Blockchain Based Digital Evidence Verification System

Anwar Faris Khaleel and Khalid Kadhim Jabbar
[1]*Department of Computer Science, College of Education, Al-Mustansiriya University, 10011 Baghdad, Iraq*
anwarfariskhaleel@uomustansiriyah.edu.iq, khalidk.jabbar@uomustansiriyah.edu.iq

Keywords: Blockchain, Digital Evidence, Image Authentication, Tamper Detection, Image Forensics, Block Hashing, Level Analysis.

Abstract: This framework focuses on verifying the ownership of digital evidence and authenticity with the help of localized tamper detection on a blockchain platform. Even though authentication has been tried before, there are concerns over the inability to make the data immutable and as to where exactly the modification is taking place. The algorithm divides the original image into 8x8 pixel blocks, which are non-overlapping, followed by cryptographic hash generation of the content of the block separately. The created partial hashes are then stored on an underlying layer of a decentralized blockchain to ensure immutability. The system allows comparison in two modes to achieve reliability, which includes block-level comparison of the recovered hashes and comparison upon reconstructing the original image. Also, at the stage of the interactive analysis of the workflow, sophisticated forensic tools are employed, such as Error Level Analysis and the Copy-and-Move algorithm, in order to identify the type and character of manipulations at the identified locations. Empirical evidence demonstrates that the technique offers an indelible computerized fingerprint of each portion of the photograph and deters an area that was altered; therefore, it enhances the dependability in a legal setting involving computerized evidence.

1 INTRODUCTION

The digital age that we are living in is marked with unmatched reliance on digitalized evidence, in particular, images, in the legal and criminal investigations as well as in financial and business documents [1], [2]. Due to its intangible and easily transferable nature, digital evidence has now emerged as an important element in the investigation process [2], [3]. Nevertheless, the same ease poses the basic issue: how is it possible to ensure the security of such evidence and its chain of custody since it is gathered up until it is introduced into the court [4].

The basic issue is that the conventional systems to record evidence, be it manual or centralized are susceptible to a myriad of risks including loss, theft, manipulation, or even distortion of data within the system by access by unauthorized individuals [3], [5] in the case of images, it becomes an uphill task to address localized tampering i.e. adding or deleting a small portion of the image to it. Even a single pixel of an image is manipulated and the full-image hashing methods will not work and so the entire body of evidence is discarded [2].

In that regard, the blockchain technology has become a new promising resource of providing security and integrity of digital evidence. Blockchain can ensure data integrity of any kind permanently with its built-in features of decentralization, immutability, and traceability [4]. To ensure the security of digital evidence in the context of many different areas [1], [2].

To address the drawbacks of the existing methods in detecting localized tampering, this study presents a system of combined image authentication and tamper detection [4].

The proposed system will have combined authentication power of blockchain and accuracy of forensic analysis with:

1) Micro-hashing involves partitioning the image into small blocks (8×8 pixels) and producing an individual cryptographic hash for each block, ensuring that the fingerprint of every image segment remains immutable.
2) Decentralized authentication: Storing these partial hashes on the blockchain layer.
3) Integrated analysis: Using advanced forensic analysis tools such as (ELA) and (Copy-Move) for determine the type and category of

tampering at certain spots flagged by discrepancies in partial hashes.

The primary goal of this research is to give the complete answer that not only proves the overall truth of an image but also finds the exact area of tampering and confirms its kind, thus increasing the trustworthiness and acceptance of digital proof in legal and investigative settings.

2 CONCEPTUAL BACKGROUND

This part talks about the theory behind photographic authentication and the way the technology of blockchain fits into it. This is the first part of the comparison that comes next.

2.1 Image Authentication

Digital image authentication makes sure that an image remains the same as it was when it was captured or made and that no one has changed it or messed with it with no permission [6]. This approach is very helpful in many fields, such as forensic computing, where photos are used as proof in court; reporting and the media, where it battles fake news; and protecting the creative works of artists and imaging professionals [7]. The processing of digital photographs is getting better swiftly, which makes it easier to produce fake pictures. This makes them less useful and less reliable as proof [8]. There are two main ways to tell if a picture is real: passive authentication and active authentication. Active authentication uses things that are already there, like watermarks or digital signatures, to check the picture [9]. But passive authentication does not demand any information ahead of time. Instead, it looks for signs of tampering or forgery in the image itself, like noise analysis or fingerprints left by the camera hardware [10]. But both methods have big problems with their traditional methods. For example, advanced tools can remove watermarks, and some active authentication methods require strict rules about what changes can be made to the image. Passive methods may not always work to tell if an image is real. Show as Figure 1.

2.2 Blockchain Technology

Blockchain is a decentralized distributed ledger technology (DLT) that was first made to support the digital currency Bitcoin [11]. This technology keeps track of transactions in "blocks" that are linked together in a way that is both sequential and encrypted, making a "chain" that can't be changed. Transparency is one of the most important things about blockchain. Everyone on the network can see a copy of the ledger and check transactions [12]. Smart contracts are important for a lot of blockchain systems, especially Ethereum. When certain conditions are met, smart contracts automatically carry out the terms that both parties agreed to [13]. These programs are stored and run on the blockchain. Blockchain is useful for a lot of things, not just cryptocurrencies. It can also do tasks automatically in a clear and safe way [14]. For example, it can be used to check digital pictures.

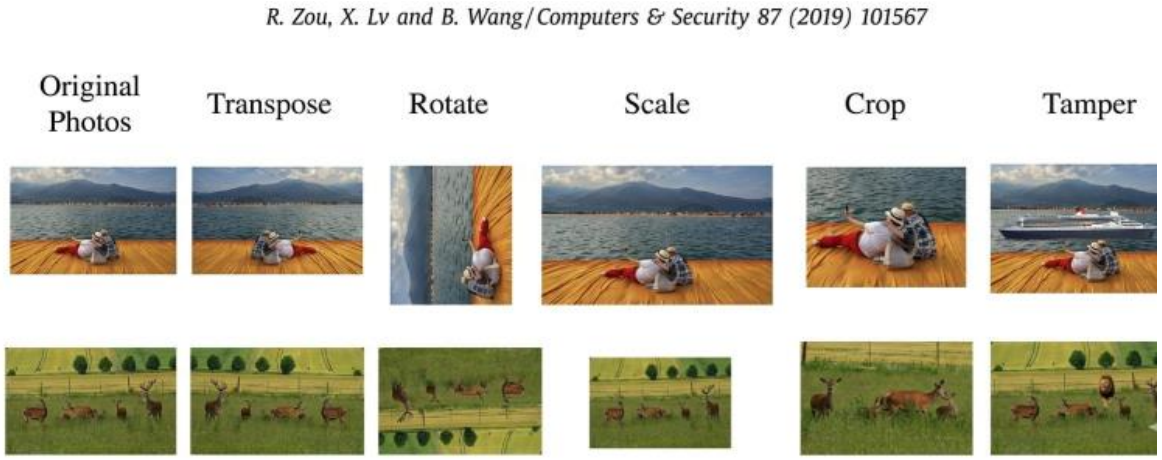

Figure 1: Some transformed tested in paper.

3 A COMPARATIVE STUDY OF BLOCKCHAIN-BASED APPROACHES FOR IMAGE AUTHENTICATION

In recent years, blockchain technology has been employed in various approaches to authenticate and secure digital images. These approaches primarily focus on issues such as image authenticity preservation, prevention of image theft, and protection of copyright. The decentralized and permanent nature of blockchain helps achieve these goals. This section groups the main methods according to their basic ideas, describes how they work, and lists their benefits, disadvantages, and current problems. Figure 2 shows an example of a blockchain-based image authentication process. In this framework, Photo 0 represents the original image, while Photos 1, 2, ..., i denote authenticated versions stored and verified through the blockchain. When a user modifies an authenticated image (Photo i) to create a new version (Photo i+1), the updated image is submitted to the system to verify ownership and establish a new authentication record. This process enables the traceability of image modifications and supports copyright protection through immutable blockchain records.

3.1 Perceptual Hashing and Blockchain-Informed Techniques

Perception hashing is used in this method to make a unique fingerprint that shows what the picture looks like. The fingerprint is stored on the blockchain so that it can't be changed and so that picture authentication works. Dingie Xu and Na Ren found a way to keep Industrial Internet of Things (I IoT) settings safe by combining perceptual hashing with blockchain technology. Their method creates strong visual hashes that can detect both small and large changes in images. You can keep track of changes to images more easily with blockchain storage, which makes these numbers safer. These steps work together to keep the picture safe all the time. Salim and Batool Arif demonstrated the application of blockchain technology and cognitive hashing to identify and rectify image distortion. The most advanced cognitive hashing methods help them find even the tiniest changes. The blockchain's job is to keep numbers safe. Tests have shown that the technology can find places that have changed correctly. However, large storage requirements for images or for blockchain storage requirements may hinder salability [11]. The situation is like that in Figure 3. Zhang and Qiu-Yu explored a cognitive hashing-based approach for intellectual property protection using blockchain technology. Their approach aims to detect subversion attacks at the ownership level with low distortion and to protect intellectual property rights. Experimental results show that the method retains ownership protection while allowing controlled modifications to the content [12].

3.2 Provenance and Tamper-Detection Techniques

Much work has been done on using blockchain to record the origin of images while at the same time keeping track of changes made to them. These methods usually put a hash value or some other unique ID of the image onto an unchangeable ledger so that tampering can be seen. Zou et al. showed a system that allows checking, protecting, and tracking the origin of photos; by tying these proofs to the blockchain, the truth of photographic proof is kept.

These proofs help with both finding out who owns it and a full check of all related edits. The suggested plan brings together blockchain tech with regular ways to check images and comes up with a new extraction method that pays miners for checking images. The authors Rout and Mishra proposed the BICAFD method that aims to detect the counterfeit content and authenticate the visual media. The concept is to use the immutable property of blockchain to create an initial record that is not alterable, thus ensuring that an image is not modified from its original input. These methods generally use cryptographic hash functions like SHA-256 to generate a unique fingerprint for each image; any change, however minor, will produce a completely different hash value.

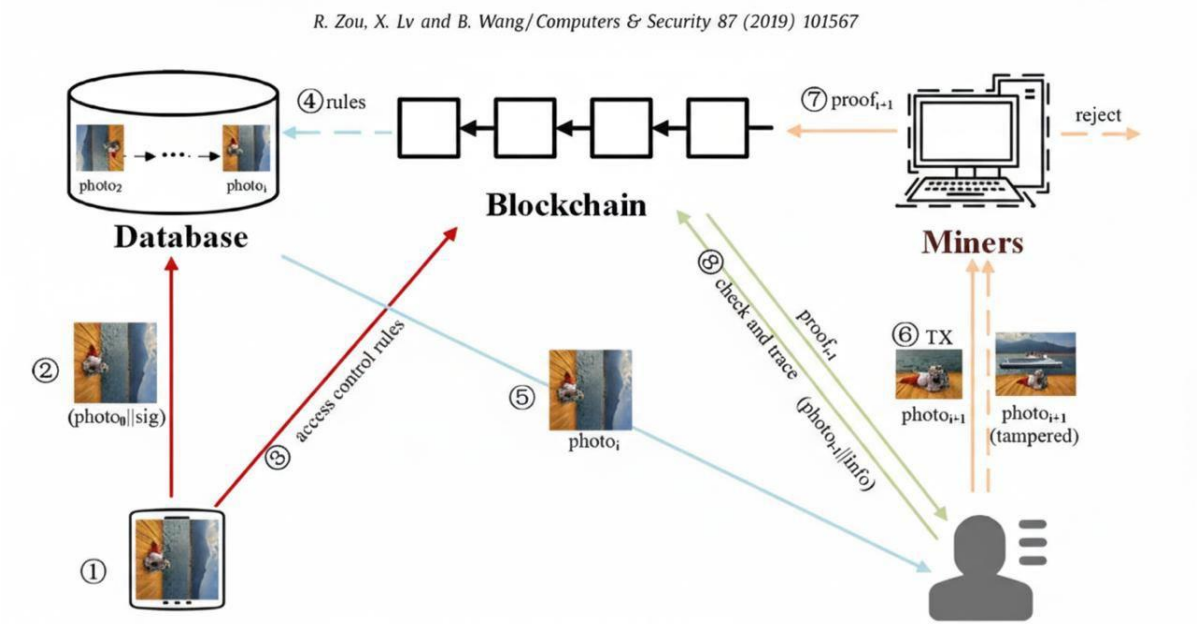

Figure 2: Workflow of the blockchain-based image authentication model.

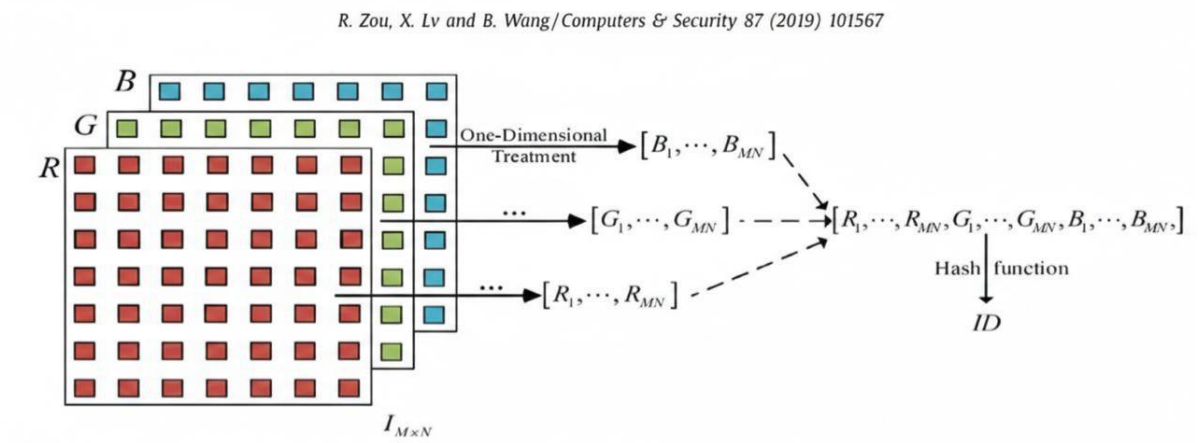

Figure 3: The hash data Global (ID).

3.3 Approaches to Protecting Intellectual Property

In the present climate, safeguarding the intellectual property rights of digital images has become increasingly difficult. Some researchers argue that blockchain technology could provide an answer to this problem. One approach that these methods take to protecting IP involves using blockchain to keep an unchangeable record of ownership and usage rights for each image. In this area, systems are using blockchain to record ownership and allowed uses of pictures. Blockchain is a public, transparent, and tamper-proof ledger. The aim here is to create a blockchain-based system for managing picture IP rights whereby the registration of ownership is both visible and secure. Smart contracts allow photo owners to enter details about ownership and set up rules for access and use.

At the same time, Kalita et al. discussed how blockchain technology could be used for safely storing and sharing copyrighted pictures in order to minimize the risk of infringement while protecting IP rights and enabling safe sharing without servers. In the same way, Chang and Chen suggested a perceptual hashing approach based on blockchain for

intellectual property protection which also helps in identifying modified or counterfeit versions. To bolster the security of authentication watermarks, Abrar et al. incorporated features from blockchain technology to resist watermark alteration or removal. Mohsin, Sajjad Abdulkareem, compared smart contract-based applications designed for image IP protection across various blockchain platforms with respect to monitoring ownership, usage, and licensing through smart contracts. The principal conclusions were the advantages and disadvantages of the platforms, specifically, Ethereum and Hyperledger, in the context of cost, scalability, and efficiency to protect intellectual property. The other urgent problem, which was raised, was the legal and regulatory aspects that came along with the regulation of digital property right across the borders.

3.4 Techniques for Digital Image Forensics

These methods utilize the blockchain to verify the original identity of an image and its later lineage. This allows for finding tampering and tracing the source. Zou et al. offered a blockchain-based image-forensics system for tracking images, protecting copyright, and fighting piracy. Their framework combines blockchain with traditional techniques for image verification and presents a new mining protocol that rewards miners who check image content. The main results show this system can verify images, protect copyrights, and track changes.

Igonor, Oshoke Samson presented a secure digital image-forensics framework that employs blockchain technology. This framework uses blockchain for the storage of image metadata and fingerprints within an unchangeable chain of custody. Results indicated that this framework increases the reliability and integrity of forensic image processes though it may have some limitations with respect to the storage capacity of the blockchain and speed in retrieving records.

Rout et al., Rout and Mishra proposed a system named "BICAFD: Blockchain-based Picture Content Authentication as well as Forgery Detection" which detects and authenticates fraudulent content in images. Empirical results prove its efficacy in counterfeiting detection and content authentication.

Wang and Zhang discussed using blockchain in digital forensics dealing with image modifications. Their study comprises other works that applied blockchain for enhancing forensic tools' accuracy.

The study's primary findings show that blockchain technology could provide the safe yet unchangeable archive of images features to help find any tampering in the images. The limits come from the difficulty of calculation and the high storage needs linked with large amounts of data.

4 RELATED WORK

In recent years, the integrity of (digital evidence) and the (chain of custody) has been a growing concern. On this context, blockchain technology is increasingly being seen as an effective way to create a permanent and unchangeable record. The literature on this topic can be categorized into three main themes: authentication of the (chain of custody), assurance and verification of data integrity, and proof of ownership and traceability.

4.1 Authentication of Digital Evidence: Chain of Custody

The large body of literature uses (blockchain) to overcome the limitations of manual or centralized (chain of custody) records.

Santamaría et al. [15] study the application of smart contracts for managing and verifying the chain of custody of digital evidence, showcasing a practical example of how blockchain can be utilized to create a verifiable and auditable record among all parties involved.

4.2 Data Integrity and Decentralized Auditing

The ability to audit data integrity is a key requirement for decentralized storage.

According to Yuan et. al. [16], the (blockchain) model of self-auditing of decentralized storage is implemented on (PDP/POR) protocols to ensure this integrity of data stored in the cloud. The value of this work lies in the fact that it provides an autonomous mechanism of verifying the integrity of data without the necessity of having a local copy.

Akhtar and Feng [17] also looked at the use of blockchain technologies and hashing algorithms to improve the security of digital forensics in IoT systems. They highlighted that challenges related to security and data integrity still exist, which require smart and efficient solutions based on blockchain.

4.3 Tracking Ownership and History

Another issue that falls under blockchain research is the proof of ownership and the tracing of the

provenance of assets. This has a direct bearing on the question of authenticating original images.

1) Sheldon [18] developed a framework for tracking ownership and provenance for physical objects through blockchain, arguing that the shared, append-only database in a blockchain is very appropriate for tracking provenance.
2) Cu et. al. [19] proposed a model of the Continuous Timestamps Tracking System to increase trust in asset ownership data by making use of the traceability and irreversibility properties of blockchain.
3) Trujillo and Zhang [20] discuss hyper-ownership and non-repudiable digital identity based on the use of the non fungible tokens (NFTs) with smart contracts for verifying and tracing digital ownership.

4.4 Gaps in Proposed Research and Methodology

While these studies cited show dependable chain-of-custody procedures, ensure that the overall data are secure and prove ownership, they often have gaps in addressing visual evidence that can be tampered with locally.

5 PROBLEM DESCRIPTION

The main point is that current methods used to verify digital image evidence have shortcomings in several areas: Guaranteeing data integrity and permanence by recording part of the image hashes on a decentralized blockchain network. Accurately pinpointing where alterations have taken place by using a method that hashes 8x8 pixel blocks and comparing hashes block by block, which can find up to 16 changed blocks within a 64-block frame instead of rejecting the whole image. By incorporating forensic analysis through the combination of ELA and Copy-Move detection algorithm into a single interactive analysis interface, investigators are able to confirm the manner of tampering (e.g. JPEG compression manipulation) at specific positions with regard to hashes. Practical application outcomes indicate that such a system can be an adequate enough solution in the strengthening of the digital evidence (chain of custody) and the presentation of precise and definitive forensic proof in an investigation.

6 THE PROPOSED METHOD

This approach introduces a hybrid approach, which is founded on the properties that cannot be changed with the blockchain technology to guarantee authentication of digital images and the identification of localized manipulation. The system consists of three basic algorithms it uses in both authentication and verification mechanisms and two arduous operations (cryptography and block hashing). The situation is like that in Figure 4.

6.1 General Structure and Procedures for Encryption and Hashing

This method converts an image into data that can be stored and verified on the (blockchain). This is done through several steps, with the first being image segmentation.

1) This source image is divided into equal 8 × 8 pixel subblocks. This allows easy identification of possible forgeries (small changes) made to the image without affecting its large-scale authenticity. Second, hash computation.
2) A one-way hash function such as SHA-256 or an equivalent algorithm shall be applied over the content of each block O' i,j independently to produce a different hash for every segment. Lastly, blockchain anchoring.
3) The resulting partial hashes are kept with a unique block identifier (Block ID) for every subblock inside a node on the blockchain. This ensures that the digital fingerprint of each segment of the image is stored forever and cannot be changed.

6.2 Algorithms for the Proposed System

The process includes an algorithm for registering the original image and two algorithms developed to check authenticity.

6.2.1 Verification of the Original Image

This step aims to ensure that the original image is verified in an unchangeable way on the blockchain.

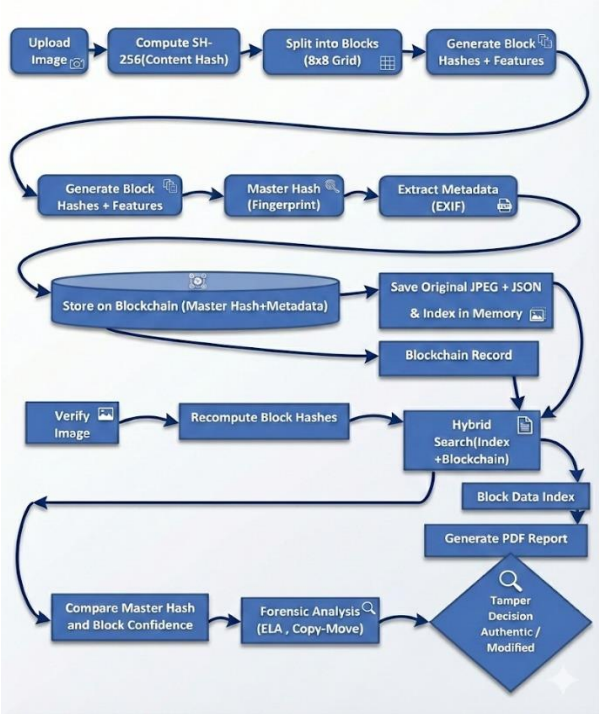

Figure 4: The proposed system.

Algorithm 1: Image registration and blockchain storage algorithm

Input: The original image, the hash function, additional the hash function

Output: The registered image

Begin

1. Get the first picture 0.
2. Break 0 up into 8×8 pieces that don't overlap ($O'_{i,j}$).
3. Use a hash function with extra of hash function on each block for make the encrypt blocks ($O''_{i,j}$).
4. Send of each encrypted block $O''_{i,j}$ to a nodes on the blockchain.
5. Write down the picture that comes out like Or(i,j).
6. The End

6.2.2 Evidence of Reliability (First Approach): Block Wise Comparison

This method focuses on the accuracy of the detection of tampering by directly comparing each block of the received image with the corresponding block stored in the blockchain.

Algorithm 2: Block-wise image authenticity verification algorithm

Input: Register images *Or(i,j)*, receive images *R0*

Output: The authentications proof

Begin

1. Import the picture R0 that you got and the aligned image Or(i,j).
2. Break Ro into pieces that are 8×8 (Ro′(i,j)).
3. Get Or(i,j) from the blockchain nodes and call it Or′(i,j).
4. Use the hash functions to read each block and get Or(i,j).
5. Make sure that each Ro′(i,j) block is linked to the right Or″(i,j) block. If they are the same, write down 1. If they are different, write down 0.
6. Put the binary numbers in the right order.
7. If all the pieces fit together, the proof is thought to be true. The number of zeros shows how big the differences are if not.
8. The End

6.2.3 Verification of Reliability (Second Method): A Full-Image Reconstruction Via Original Image Blocks Compared to the Received Image

This method reconstructs the original full image using documented blocks and compares it with the received image. It is a faster technique but less accurate in local manipulation detection.

6.3 Phases of Interactive Forensic Analysis

After unreliability is established and variable blocks are identified using the (Block by Block) algorithm, the process moves on to the Interactive Tampering Analysis phase. This phase utilizes standard forensic tools in an attempt to validate the specific type of tampering within those regions: (Error Level Analysis) Used for show areas where the level of compression changes (JPEG) compression inconsistency, which can mean that the images has been saved again or new parts added. (Copy-Move Analysis) Used to find if a part of the images has been copied and pasted in the same images. (Block Matching) Kept as an ongoing task for direct comparison between block data and its hash saved on the blockchain.

Algorithm 3: Full-image reconstruction verification algorithm

Input: The registered images *Or(i,j)*, receive images *Ro*

Output: The authentcation proof

Begin

1. Add the aligned image Or(i,j) and the picture Ro that you got.
2. Get Or(i,j) from the blockchain nodes and call it Or′(i,j).
3. To get $Or^3(i,j)$, you have to decrypt each block one at a time.
4. To put the picture back together, use Or"(i,j) to make RI"(i,j).
5. Check to see how well each part of Ro fits with the part of RI that goes with it. Write down 1 if they are the same and 0 if they are not.
6. Write down what has happened.
7. If the similarity rate is 100%, the picture is thought to be reliable. If not, the number of zeros is used to figure out how bad the data is.
8. The End

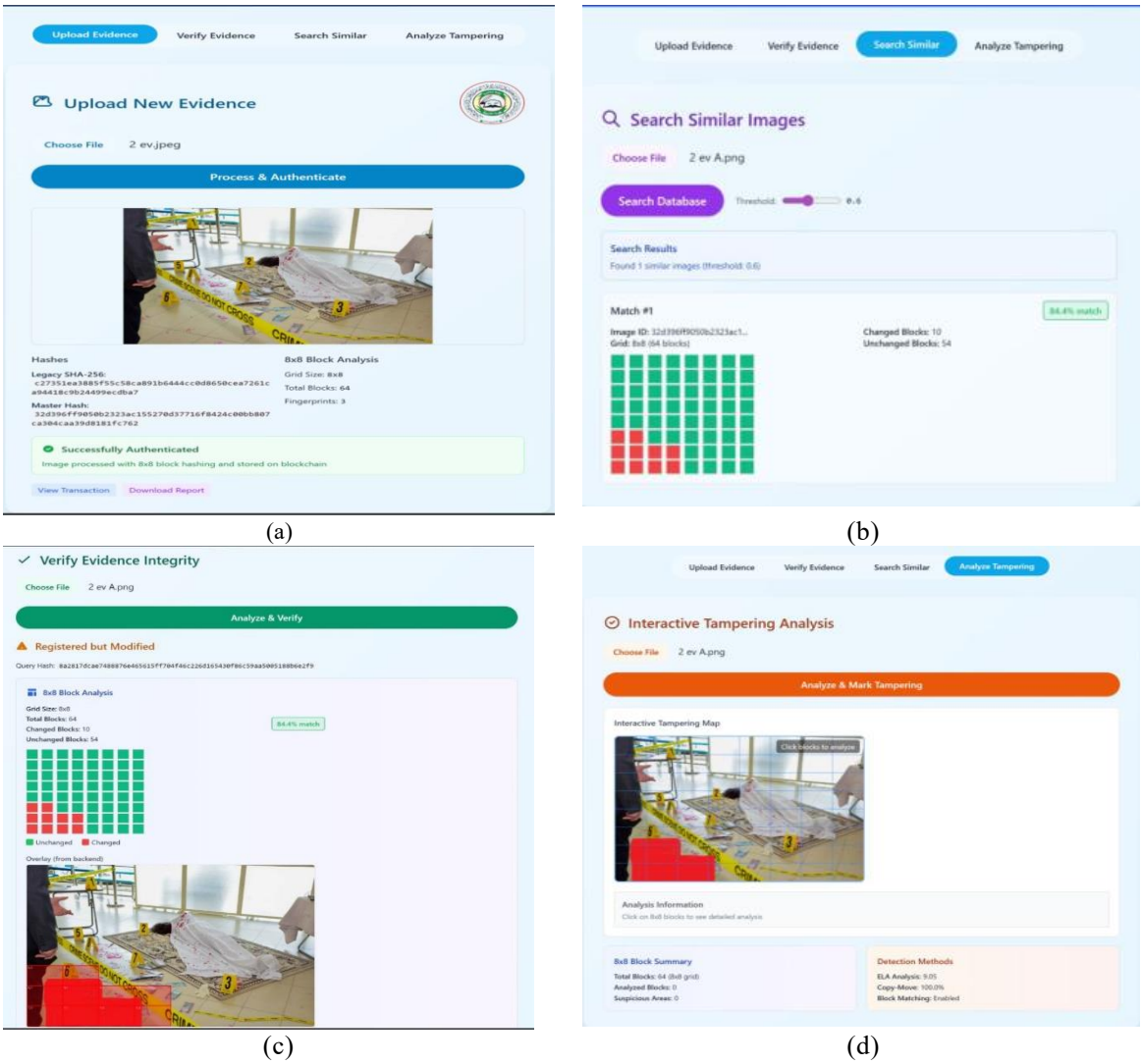

Figure 5: Comprehensive system workflow and multi-phase tampering analysis with blockchain verification results: a) state one (comprehensive system workflow and multi-phase tampering analysis); b) state two (comprehensive system workflow and multi-phase tampering analysis); c) state three (comprehensive system workflow and multi-phase tampering analysis); d) state four (comprehensive system workflow and multi-phase tampering analysis).

Table 1: Results of block hash matching and tampering localization.

Metric	Value	Analytical Implication
Grid Size	8×8	Represents the granularity of the localized analysis.
Total Blocks	64	The total number of sub-units for integrity check.
Unchanged Blocks (Green)	54 Blocks	84.4% of the image content matched the authenticated Blockchain record.
Changed Blocks (Red)	10 Blocks	Precisely identifies the tampered region, accounting for 55% of the total image area.
Overall Match Percentage	84.4%	Confirms the partial nature of the tampering, validating the localized detection strategy.

Table 2: Results of the integrated tools analysis on the variable blocks.

Integrated Detection Method	Value Recorded	Function and Objective	Analysis and Tampering Confirmation
ELA Analysis (Error Level Analysis)	9.05	Detects areas with varying compression levels (JPEG Inconsistencies), indicating re-saving or content merging.	The elevated value of 9.05 strongly confirms that the 10 blocks were subjected to modification and re-compression, validating the tampering indicated by the hash mismatch.
Copy Move	100.0%	Identifies if a part of the image has been copied and pasted elsewhere within the same image.	The value of 100.0% excludes "Copy-Move Forgery" as the type of tampering in this specific case, directing investigators toward other types of manipulation.
Block Matching	Enabled	Provides continuous, direct comparison between the block's data and the authenticated Blockchain hash.	Served as the primary authentication layer, whose failure was subsequently confirmed by the forensic tools.

7 RESULTS AND ANALYSIS

This section presents the practical results obtained from the proposed system. The main focus is on evaluating its ability to accurately localize image tampering and determine the type of manipulation using integrated forensic tools. The overall workflow of the proposed forensic framework, including blockchain-based verification, is illustrated in Figure 5a–5d.

7.1 Overcoming the Challenge of Localized Tampering

The results presented in Table 1 show that reliable detection can be achieved by analyzing only 16 image blocks, which is sufficient to overcome the limitations of traditional global hashing techniques. These conventional methods typically classify an entire image as either tampered or untampered, even when only small regions are modified.

The proposed approach replaces this binary decision model with a localized similarity-based assessment, achieving an 84.4% match score. This represents a significant improvement in forensic precision and provides more meaningful evidence for digital investigation.

In addition, the spatial distribution of the detected red blocks in Figure 4 confirms that the manipulation is restricted to a limited region of the image. Instead of labeling the entire image as corrupted, the system successfully isolates the affected area. This demonstrates that the 8×8 segmentation strategy ensures high localization accuracy.

7.2 Results of Advanced Analysis and Qualitative Confirmation

The Interactive Tampering Analysis (ITA) phase extends the investigation from identifying *where* the modification occurred to understanding *how* it was performed. In this stage, forensic analysis is applied to the selected 16 variable blocks.

As shown in Table 2, the combination of hash-based matching for spatial localization and Error Level Analysis (ELA) for tampering type identification provides the strongest capability of the proposed system. Together, these techniques generate multi-dimensional forensic evidence that increases the reliability of the final detection decision.

The complete workflow of the proposed system and its blockchain verification process is illustrated in Figure 5a–5d, demonstrating the system behavior across different operational states.

8 CONCLUSIONS

This study seeks to deliver a hybrid system for the documentation of digital evidence as well as the in-situ detection of any possible tampering, based on blockchain technology. The experiment results have been very successful in achieving the goals. The main part of the contribution is based on separating an image into non-overlapping 8 × 8 pixel blocks and capturing their respective partial hashes on the blockchain to provide immutability and non-repudiation. Results show that tampering can be detected with high accuracy by isolating just 10 variable blocks out of a total of 64, which gives an overall match rate of 84.4%. The situation is like that in Figure 5:(c). This solves the problems related to full-hash methods. Additionally, integration with forensic tools improved reliability since an Error Level Analysis value of 84.4% indicated pressure variation found within suspicious blocks as qualitative proof of tampering. Accordingly, the proposed system provides a three-layer evidence (documentation, location, and type), focused on providing a strong and reliable answer for enhancing the protection of the digital evidence security chain in investigation environments.

ACKNOWLEDGMENTS

The author(s) would like to thank Al-Mustansiriyah University (www.uomustansiriyah.edu.iq) Baghdad-Iraq for its support in the present work.

REFERENCES

[1] P. Santamaría, L. Tobarra, R. Pastor-Vargas, and A. Robles-Gómez, "Smart contracts for managing the chain-of-custody of digital evidence: A practical case of study," Smart Cities, vol. 6, no. 2, pp. 709-727, 2023, [Online]. Available: https://doi.org/10.3390/smartcities6020034.

[2] M. S. Akhtar and T. Feng, "Using blockchain to ensure the integrity of digital forensic evidence in an IoT environment," EAI Endorsed Transactions on Creative Technologies, vol. 9, no. 31, 2022, [Online]. Available: http://dx.doi.org/10.4108/eai.3-6-2022.174089.

[3] H. Patil, R. K. Kohli, S. Puri, and P. Puri, "Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework," Egyptian Journal of Forensic Sciences, vol. 14, Art. no. 12, 2024, [Online]. Available: https://doi.org/10.1186/s41935-023-00383-w.

[4] H. S. Shrunga, M. Ashwini, U. Deepthi, R. Spandana, and K. R. Rakesh, "A survey on blockchain based digital forensics framework," International Journal of Research in Applied Science & Engineering Technology, vol. 10, no. 4, pp. 2542-2549, 2022, [Online]. Available: https://doi.org/10.22214/ijraset.2022.41841.

[5] H. Christine, K. T. Novelianto, M. Restiawati, H. Y. Jayanti, and A. Afriyadi, "A study of permissioned blockchain-based framework for land ownership tracking in Indonesia," Interkom, vol. 17, no. 3, pp. 119-126, 2022, [Online]. Available: https://doi.org/10.35969/interkom.v17i3.258.

[6] F. Ghozzi, K. K. Jabbar, and A. Fakhfakh, "Image Authentication Proofing Scheme Based on RLG by Employing the Characteristics of DCT," Iraqi Journal of Science, 2025, doi: 10.24996/ijs.2025.66.9.34.

[7] B. A. Salim, H. A. Younis, and M. A. Aljabery, "A study on secure image encryption based on blockchain," Iraqi Journal of Intelligent Computing and Informatics (IJICI), vol. 3, no. 1, pp. 22-29, 2024, [Online]. Available: https://doi.org/10.52940/ijici.v3i1.88.

[8] S. K. Gaid and K. K. Jabbar, "Frequency Domain for Color Image Authentication Proofing," Journal of Physics: Conference Series, vol. 1963, no. 1, p. 012094, 2021, [Online]. Available: https://doi.org/10.1088/1742-6596/1963/1/012094.

[9] R. Kumar et al., "Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images," Computerized Medical Imaging and Graphics, vol. 102, p. 102139, 2022, [Online]. Available: https://doi.org/10.1016/j.compmedimag.2022.102139.

[10] K. K. Jabbar and G. Y. Whaib, "Image encryption using RC4 based 5D-chaotic system under spatial domain," AIP Conference Proceedings, vol. 2591, p. 030016, 2023, [Online]. Available: https://doi.org/10.1063/5.0120413.

[11] M. Bin Saif, S. Migliorini, and F. Spoto, "Efficient and Secure Distributed Data Storage and Retrieval Using Interplanetary File System and Blockchain," Future Internet, vol. 16, no. 3, p. 98, 2024, [Online]. Available: https://doi.org/10.3390/fi16030098.

[12] A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," IEEE Access, vol. 10, pp. 11065-11089, 2022, [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3142508.

[13] S. A. Mohsin and R. A. Muhajjar, "A Review of Blockchain Based Solutions for Intellectual Property Rights Protection and Management," Iraqi J. Intell. Comput. Inf., vol. 4, no. 2, pp. 90-102, 2025.

[14] O. Kuznetsov, P. Sernani, L. Romeo, E. Frontoni, and A. Mancini, "On the Integration of Artificial Intelligence and Blockchain Technology: A Perspective About Security," IEEE Access, vol. 12, pp. 3881-3897, 2024, [Online]. Available: https://doi.org/10.1109/ACCESS.2023.3349019.

[15] M. Cu, G. Peko, J. Chan, and D. Sundaram, "Blockchain-based Continuous Timestamps Tracking System: Towards Ownership Information Believability," in Proc. 56th Hawaii Int. Conf. System Sciences (HICSS), 2023, pp. 5343-5352, [Online]. Available: https://doi.org/10.24251/HICSS.2023.652.

[16] Z. Yuan, J. Wu, J. Gong, Y. Liu, G. Tian, and J. Wang, "Blockchain-Based Self-Auditing Scheme with Batch Verification for Decentralized Storage," Wireless Commun. Mobile Comput., vol. 2022, Art. no. 6998046, 2022, [Online]. Available: https://doi.org/10.1155/2022/6998046.

[17] M. D. Sheldon, "Tracking Tangible Asset Ownership and Provenance with Blockchain," Journal of Information Systems, vol. 36, no. 3, pp. 153-175, 2022, [Online]. Available: https://doi.org/10.2308/ISYS-2020-042.

[18] Y. Liu, Y. Zhang, Y. Yang, and Y. Ma, "DOCS: A Data Ownership Confirmation Scheme for Distributed Data Trading," Systems, vol. 10, no. 6, p. 226, 2022, [Online]. Available: https://doi.org/10.3390/systems10060226.

[19] A. R. Nugroho, S. Anoraga, and F. Esfandiari, "Guarantee of Protection of Electronic Land Certificates as Proof of Ownership of Land Rights," Indonesia Law Reform Journal, vol. 3, no. 2, pp. 234-242, 2023, [Online]. Available: https://doi.org/10.22219/ilrej.v3i2.29197.

[20] A. Trujillo, "Hyperownership: Beyond the Current State of Interaction with Digital Property," in Proc. 33rd ACM Conf. Hypertext and Social Media, 2022, pp. 240-243, [Online]. Available: https://doi.org/10.1145/3511095.3536373.