 148 | Hurriyati Ratih, Tjahjono Benny,
GafarAbdullah Ade, Sulastri, Lisnawati.
"Advances in Business, Management and
Entrepreneurship", CRC Press, 2020
Publication | <1 % |
| 149 | Mar'atun Sa'diah. "Perception of Merchants
and Consumers Towards Payments Using
Qris for UMKM in Mataram", JURNAL
PENDIDIKAN IPS, 2024
Publication | <1 % |
| 150 | Maulidah Narastri. "FINANCIAL TECHNOLOGY
(FINTECH) DI INDONESIA DITINJAU DARI
PERSPEKTIF ISLAM", Indonesian
Interdisciplinary Journal of Sharia Economics
(IJSE), 2020
Publication | <1 % |
| 151 | doku.pub
Internet Source | <1 % |

Lampiran 3. Bukti Submit Jurnal



Diba Salsa <salsadiba210@gmail.com>

[syntax] Submission Acknowledgement

Ibnu Rusydi <ojs@dharmawangsa.ac.id>
Ke: Adibah Salsabilah <salsadiba210@gmail.com>

Sel, 12 Mei, 01.22

Adibah Salsabilah:

Thank you for submitting the manuscript, "ANALISIS FORENSIK DIGITAL UNTUK VERIFIKASI KEASLIAN BUKTI TRANSAKSI PEMBAYARAN QRIS MENGGUNAKAN ALGORITMA HASH SHA-256 SEBAGAI UPAYA DETEKSI MANIPULASI DOKUMEN DIGITAL" to Syntax : Journal of Software Engineering, Computer Science and Information Technology. With the online journal management system that we are using, you will be able to track its progress through the editorial process by logging in to the journal web site:

Manuscript URL:
<https://jurnal.dharmawangsa.ac.id/index.php/syntax/author/submission/8782>
Username: bila01_2004

If you have any questions, please contact me. Thank you for considering this journal as a venue for your work.

Ibnu Rusydi
Syntax : Journal of Software Engineering, Computer Science and Information Technology

Terima Kasih

Syntax:
Journal of Software Engineering, Computer Science and Information Technology
<http://jurnal.dharmawangsa.ac.id/index.php/syntax>

Lampiran 4. Lembar Bimbingan Min 8X



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi A dan Swadana Reputasi Badan Akreditasi Nasional Perguruan Tinggi No. 58/SK/BSN-PT/AkredPT/000019

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

Website: www.umsu.ac.id Email: info@umsu.ac.id Instagram: @umsuamedan Facebook: umsumedan Twitter: umsumedan YouTube: umsumedan

Berita Acara Pembimbingan Proposal

Nama Mahasiswa	: Adibah Salsabilah	Program Studi	: Sistem Informasi
NPM	: 2209010064	Judul Penelitian	: Analisis Forensik Digital Untuk Verifikasi Keaslian Bukti Transaksi Pembayaran QRIS Menggunakan Algoritma Hash SHA-256 Sebagai Upaya Deteksi Manipulasi Dokumen Digital

Nama Dosen Pembimbing : Mahardika Abdi Prawira
Tanjung, S.Kom., M.Kom

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
Senin / 12 Januari 2026	- Pernyataan tidak disitasi - Penjelasan Flowchart terlalu sedikit	
Rabu / 14 Januari 2026	- Jarak spasi daftar isi yang terlalu dekat - Gambar yang terlalu kecil / dibesarkan	
Jum'at / 23 Januari 2026	- Teknik Pengumpulan Data dibuat pakai Diagram - Tahapan Penelitian belum ada	
Sabtu / 17 Januari 2026	- Rancangan UI/UX belum dibuat	
Rabu / 21 Januari 2026	- Tambahkan Daftar Pustaka minimal 5 publikasi Dosen sendiri	

Jum'at / 23 Januari 2026	- ACC SEMINAR PROPOSAL	ht
Jum'at / 10 April 2026	- Halaman nya diperbaiki	ht
Senin / 13 April 2026	- ACC SIDANG	ht

Diketahui oleh :
Ketua Program Studi



(Mahardika Abdi Prawira
Tanjung, S.Kom., M.Kom)

Medan, 14 April 2026

Disetujui oleh :
Dosen Pembimbing



(Mahardika Abdi Prawira
Tanjung, S.Kom., M.Kom)

