International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 12, No.1 (Oct-2022)

https://dx.doi.org/10.12785/ijcds/1201100

Video Data Authentication Model Using Blockchain Technology

Noor Adil Abdel Moneim[1] and Methaq Talib Gaata[2]

[1,2]*Department of Computer Science, Mustansiriyah University, Baghdad, Iraq*

Received 22 Jan. 2021, Revised 15 Jul. 2022, Accepted 23 Jul. 2022, Published 31 Oct. 2022

Abstract: Video authentication is becoming increasingly important as video obtain and editing has become easier with the help of modern technologies. Also, tamper localization is getting more and more difficult due to the great development of editing software. Signature-based video authentication technologies rely on storing the video signature until authentication is required. This is a drawback because the signature is controlled by a single entity that can fail. Therefore, the centralized approach is not at all trustworthy. This paper proposes the use of Blockchain technology to store video signatures to solve such problems. In this framework, the video signature is stored in a decentralized network. It eliminates the need for a trusted third party and allowing for the control of private data. This system provides the ability to protect large data from manipulation and alteration attacks on the content. Where the size of the vector that is embedded on the blockchain is very small in comparison to the size of the video extracted from it. The change in the vector values indicates the change caused by manipulation within the single frame, so it can be determined which frames were attacked.

Keywords: Video authentication, Multimedia Security, Tamper localization, Blockchain technology

1. Introduction

At present, there are a lot of video recording devices, also a lot of editing programs used to modify these videos. This availability of editing tools makes digital videos unreliable. Therefore, there is a great need for means to authenticate digital videos, and to check what modifications may have been made to them [1]. The digital media content authentication problem can be solved by two main directions: watermark-based authentication [2], [3], [4], and signature-based authentication [5], [6].

Watermark-based authentication technologies add a series of data (watermark) hidden in the content that needs to be secured. The addition must be in a way that does not affect the perceptual quality of the content. The watermark is extracted from the content and compared with the reference one to discover if the content was forged or not. For the content to be authentic, the sequences must identical [7].

The second way to secure the content of the multimedia is to create a digital signature, where the unique features are extracted from the content and stored as a signature. When the received multimedia authentication is requested features are extracted from the received content and compared with the stored signature. If the content has been forged, the new extracted feature sequence will differ from the stored digital signature sequence. The necessity of having a digital signature available on the side of the encoder, or adding authentication data to the content itself is a major drawback of these technologies [6].

The rest of this paper is organized as follows: Section 2 presents relevant works. Section 3 explains the blockchain technique, section 4 describes the proposed video documentation method, the results of the scheme are discussed in section 5, and finally the conclusion in section 6.

2. RELATED WORK

In recent times, a lot of research conducted based on blockchain technology, due to the advantages that this technology provides [8]. The research [9] suggested a multimedia framework, in which a watermark is embedded in the images to be authenticated. This watermark contains the blockchain transaction ID. Once the watermark is extracted, the ID is passed to the distributed ledger to retrieve the transaction path.

The research [10] presented a design that will apply data integrity through an Android device, in which the integrity of the recorded video is verified over the Internet. A video cryptography hash is created, and then this hash is transferred to the blockchain. During the integrity assurance process, a hash of the received video is created for comparison with those found in the blockchain.

The research [11] relied upon blockchain to create a design for multimedia digital rights management (DRM). The content owner information is embedded in the content data itself. The content is then stored with DRM in a decen-

E-mail address: noor.adil.04@uomustansiriyah.edu.iq

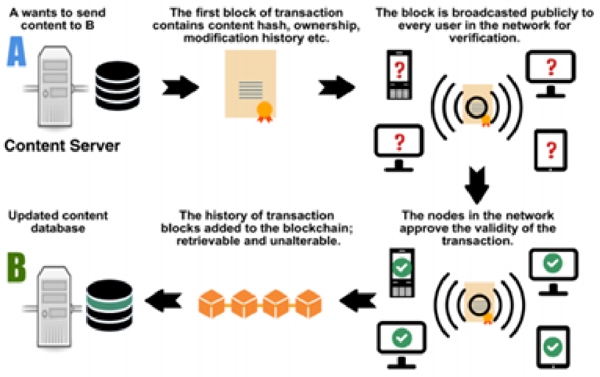

A wants to send content to B
A
Content Server
The first block of transaction contains content hash, ownership, modification history etc.
The block is broadcasted publicly to every user in the network for verification.
?
The nodes in the network approve the validity of the transaction.
The history of transaction blocks added to the blockchain; retrievable and unalterable.
Updated content database
B

Figure 1. An overview of the working principle of the blockchain [9]

tralized ledger to ensure protection, and misuse detection of multimedia.

In [12] a prototype video fraud detection was proposed through the blockchain. The hash value of the video is created after it is stored via the blockchain nodes. The video tampering process leads to changes in the hash value of the video.

Blockchain technology is being exploited in [13] to ensure that the summary of videos is transmitted safely, and reliably to consumers. A cryptography hash is created for the summarized video that is sent via the blockchain, the system allows remote users to have access to a summarized video that cannot be tampered with.

The proposed technology ensures video authentication and detection of where video frames have been tampered with, by embedding the hash of a blockchain transaction in the video that wants to be validated.

3. BLOCKCHAIN TECHNOLOGY DESCRIPTION

A blockchain is known as a distributed ledger, which is structured in a linked list of blocks. Each block contains transactions in an organized set [14]. This technology provides a new model for securely storing data, as it relies mainly on decentralization in its work [15]. Fig. 1 shows an example of how the blockchain works, where payment is sent from A to B. The transaction is validated by other nodes. If the transaction fails or is tampered with, the transaction will not be acknowledged. Eventually, all nodes will verify the transaction and add it to their copy of the ledger. Blocks of information about transactions are arranged and stored together in chronological order and are thus called a blockchain [9].

All blockchain nodes hold a copy of the information so that it is not easily taken malicious action against such information [16]. The new block is linked to the previous blocks through a unique cryptography hash. To make any modification for the content of a block, the previous block will still contain the hash of the next block. Therefore, the hacker must change all the next blocks for a very large number of devices that have a copy of the blockchain to hide the change on one block [17]. So that, the information on the blockchain is secure, and cannot be tampered with.

By virtue use of blockchain technology, the broker (such as the bank) has been removed from cash transfer transactions [18]. As a result, the cost of these transactions was reduced as well as the risks associated with having that broker. Blockchain technology has proven efficient, and secure storage of transactions [19]. Originally the blockchain was used for digital currency Bitcoin [20]. But recently they are relied on it during various applications for several purposes and implemented it on many platforms.

The blockchain is a special type of database, in which data is replicated to all participating nodes on the network instead of stored on a centralized server. Created applications called decentralized applications “DApp”, to take advantage of this database in storing and retrieving data. These applications do not depend on a central database, but rather on decentralized databases based on the blockchain. Therefore, there is no single point of control or failure [21].

In this approach, it is suggested to use blockchain technology due to its proven reliability when it comes to efficient and secure storage. Through the blockchain, the video authentication is confirmed, and the tampered video frames are revealed. This is done by including the hash of the blockchain transaction in the video to be authenticated. The exact details of the process will be explained in the next section.

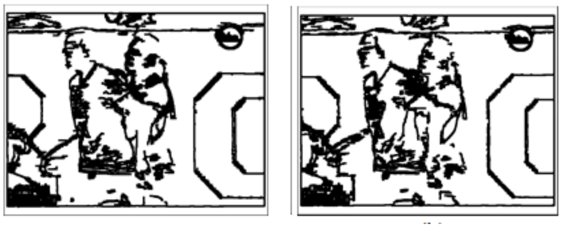
4. PROPOSED THE VIDEO AUTHENTICATION METHOD

Content authentication is the technology by which the user guarantees that the data received by him is original, and has not been tampered with. For video validation, two consecutive frames of the test video (let’s say they are A and B) were taken as shown in Fig. 2. The edge detection technique is then applied to each of the A and B frames (Canny detector was used) to produce two binary images as shown in Fig. 3 . Set the edge pixel newly appeared in frame B away from the edge pixel of frame A as the edge input pixel (EI). Also, the edge pixel that disappeared in frame B away from the edge pixel of frame A was defined as an edge output pixel (EO).

The difference between the two frames is measured by calculating the difference between the sum of the input edge, and the sum of the output edge (D1 = EI - EO). This process repeated for each pair of test video frames, as a result, a series of values for the difference between edges of frames were obtained. That series of different values were represented as a vector, as shown in Fig. 4. The edge difference vector can be considered as a signature of the video since it represents a unique feature of that video.

(a) (b)

Figure 2. Input frame from video: (a) first frame A and (b) second frame B



(a) (b)

Figure 3. Edge detection: (a) edges of the first frame A and (b) edges of the second frame B

It is important to note that the signature extraction process does not change the quality of the video in any way, as these calculations are made to obtain the signature while the video remains the same. Most of the methods in the literature that depends on the signature for authentication stop here, and rely on sending the signature encrypted in a file with the video to be authenticated.

For this application, the blockchain provided by [22] was used due to the big size of the blocks used. But any other blockchain technology can be used that provides a large block size. To store data on the specific blockchain, an account is registered on their website https://docs.originstamp.com/. After creating the account, the user will be able to send transactions that carry the signature of video to the network, which ensures that it is not possible to manipulate this data by any malicious party. Once the transaction is posted on the network, a unique transaction ID consisting of 64 hexadecimal digits is generated. The video signature can be found at any time on the specified blockchain if one owns the transaction ID. The transaction ID is also then included in a set of video frames. The LSP algorithm was used to include the transaction ID inside frames.

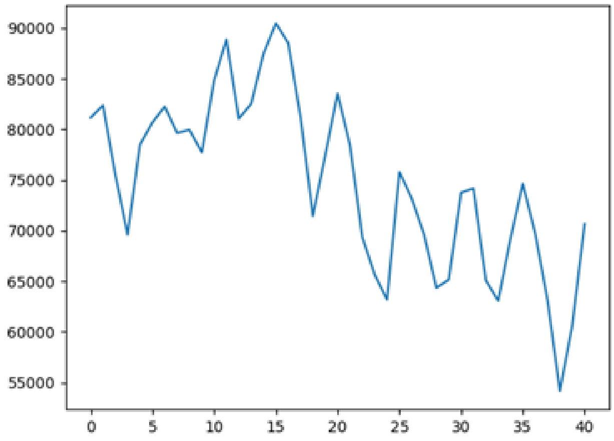


Figure 4. Edge difference vector of the original video

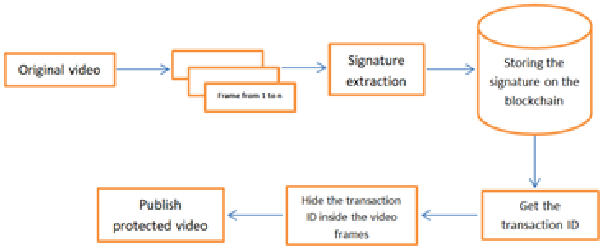


Figure 5. Overview of the proposed video authentication

Fig. 5 is a scheme that shows the path proposed to authentication the video.

To test the authenticity of the received video, one needs to know where the transaction ID hides, to extract it. Then one can search for the transaction on the blockchain to retrieve the original copy of the signature. The signature obtained from the blockchain is compared with the signature extracted using the same algorithm from the video received. It is declared that the received video is original, and did not tamper with when the two signatures are identical. If the video is tampered with, the signature values extracted from the received video will differ from those stored on the blockchain. This method can locate the tampered frames in the video.

Fig. 6 shows the proposed method to ensure the integrity of the submitted video.

5. RESULTS AND DISCUSSION

Python was used to extract the video signature as well as to embed the transaction ID inside the video frames because it is supported by many libraries that facilitate working with videos. To simulate the manipulation of video authentication, testing was performed on AVI videos. It is also possible to perform the authentication for any type of video. To obtain the results, the video signature represented by a vector of values was extracted, which was mentioned in Fig. 4. Then these values were stored by the blockchain to ensure that they were not tampered with. After that, the blockchain transaction ID is embedded inside the video frames, so that the user can find the original signature of the video by transaction ID without return to the owner of the

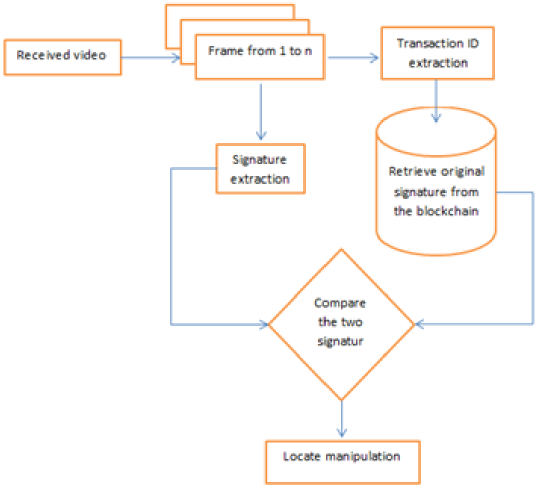


Figure 6. The proposed method to ensure the integrity of the submitted video

video. Once the transaction ID was included in the video frames, the video frames were tampered with by adding salt and pepper noise, by a very small percentage (0.001). Only the frames (4, 18, and 37) have been a modification, shown in Fig.7 , which represents the frames before the manipulation, and Fig. 8 , which shows the frames after the attack. Fig. 9 shows the change in the signature vector after modifying video frames.

The signature stored on the blockchain is retrieved by looking up the transaction ID within the blockchain. Once the signature is obtained from the blockchain, it is compared to the signature extracted from the newly received video. Spots of tampering in video frames can be detected where the tampering appears in the frames (4, 18, 37), it can be seen that the manipulation of a single frame affects two values of the signature vector. . Due to the comparison of the edges of Frame 3 with the edges of Frame 4 as well as the comparison of the edges of Frame 4 with the edges of Frame 5, the manipulation performed on Frame 4 will affect two of the signature vector values.

The signature was extracted from the original video (81157. 82370. 75494. 69590. 78498. 80672. 82254. 79649. 79963. 77741. 84869. 88883. 81059. 82514. 87479. 90495. 88517. 81152. 71432. 77418. 83559. 78446. 69353. 65642. 63174. 75788. 73191. 69636. 64346. 65149. 73755. 74164. 65085. 63054. 69173. 74624. 69745. 63125. 54147. 60626. 70669.).

And the signature extracted from the attacker's video (81157. 82370. 75494. 71973. 80700. 80672. 82254. 79649. 79963. 77741. 84869. 88883. 81059. 82514. 87479. 90495. 88517. 84336. 75455. 77418. 83559. 78446. 69353. 65642. 63174. 75788. 73191. 69636. 64346. 65149. 73755. 74164. 65085. 63054. 69173. 74624. 73417. 66140. 54147.

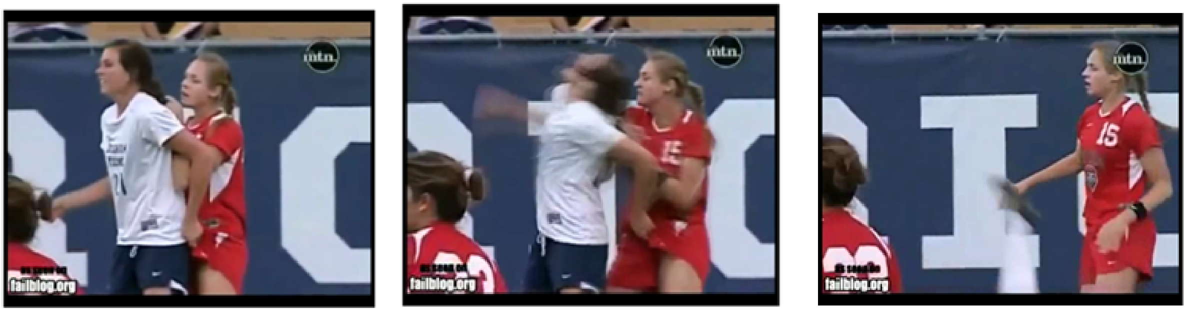
To facilitate the task of detecting tampered frames in a video, an application has been created in Python to compare the signature retrieved from the blockchain with the new signature extracted from the video. If the frame is intact and tamper-free, the difference between the two values is denoted by 0, but if the frame is tampered with, the difference between the two values is denoted by 1. Fig. 10 clearly shows the locations of the manipulation inside the three video frames.

To further verify the system efficiency in detecting tampered areas, the dimensions of the video frames were changed without deletions or additions within the frame. Using the proposed system, an edge difference vector was generated for the original video, which is used to verify the integrity of the video. Fig. 11 shows the first and last frames of the original video. The edge difference vector has been added to the blockchain database to prevent it from messing around. Then the original video frames were attacked to change the dimensions of the protected video frame. Fig. 12 shows the dimensions of the first and last frames after the change. To prove the process of alteration made to the video, a new edge difference vector was generated for the video that was manipulated, that was received from the sender. The tamper-proof edge difference vector is then retrieved from the blockchain. Through the previous Python software, in a few simple steps, the edge difference vector generated for the video received from the sender is compared with the edge difference vector downloaded from the blockchain.

The signature was extracted from the original video: (81157. 82370. 75494. 69590. 78498. 80672. 82254. 79649. 79963. 77741. 84869. 88883. 81059. 82514. 87479. 90495. 88517. 81152. 71432. 77418. 83559. 78446. 69353. 65642. 63174. 75788. 73191. 69636. 64346. 65149. 73755. 74164. 65085. 63054. 69173. 74624. 69745. 63125. 54147. 60626. 70669.).

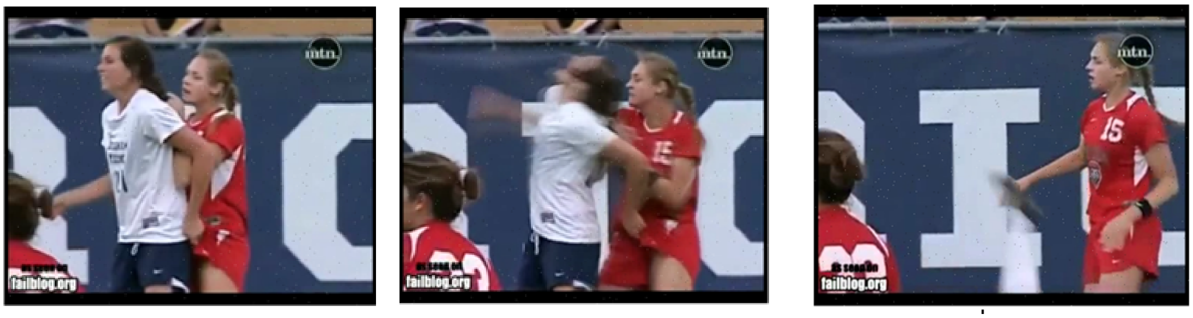
And the signature extracted from the video that was attacked: (51131. 55635. 53401. 50056. 54133. 51918. 55748. 56637. 56021. 53831. 56466. 59875. 56165. 56568. 57977. 58147. 60909. 57900. 52646. 54887. 55089. 52645. 50071. 50531. 46917. 48844. 48269. 48662. 43786. 44260. 47709. 49715. 45672. 44883. 47542. 44508. 44951. 42844. 36810. 40019. 43969.).

Through the comparison process, it has been proven that all video frames have been tampered with due to the change in the dimensions of these frames. Thus, the safety of video frames from video manipulation attacks can be ensured, as well as identification of those attacks without compromising the accuracy of the video or changing its original content. The vector of the signature values embedded in the blockchain is drawn to ensure they are not tampered with. A vector for the signature values extracted from the received video has also been drawn. The locations of the attacks on the video frames can be found by plotting the



(a) (b) (c)

Figure 7. The frames before tampering: (a) frame no.4 (b) frame no.18 and (c) frame no.37



(a) (b) (c)

Figure 8. The frames after the attack: (a) frame no.4 (b) frame no.18 and (c) frame no.37

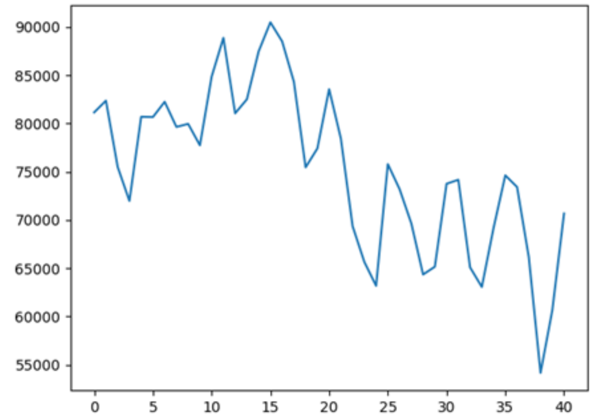


Figure 9. Edge difference vector for the attacked video.

difference vector between the two previous vectors. Fig. 13 shows the difference between the two vectors, showing that the attacks affected all video frames.

Through previous experiences, it was proved that the system can detect tampering spots inside video frames. Also, a change in the length of the vector embedded in the blockchain can detect attacks by which some frames

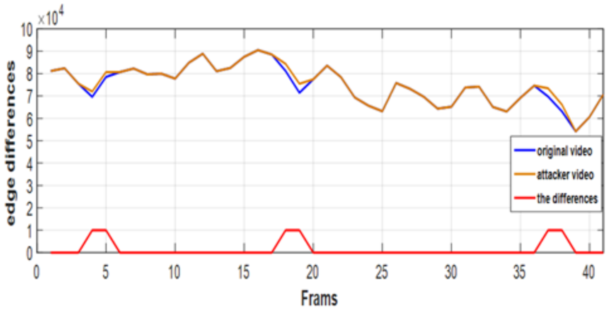
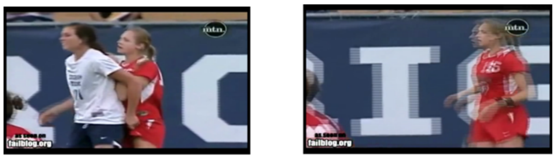


Figure 10. The difference between the two signatures to identify which frames tampered with.

(a) (b)

Figure 11. Frames from the original video: (a) first frame, and (b) last frame



(a) (b)

Figure 12. Frames from the video that was attacked: (a) first frame, and (b) last frame

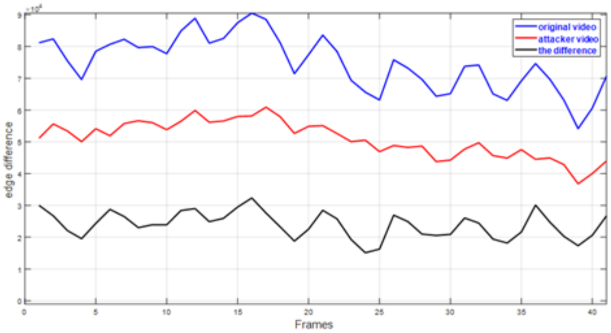


Figure 13. Compare vectors to locate attacks.

were added or deleted on the original video frames. Since the increase in the values of the signature extracted from the received video compared to the signature embedded in the blockchain indicates that additional frames were inserted within the original video. Also, the decrease in the signature values indicates the presence of some frames that have been deleted from within the original video.

Several videos have been downloaded from YouTube to implement and test the proposed system. The results showed that the proposed system can authenticate the video files correctly with the ability to identify the places of tampering. On the other hand, traditional methods of authenticating video files require either reducing their quality or increasing their size in addition to being time-consuming. While, decentralization technology is safe and reliable, and it is an effective tool for authenticating digital file content without compromising video quality or increasing size.

6. CONCLUSIONS

In this paper, a new framework for video authentication is proposed and identifies the places of manipulation based on the blockchain. The signature extracted from the video to be authenticated is published on the blockchain, based on the difference in edges between the video frames. After the video reaches the target, the original video signature is retrieved from the blockchain, which will be compared to the signature extracted from the received video. Changing a single pixel within a video frame will change the value in the vector. This ensuring the ability of detects small manipulations with video frames. Also, a change in the number of vector values indicates deletions and additions of video frames, ensuring that video frames are preserved without tampering. Finally, this research demonstrated the potential to facilitate the task of detecting fraud and locating manipulation within video frames.

As future work, a video authentication system could be developed using Blockchain technology to authenticate audio recordings and detect fraud. We expect the proposed digital authentication system to improve the security of all digital files, quickly, and easily will detect tampering sites.

References

[1] B. Azizian and S. Ghaemmaghami, “Tampering detection and restoration of compressed video,” in *2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)*. IEEE, 2018, pp. 1–5.

[2] T. Venugopal and V. S. K. Reddy, “Image watermarking using two level encryption method based on chaotic logistic mapping and rivest shamir adleman algorithm,” *International Journal of Intelligent Engineering and Systems*, vol. 11, no. 6, pp. 271–281, 2018.

[3] L. Rakhmawati, S. Suwadi, and W. Wirawan, “Blind robust and self-embedding fragile image watermarking for image authentication and copyright protection with recovery capability,” *International Journal of Intelligent Engineering and Systems*, vol. 13, no. 5, pp. 197–210, 2020.

[4] N. N. Mood and V. S. Konkula, “A novel image watermarking scheme based on wavelet transform and genetic algorithm,” *Int. J. Intell. Eng. Syst*, vol. 11, no. 3, pp. 251–260, 2018.

[5] K. Sowmya and H. Chennamma, “Video authentication using watermark and digital signature—a study,” in *Proceedings of the First International Conference on Computational Intelligence and Informatics*. Springer, 2017, pp. 53–64.

[6] R. A. Dobre, R. O. Preda, C. C. Oprea, and I. Pirnog, “Authentication of jpeg images on the blockchain,” in *2018 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO)*. IEEE, 2018, pp. 211–215.

[7] C.-F. Lee, J.-J. Shen, and Z.-R. Chen, “A survey of watermarking-based authentication for digital image,” in *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*. IEEE, 2018, pp. 207–211.

[8] H. Zhao, Y. Liu, Y. Wang, X. Wang, and J. Li, “A blockchain-based data hiding method for data protection in digital video,” in *International Conference on Smart Blockchain*. Springer, 2018, pp. 99–110.

[9] D. Bhowmik and T. Feng, “The multimedia blockchain: A distributed and tamper-proof media transaction framework,” in *2017 22nd International Conference on Digital Signal Processing (DSP)*. IEEE, 2017, pp. 1–5.

[10] A. Hemlin Billström and F. Huss, “Video integrity through blockchain technology,” 2017.

[11] M. Zhaofeng, H. Weihua, and G. Hongmin, “A new blockchain-based trusted drm scheme for built-in content protection,” *EURASIP Journal on Image and Video Processing*, vol. 2018, no. 1, pp. 1–12, 2018.

[12] A. Dhiran, D. Kumar, A. Arora *et al.*, "Video fraud detection using blockchain," in *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*. IEEE, 2020, pp. 102–107.

[13] G. Khan, S. Jabeen, M. Z. Khan, M. U. G. Khan, and R. Iqbal, "Blockchain-enabled deep semantic video-to-video summarization for iot devices," *Computers & Electrical Engineering*, vol. 81, p. 106524, 2020.

[14] X. Xu, I. Weber, and M. Staples, *Architecture for blockchain applications*. Springer, 2019.

[15] Z. Meng, T. Morizumi, S. Miyata, and H. Kinoshita, "Design scheme of copyright management system based on digital watermarking and blockchain," in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2. IEEE, 2018, pp. 359–364.

[16] O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei, and K. A. Ogudo, "A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications," *International Journal of e-Collaboration (IJeC)*, vol. 16, no. 1, pp. 16–32, 2020.

[17] S. Ghimire, J. Y. Choi, and B. Lee, "Using blockchain for improved video integrity verification," *IEEE Transactions on Multimedia*, vol. 22, no. 1, pp. 108–121, 2019.

[18] A. Muwafaq and S. N. Alsaad, "Design scheme for copyright management system using blockchain and ipfs," *International Journal of Computing and Digital Systems*, vol. 10, pp. 613–618, 2021.

[19] P. W. Khan, Y.-C. Byun, and N. Park, "A data verification system for cctv surveillance cameras using blockchain technology in smart cities," *Electronics*, vol. 9, no. 3, p. 484, 2020.

[20] R. Xu, L. Zhang, H. Zhao, and Y. Peng, "Design of network media's digital rights management scheme based on blockchain technology," in *2017 IEEE 13th international symposium on autonomous decentralized system (ISADS)*. IEEE, 2017, pp. 128–133.

[21] B. Singhal, G. Dhameja, and P. S. Panda, *Beginning Blockchain: A Beginner's guide to building Blockchain solutions*. Springer, 2018.

[22] OriginStamp, "Blockchain Timestamps for Businesses." [Online]. Available: https://originstamp.com/

Noor Adil Abdel Moneim is a Master's student in the Department of Computer Science/ College of Science/ Mustansiriyah University. She is interested in information security.

Methaq Talib Gaata is a Professor in Computer Science at College of Science/ Mustansiriyah University / Baghdad / Iraq. He is interested in information Security and multimedia processing.