

**University of Mosul
College of Education
For Pure Sciences**



A Blockchain based System for Detecting Digital Content Manipulation Using Integrity Verification Approach

Omar Ahmad Hussein Ali Alobaidy

M.Sc. Thesis

Computer science

Supervised by

Assist. Prof.

Dr. Raya Basil Ahmad Hasan Alothman

2026 A.D.

1448A.H.

ABSTRACT

Digital content is often copied and edited, which affects trust in academic, governmental, and healthcare records. Blockchain-based ledgers offer tamper-evident registration; cryptographic hashing provides proof of bit-level integrity; and intrusion-detection mechanisms secure the verification platform. However, integrity verification, tamper analysis, and access security tend to be discussed separately rather than as being part of a total solution. In this thesis, a complete software system is designed, implemented, and evaluated using immutable blockchain-based file hash and metadata registration using linked blocks with proof-of-work, Merkle aggregation and chain validation; multi-hash, format-agnostic tamper detection of heterogeneous file types via SHA-256, SHA-3, and BLAKE2; and intrusion-oriented access security through composite risk score (0–100) obtained from failed login attempts, user-agent heuristics, and the IP/geolocation context; and mandatory face-assisted verification and intruder snapshot logging. The proposed system combines blockchain integrity validation, tamper detection, and intrusion-oriented security with a consolidated operational framework. The experimental evaluation consisted of 4,574 files and 200 simulated intrusion scenarios. Results showed 100% tamper-detection accuracy across 4,574 files, a 98.5% intrusion-detection rate with a 2.3% false-positive rate across 200 simulated scenarios, 100% blockchain chain validation and signature verification across all 4,574 blocks, and acceptable runtime characteristics (~145 ms hashing and ~165 ms verification for a 1 MB file). The approach delivered by this work provides a complete system-wide prototype and yields quantitative indicators of data integrity, platform security, and system performance appropriate for institution-oriented deployment

المستخلص

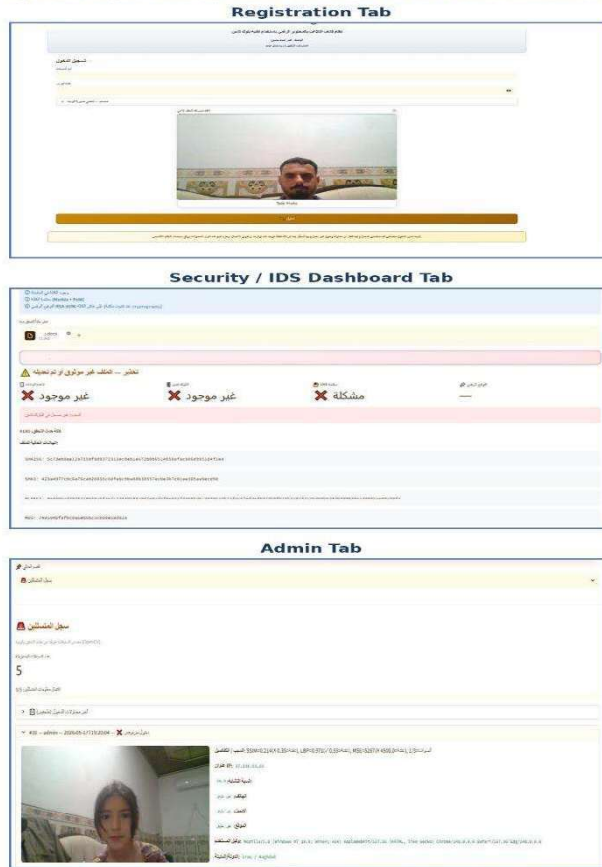
غالبًا ما يتم نسخ المحتوى الرقمي وتعديله، مما يؤثر في الثقة بالسجلات الأكاديمية والحكومية والرعاية الصحية. توفر دفاتر الأستاذ القائمة على تقنية البلوك تشين تسجيلًا يكشف العبث، بينما توفر دوال التجزئة التشفيرية دليلًا على سلامة البيانات على مستوى البت، كما تؤمن آليات كشف التسلل منصة التحقق. ومع ذلك، غالبًا ما تتم مناقشة التحقق من السلامة، وتحليل العبث، وأمن الوصول بصورة منفصلة بدلاً من دمجها ضمن حل متكامل. في هذه الرسالة، تم تصميم وتنفيذ وتقييم نظام برمجي متكامل يعتمد على التسجيل غير القابل للتغيير لبصمات الملفات (Hash) والبيانات الوصفية باستخدام البلوك تشين من خلال كتل مترابطة تعتمد على إثبات العمل (Proof-of-Work)، وتجميع ميركل (Merkle Aggregation)، والتحقق من صحة السلسلة (Chain Validation)، إضافةً إلى كشف العبث متعدد التجزئة والمحايد لنوع الملف لمختلف أنواع الملفات باستخدام خوارزميات SHA-256 و SHA-3 و BLAKE2، فضلاً عن تأمين الوصول الموجّه لاكتشاف التسلل من خلال درجة مخاطر مركبة (0-100) تُحتسب بالاعتماد على محاولات تسجيل الدخول الفاشلة، وخصائص وكيل المستخدم (User-Agent Heuristics)، وسياق عنوان بروتوكول الإنترنت/الموقع الجغرافي (IP/Geolocation)، بالإضافة إلى التحقق الإلزامي بمساعدة التعرف على الوجه وتسجيل صور المتسللين. يجمع النظام المقترح بين التحقق من سلامة البلوك تشين، وكشف العبث، والأمن الموجّه لاكتشاف التسلل ضمن إطار تشغيلي موحد. شمل التقييم التجريبي 4,574 ملفًا و 200 سيناريو محاكاة للتسلل. وأظهرت النتائج تحقيق دقة بلغت 100% في كشف العبث عبر 4,574 ملفًا، ومعدل كشف للتسلل بلغ 98.5% مع معدل إيجابيات كاذبة بلغ 2.3% عبر 200 سيناريو محاكاة، ونجاحًا بنسبة 100% في التحقق من صحة سلسلة البلوك تشين والتحقق من التواقيع الرقمية عبر جميع الكتل البالغ عددها 4,574 كتلة، إلى جانب خصائص أداء مقبولة من حيث زمن التنفيذ (حوالي 145 مللي ثانية لتوليد التجزئة، وحوالي 165 مللي ثانية للتحقق لملف بحجم 1 ميغابايت). يقدم هذا العمل نموذجًا أوليًا متكاملًا على مستوى النظام، ويوفر مؤشرات كمية لسلامة البيانات، وأمن المنصة، وأداء النظام، بما يجعله مناسبًا للتطبيق في المؤسسات.

HIGHLIGHTS

- Complete blockchain-based system unifying integrity verification, tamper detection, and intrusion-oriented access security in one framework.
- Immutable file hash and metadata registration via linked blocks with proof-of-work, Merkle aggregation, and chain validation.
- Format-agnostic, multi-hash tamper detection (SHA-256, SHA-3, BLAKE2) across heterogeneous file types.
- Intrusion-oriented access security via composite risk score (0-100), mandatory face-assisted verification, and intruder snapshot logging.
- Evaluated on 4,574 files and 200 simulated intrusion scenarios: 100% tamper-detection accuracy, 98.5% intrusion-detection rate (2.3% false-positive rate).
- 100% blockchain chain validation across 4,574 blocks; real-time performance (~145 ms hashing, ~165 ms verification for a 1 MB file).

GRAPHICAL ABSTRACT

System Operational Walkthrough (Streamlit Interface)



Keywords:

ABSTRACT

Blockchain
Tamper Detection
Multi-Hash
Cryptography
Intrusion Detection
Face Verification
Digital Content Integrity
Format-Agnostic
Risk Scoring
Chain Validation

Digital content is often copied and edited, which affects trust in academic, governmental, and healthcare records. Blockchain-based ledgers offer tamper-evident registration; cryptographic hashing provides proof of bit-level integrity; and intrusion-detection mechanisms secure the verification platform. However, integrity verification, tamper analysis, and access security tend to be discussed separately rather than as being part of a total solution. In this thesis, a complete software system is designed, implemented, and evaluated using immutable blockchain-based file hash and metadata registration using linked blocks with proof-of-work, Merkle aggregation and chain validation; multi-hash, format-agnostic tamper detection of heterogeneous file types via SHA-256, SHA-3, and BLAKE2; and intrusion-oriented access security through composite risk score (0-100) obtained from failed login attempts, user-agent heuristics, and the IP/geolocation context; and mandatory face-assisted verification and intruder snapshot logging. The proposed system combines blockchain integrity validation, tamper detection, and intrusion-oriented security with a consolidated operational framework. The experimental evaluation consisted of 4,574 files and 200 simulated intrusion scenarios. Results showed 100% tamper-detection accuracy across 4,574 files, a 98.5% intrusion-detection rate with a 2.3% false-positive rate across 200 simulated scenarios, 100% blockchain chain validation across all 4,574 blocks, and acceptable runtime characteristics (~145 ms hashing and ~165 ms verification for a 1 MB file). The approach delivered by this work provides a complete system-wide prototype and yields quantitative indicators of data integrity, platform security, and system performance appropriate for institution-oriented deployment.

O07508690a@gmail.com

(سورة المجادلة: الآية: 11)



جامعة الموصل

كلية التربية للعلوم الصرفة

نظام قائم على تقنية البلوك تشين لكشف التلاعب بالمحتوى الرقمي باستخدام نهج سلامة التحقق

عمر احمد حسين علي العبيدي

رسالة ماجستير

علوم الحاسوب

بإشراف

الأستاذ المساعد

الدكتورة ريا باسل احمد حسن العثمان