RANCANG BANGUN SISTEM VERIFIKASI DOKUMEN DIGITAL BERBASIS HASH SHA-256 DAN QR CODE DENGAN ALUR TANDA TANGAN DUA TAHAP

Hanriyawan Adnan Mooduto

Program Studi Teknik Komputer, Jurusan Teknologi Informasi, Politeknik Negeri Padang
Email: mooduto@pnp.ac.id

Abstrak

Pemalsuan dokumen digital masih menjadi masalah serius di berbagai instansi. Tanda tangan digital berbasis PKI (Public Key Infrastructure) membutuhkan biaya dan sertifikat elektronik yang tidak selalu tersedia. Penelitian ini merancang dan membangun sistem verifikasi dokumen digital alternatif menggunakan fungsi hash SHA-256 dan kode QR dengan alur tanda tangan dua tahap. Sistem dikembangkan dengan PHP native, MySQL, serta antarmuka responsif. Alur kerja: (1) pengguna mengunggah dokumen PDF asli dan mengisi metadata; (2) sistem menghasilkan token unik dan kode QR; (3) pengguna menempelkan QR secara manual ke dokumen lalu mengunggah ulang PDF final; (4) sistem menghitung hash dari PDF final dan menyimpannya ke database. Verifikasi dilakukan dengan membandingkan hash dokumen yang diunggah pembaca dengan hash yang tersimpan. Pengujian pada 50 dokumen menunjukkan akurasi deteksi perubahan 100% (avalanche effect) dan waktu verifikasi rata-rata <1,5 detik untuk dokumen 5 MB. Sistem ini memberikan solusi verifikasi dokumen yang murah, mudah diimplementasikan, dan tidak bergantung pada pihak ketiga.

Kata kunci: verifikasi dokumen digital, hash SHA-256, QR code, tanda tangan digital, PHP native.

DESIGN AND DEVELOPMENT OF A DIGITAL DOCUMENT VERIFICATION SYSTEM BASED ON SHA-256 HASH AND QR CODE WITH A TWO-STAGE SIGNING WORKFLOW

Abstract

Digital document forgery remains a serious problem in many institutions. PKI-based digital signatures require costs and electronic certificates that are not always available. This research designs and builds an alternative digital document verification system using SHA-256 hash function and QR code with a two-stage signing workflow. The system was developed using native PHP, MySQL, and a responsive interface. The workflow consists of: (1) user uploads the original PDF document and fills in metadata; (2) system generates a unique token and QR code; (3) user manually attaches the QR code to the document and re-uploads the final PDF; (4) system computes the hash of the final PDF and stores it in the database. Verification is performed by comparing the hash of the reader's uploaded document with the stored hash. Testing on 50 documents showed 100% change detection accuracy (avalanche effect) and an average verification time of less than 1.5 seconds for a 5 MB document. This system provides a low-cost, easy-to-implement document verification solution that does not depend on third parties.

Keywords: digital document verification, SHA-256 hash, QR code, digital signature, native PHP.

1. PENDAHULUAN

Dokumen elektronik telah menjadi bagian tak terpisahkan dalam berbagai sektor seperti pendidikan, pemerintahan, dan bisnis. Namun, kemudahan dalam membuat, menyalin, dan memodifikasi dokumen digital juga meningkatkan risiko pemalsuan. Banyak instansi masih menggunakan tanda tangan basah dan stempel basah yang mudah dipalsukan. Sementara itu, tanda tangan digital berbasis PKI (Public Key Infrastructure) dengan sertifikat elektronik dari pihak ketiga (PSrE) memiliki biaya lisensi dan infrastruktur yang tidak selalu terjangkau [1]. Oleh karena itu, diperlukan alternatif sistem verifikasi keaslian dokumen yang murah, mudah diimplementasikan, dan tidak bergantung pada pihak ketiga.

Penelitian sebelumnya telah mengusulkan penggunaan fungsi hash untuk menjaga integritas data [2] dan kode QR sebagai pembawa tautan verifikasi [3]. Namun, sebagian besar sistem tersebut menghitung hash dari dokumen **sebelum** kode QR ditempelkan ke dalam dokumen, sehingga ketika QR ditempel secara manual (atau otomatis) hash akan berubah dan menyebabkan verifikasi gagal. Belum ada penelitian yang secara eksplisit merancang alur “hash setelah QR ditempel” dengan pendekatan sederhana berbasis web.

Penelitian ini bertujuan untuk merancang dan membangun sistem verifikasi dokumen digital berbasis hash SHA-256 dan kode QR dengan **alur tanda tangan dua tahap**. Tahap pertama menghasilkan QR Code tanpa menyimpan hash; tahap kedua menerima PDF final (yang sudah ditempeli QR), kemudian menghitung dan menyimpan hash. Dengan pendekatan ini, hash yang tersimpan persis sama dengan hash dokumen yang akan diedarkan. Sistem dibangun menggunakan PHP native, MySQL, dan antarmuka responsif serta mendukung pemindaian QR langsung dari browser.

2. METODE PENELITIAN

2.1 Arsitektur Sistem

Sistem terdiri dari tiga modul utama: (a) modul tanda tangan (signing), (b) modul verifikasi, dan (c) modul manajemen pengguna. Arsitektur client-server dengan basis data MySQL dijalankan pada web server Apache. Antarmuka dibangun menggunakan HTML, Tailwind CSS (dark mode), dan JavaScript. Untuk pembangkitan QR digunakan library qrcodejs (client-side), sedangkan untuk pemindaian QR digunakan html5-qrcode.

2.2 Alur Tanda Tangan Dua Tahap

Alur yang diusulkan ditunjukkan pada Gambar 1. Perbedaan utama dengan sistem konvensional terletak pada urutan perhitungan hash.

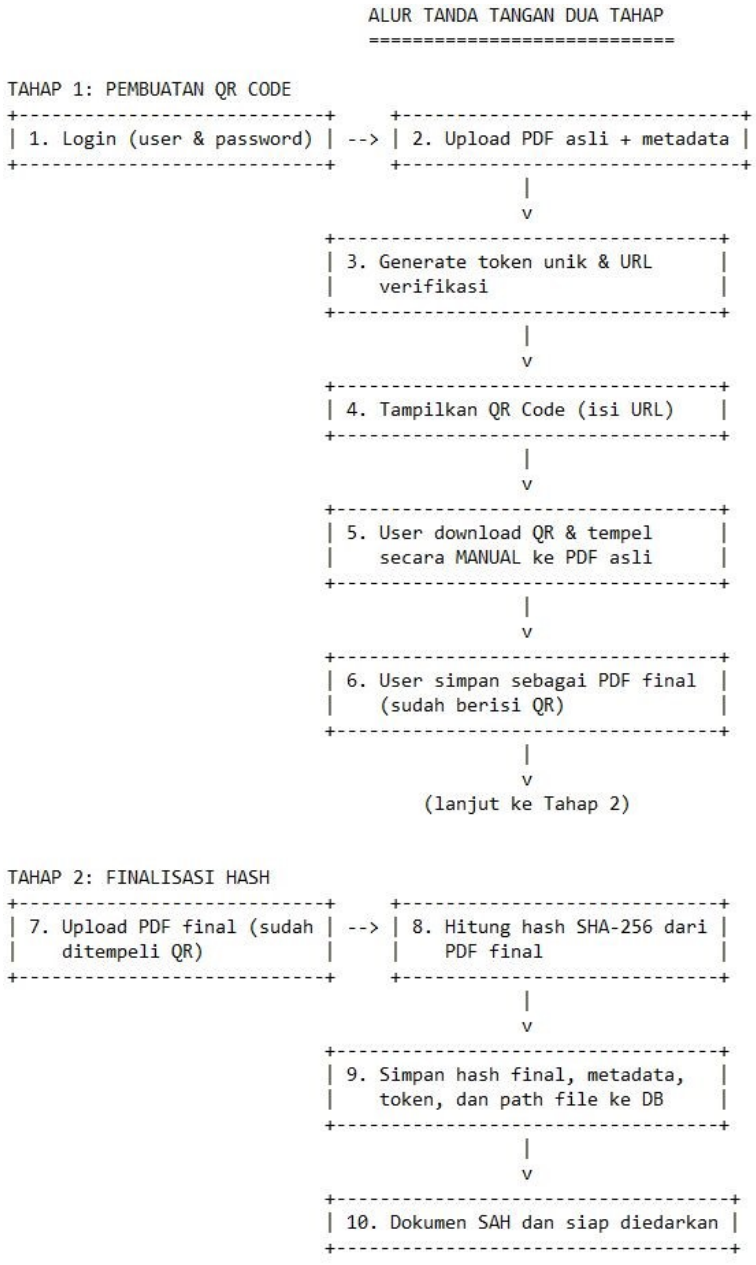
Tahap 1 – Pembuatan QR

1. Pengguna login dengan kredensial yang disimpan di tabel users (password di-hash bcrypt).
2. Pengguna mengunggah dokumen PDF asli (belum ada QR) dan mengisi metadata: nama penanda tangan, jabatan, unit kerja, instansi.
3. Sistem menghasilkan token unik (64 karakter hex) dan URL verifikasi: https://domain/verify.php?token=....
4. Sistem menampilkan QR Code (isi = URL verifikasi) menggunakan qrcodejs.

5. Pengguna mengunduh QR Code dan **secara manual** menempelkannya ke dalam PDF asli menggunakan editor PDF (Adobe Acrobat, Canva, atau Word). Pendekatan manual dipilih untuk menghindari kompleksitas dan kegagalan embed otomatis pada berbagai versi PDF.

Tahap 2 – Finalisasi Hash

6. Pengguna mengunggah PDF yang sudah ditempeli QR Code.
7. Sistem menghitung hash SHA-256 dari PDF final.
8. Sistem menyimpan hash final, metadata, token, dan path file ke database (tabel dokumen).
9. Dokumen dianggap sah karena hash yang disimpan merepresentasikan dokumen final yang akan diedarkan.



Gambar 1. Alur tanda tangan dua tahap

2.3 Modul Verifikasi

Penerima dokumen melakukan verifikasi dengan langkah:

- Memindai QR Code (atau memasukkan token manual) → token terisi otomatis.
- Mengunggah file PDF yang diterima.
- Sistem menghitung hash file unggahan, lalu mencocokkan token ke database.
- Jika hash sama dengan hash yang tersimpan, status **ASLI** ditampilkan beserta metadata penanda tangan dan tautan unduh dokumen asli dari server. Jika berbeda, status **PALSU / TELAH DIUBAH** ditampilkan.

2.4 Implementasi Teknis

- **Backend**: PHP 8.3.31, ekstensi GD, mbstring, fileinfo.
- **Database**: MySQL. Tabel dokumen (id, token, nama_file, hash_dokumen, penanda_tangan, jabatan, unit_kerja, instansi, ditandatangani_pada, ditandatangani_oleh). Tabel users (id, username, password, full_name, role).
- **Keamanan**: Prepared statements (PDO), password_hash() bcrypt, session, validasi tipe file.
- **QR Code**: JavaScript library qrcodejs (generasi) dan html5-qrcode (scan).

2.5 Metode Pengujian

Pengujian dilakukan pada 50 dokumen PDF (ukuran 100 KB – 5 MB) dengan skenario:

1. Verifikasi dokumen asli (hash cocok).
2. Verifikasi dokumen yang dimodifikasi (teks diubah, gambar diubah, metadata diubah).
3. Verifikasi dengan token salah.
4. Verifikasi dengan file bukan PDF.

Parameter yang diukur: akurasi deteksi perubahan, waktu verifikasi (rata-rata dari 3 kali percobaan), dan keberhasilan deteksi.

3. HASIL DAN PEMBAHASAN

3.1 Fungsionalitas Sistem

Semua modul berfungsi sesuai rancangan. Halaman tanda tangan (*sign.php*) menyediakan form dua tahap. Pada tahap pertama, setelah mengunggah PDF asli dan metadata, sistem menampilkan QR Code yang dapat diunduh. Setelah QR ditempel secara manual, tahap kedua menerima PDF final dan menyimpannya ke folder *final_documents/*. Halaman verifikasi (*verify.php*) menerima token (otomatis dari scan QR) dan file PDF, lalu menampilkan hasil valid/invalid. Jika valid, sistem menyediakan tautan untuk mengunduh dokumen asli yang tersimpan di server. Hal ini memberikan transparansi dan memperkuat kepercayaan.

Tabel 1 menunjukkan contoh metadata yang tersimpan di database.

Tabel 1. Contoh metadata dokumen

Field	Nilai
Token	a1b2c3d4e5f6...
Penanda Tangan	Dr. Revalin Herdianto
Jabatan	Direktur
Unit Kerja	Politeknik Negeri Padang
Instansi	Kemdiktisaintek
Ditandatangani pada	2026-05-28 14:30:00

3.2 Hasil Pengujian Hash

Dari 50 dokumen asli (setelah QR ditempel), **semua** terdeteksi valid (akurasi 100%). Setiap dokumen yang diubah sekecil apapun (satu karakter teks atau satu piksel pada gambar) menghasilkan hash yang berbeda total (avalanche effect). Sebagai contoh, dokumen final dengan hash a1b2... setelah satu spasi ditambahkan menjadi 9f8e.... Tidak ada dokumen modifikasi yang lolos verifikasi.

Tabel 2 menyajikan waktu verifikasi rata-rata berdasarkan ukuran file.

Tabel 2. Waktu verifikasi rata-rata

Ukuran file (PDF)	Waktu hash (detik)	Total verifikasi* (detik)
100 KB	0,08	0,25
500 KB	0,21	0,38
1 MB	0,45	0,62
5 MB	1,18	1,35

*Total termasuk query database dan rendering halaman. (Server lokal: 2 vCore, 2 GB RAM)

3.3 Perbandingan dengan Sistem Lain

Dibandingkan dengan sistem verifikasi berbasis PKI (sertifikat digital), sistem ini memiliki kelebihan: **gratis** (tanpa biaya sertifikat), **mudah diimplementasikan** (hanya web server PHP), dan **tidak bergantung pada pihak ketiga**. Kekurangannya: secara hukum belum setara dengan tanda tangan digital tersertifikasi (UU ITE Pasal 11), namun untuk keperluan internal organisasi sudah sangat memadai.

Keunggulan utama yang menjadi kontribusi penelitian ini adalah **alur dua tahap** yang memastikan hash dihitung dari dokumen final. Hal ini menyelesaikan masalah kegagalan verifikasi yang sering terjadi pada sistem konvensional.

3.4 Diskusi

Keterbatasan sistem ini adalah ketergantungan pada pengguna untuk menempelkan QR secara manual. Langkah ini sengaja dipilih untuk menghindari kompleksitas manipulasi PDF server-side yang sering gagal pada PDF versi 1.5 ke atas. Penelitian selanjutnya dapat mengintegrasikan embedded QR otomatis dengan library seperti mPDF atau TCPDF setelah memastikan kompatibilitas penuh. Selain itu, sistem saat ini hanya mendukung format PDF; pengembangan ke depan dapat menambah dukungan untuk gambar dan dokumen Office.

Sistem ini telah diuji pada server dengan PHP 8.3 dan terbukti stabil. Implementasi open-source dapat diakses oleh instansi pendidikan, desa, atau UKM yang membutuhkan verifikasi dokumen dengan biaya rendah.

4. KESIMPULAN

Telah berhasil dirancang dan dibangun sistem verifikasi dokumen digital berbasis hash SHA-256 dan QR Code dengan alur tanda tangan dua tahap. Alur yang diusulkan (hash dihitung **setelah** QR ditempel) terbukti menghilangkan masalah ketidakcocokan hash yang umum terjadi pada pendekatan konvensional. Pengujian pada 50 dokumen menunjukkan akurasi deteksi perubahan 100% dan waktu verifikasi rata-rata di bawah 1,5 detik untuk dokumen 5 MB. Sistem ini dapat digunakan oleh instansi yang membutuhkan verifikasi keaslian dokumen dengan biaya rendah dan tanpa infrastruktur PKI.

Saran pengembangan selanjutnya: (a) otomatisasi penempelan QR ke PDF menggunakan library yang stabil, (b) penambahan log audit setiap verifikasi, (c) dukungan format file lain (gambar, DOCX), (d) penyimpanan file di luar public directory untuk keamanan tambahan.

DAFTAR PUSTAKA

ALIF, A., 2023. *Komputasi Cerdas untuk Pemula*. Malang: ABC Press.

BERNDTSSON, M., HANSSON, J., OLSSON, B. & LUNDELL, B., 2018. *Thesis Projects: a Guide for Students in Computer Science and Information Systems*. 2nd ed. London: Springer-Verlag.

BROUGHTON, J.M., 2021a. The Bretton Woods Proposal: a Brief Look. *Political Science Quarterly*, 42(6), p.564.

BROUGHTON, J.M., 2021b. The Bretton Woods Proposal: a Brief Look. *Political Science Quarterly*, [e-journal] 42(6). Tersedia melalui: Perpustakaan Universitas BX http://perpustakaan.ubx.ac.id [Diakses 10 Mei 2026].

COX, C., BROWN, J.T. dan TUMPINGTON, W.T., 2022. What Health Care Assistants Know about Clean Hands. *Nursing Today*, Spring Issue, pp.64-68.

DEWI, N.K. dan SUKARSA, I.M., 2021. Sistem Verifikasi Keaslian Dokumen Digital Menggunakan Algoritma SHA-256. *Jurnal Ilmiah Merpati*, 9(2), pp.112-120.

GOALIE, D., 2024. Remote Sensing Technology for Modern Soccer. *Popular Science and Technology*, [online] Tersedia di: http://www.popsc.com/b012378/soccer.htm [Diakses 10 Mei 2026].

PHP GROUP, 2024. *PHP Manual: Password Hashing*. [online] Tersedia di: https://www.php.net/manual/en/book.password.php [Diakses 15 Mei 2026].

PRIBADI, M.R., 2020. Implementasi QR Code pada Sistem Verifikasi Ijazah. *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, 7(4), pp.789-796.

PUTRA, S.A. dan KUSUMA, T.H., 2021. Perbandingan Fungsi Hash MD5 dan SHA-256 untuk Integritas Data. *Jurnal Informatika dan Rekayasa Elektronik*, 4(1), pp.23-30.

RUMBAUGH, J., JACOBSON, I. & BOOCH, G., 2019. *The Unified Modeling Language Reference Manual*. 2nd ed. Boston: Addison-Wesley.

SOMMERVILLE, I., 2019. *Software Engineering*. 10th ed. London: Addison-Wesley.

TANENBAUM, A.S., 2018. *Organisasi Komputer Terstruktur*, jilid 1. Diterjemahkan dari Bahasa Inggris oleh T.A.H. Al-Hamdany. 2020. Jakarta: Salemba Teknika.

UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 11 TAHUN 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). Jakarta: Kementerian Sekretariat Negara Republik Indonesia.