Blockchain-based Pipeline Custody System (BPCS) for Preserving Critical Video Evidence

Yun-Yi Fan, Chit-Jie Chew, Wei-Che Hung, Ying-Chin Chen, Jung-San Lee[*]

Department of Information Engineering and Computer Science, Feng Chia University, Taiwan
a19990101152@gmail.com, cjie723@gmail.com, abcd0989290543@gmail.com, ycchen.blythe@gmail.com, leejs@fcu.edu.tw

Abstract

The explosive development of network technology has driven the evolution of civilization, leading to the higher crime rate. Hence, CCTV cameras have been widely deployed to monitor criminal behaviors. The video of CCTV is considered as significant digital evidence. Due to the property of digital data, it is easily to copy and modify without electronic footprint, unlike the physical records. In case, the law enforcement starts to employ the blockchain technique due to its advantages, decentralization, transparency, and traceability, which can improve the legal effect. Unfortunately, blockchain network produces the tremendous overhead when it processes the data preservation based on the distributed communication. Thus, the gap and burden of data synchronization are the derivative issues. In order to solve the above problems, we aim to realize a blockchain-based pipeline custody system, so-called BPCS. The critical frame determination (CFD) technique is designed to catch the potential evidence image from the monitor, which is able to mitigate the storage cost of blockchain. Especially, the pipeline and directional ring strategy is proposed to aggregate the potential evidence in a batch file. This can reduce the burden on the chain of custody and shorten the time gap. The experimental results have demonstrated that BPCS can firmly possess the features of credibility and efficient through the comparisons and storage simulation.

Keywords: Surveillance camera, Custody, Blockchain, Pipeline, Directional ring strategy

1 Introduction

Undoubtedly, convenient life functions attract people to move to the city. This situation leads to densely populated. However, the higher the density of population, the higher the crime rate. Therefore, closed circuit television (CCTV) cameras have been widely deployed to monitor criminal behaviors [1-3], which belongs to Internet of Things (IoT) device. According to Comparitech [4], the report has given the top ten cities with the highest concentration of surveillance cameras in the world, as shown in Figure 1 Cities of China are the top one with an average of 372.8 cameras for every 1,000 people. Namely, each camera is responsible for guarding three humans averagely. Taking into a global consideration, every 1,000 people is observed by at least 60.5 cameras. Meanwhile, Piza et al. have indicated that mounting CCTVs in public place can effectively lower down 16% of crime rate [1]. Undoubtedly, CCTV is a crucial tool for inhibiting the crime. The monitor system can record the long-term scene in specific areas and help recover the detail of incident. Therefore, the world has more than hundred million active CCTVs based on IHS research [5], where is set up in intersection, entrance, and exit. When the criminal incident happened, the video of CCTV is considered as significant digital evidence [3].

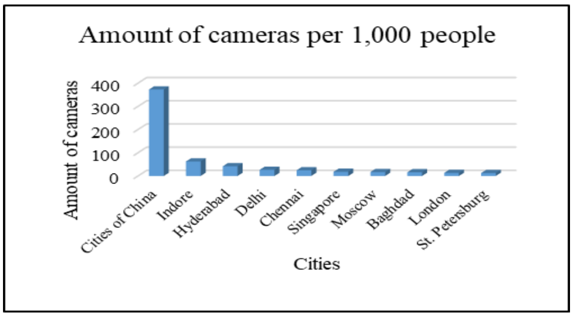


Figure 1. The top 10 cities with the highest concentration of CCTV cameras

However, CCTV recording the potential evidence might be compromised by malicious attacker. SonicWALL cyber threat report indicated that business reality has suffered from 56.9 million IoT attacks [6]. Due to the property of digital data, it is easily to copy and modify without electronic footprint, unlike the physical records. Therefore, proving the chain of custody is particularly significant in a criminal case. Following the standard of ISO/IEC 27037 [7], the potential digital evidence shall be handled through identification, collection, acquisition, and preservation of standardization procedures by valid forensic clerk therefore it can be of the evidential value. Since the evidence is free of contamination by forensic member, it is ensured the admissibility in the court. Otherwise, it cannot be accepted by judge and jury. Furthermore, storing digital evidence in a single section has the concerns of evidence integrity. The law enforcement starts to employ the blockchain technique [12-17] due to its advantages, decentralization, transparency, and traceability, which can improve the legal effect. Also, the nation gradually

[*]Corresponding Author: Jung-San Lee; E-mail: leejs@fcu.edu.tw
DOI: 10.53106/160792642024052503010

admits the blockchain network used in the law enforcement, including United States [8], France [9], China [10], and United Kingdom [11]. Unfortunately, blockchain network produces the tremendous overhead when it processes the data preservation based on the distributed communication. Thus, the gap and burden of data synchronization are the derivative issues. The former means that the time gap occurs when the digital data is uploaded and stored to the whole of peers in the blockchain network. The integrity of data might not be confirmed if it is tempered by attacker during gap period. The latter describes that the storage overhead of a 24-hour uninterrupted recording is very large; thus, uploading these data to the blockchain network for confirming the evidence is an unrealistic manner.

The critical characteristics of CCTV are as follows:

- Confidentiality: As people know that the data on the blockchain are visible and not all the evidence could be shown to the public. Thus, unauthorized participant shall not be able to learn the content of data in the blockchain.
- Integrity: All the information shall be kept the same to prevent evidence pollution.
- Availability: A legal user shall be able to access the data on the chain once they can connect to the network.
- Scalability: Even data are generated quickly and enormously, the ledger overhead of each participant shall be light and feasible to realize the platform.
- Low storage overhead: When it is confirmed that the evidence is not contaminated, it is necessary to compare the copy data. This characteristic is to ensure that only a lightweight storage cost is required in recording the evidence. In a centralized method, a record copy is kept for future investigation.

In order to solve the above problems, we aim to realize a blockchain-based pipeline custody system, so-called BPCS. The authors integrate blockchain and image processing techniques [18-21] to preserve the critical video evidence. The distributed storage architecture of blockchain is applied to guarantee the integrity, traceability, and immutability of video evidence. This can increase the credibility of surveillance camera. As to the critical streaming media, we have designed a critical frame determination (CFD) technique to catch the potential evidence image from the monitor, which is able to mitigate the storage cost of blockchain. Especially, we have proposed the pipeline and directional ring strategy to aggregate the potential evidence in a batch file. This can reduce the burden on the chain of custody and shorten the time gap. The experimental results have demonstrated that BPCS can firmly possess the features of credibility and efficient through the comparisons and storage simulation.

The rest of this article is organized as follows. The concept of blockchain is introduced in section 2, while the details of BPCS are described in section 3. The simulation results and corresponding analysis are explained in section 4, followed by the conclusions in section 5.

2 The Concept of Blockchain

The blockchain is a decentralized data storage technology [22], which has been widely applied to the fields of finance [22-23], industry [24], medicine [25-26], and IoT [27]. According to the cryptographic robustness, each block is stored in series to protect the data on the chain from being tampered. The block content is depicted as Figure 2, including the fields of timestamp, data, previous hash value, and hash value of the current block. Linking each block with the hash value of the previous one, the blockchain can achieve protection of the chain-like data. Users maintaining the blockchain data are defined as nodes. All these nodes share the responsibility for recording the data and comply with the same regulations to preserve the properties of decentralization, transparency, and non-tampering.

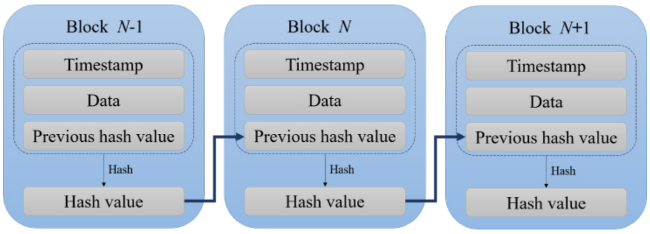


Figure 2. A scenario of blockchain diagram

Once a node has completed the block calculation of Figure 2, the block is broadcasted to the blockchain. It is then stored in the ledger of each node after a verification consensus. Actually, the majority decision rule is adopted in the blockchain to confirm the correctness of the data. It means that the block content is true when more than 51% of the nodes have approved the block, and vice versa. Therefore, a trusted third party or any central agency can be removed from the preservation of data to achieve the decentralization. Furthermore, the shared data are not generated by a specific node and public to all. Without loss of generality, this has realized the transparency that everyone is able to check the data on the chain. As each block contains the hash value of the previous block, all blocks are strongly linked together with the definition of cryptographic one-way hash function [28]. In case that a node tries to modify a specific block content without being founded, it shall have the ability to modify 51% of the nodes in the chain simultaneously, which is regarded as an infeasible assumption. Thus, the essential of non-tampering could be confirmed.

Table 1. Notations used in BPCS

Symbols	Definition
F_b	The background video frame.
F	A new video frame.
$X(x, y)$	The pixel value of image X at location (x, y).
A	The average image of F.
M_A	The mask of average operation.

Symbols	Definition
D	The difference image between F and F_b.
BM	The binary map of F.
C	The critical image of F.
M_C	The structuring element of dilation operation and erosion operation.
P	The evidence sign of F.
n	The total number of surveillance cameras
S_i	Surveillance camera i, where i =1, 2, …, n
F_i	The video frame generated from S_i
S_{start} /S_{end}	The start/end surveillance camera of one round aggregation, $S_{start}/S_{end} \in [S_1, S_2, S_3, \ldots, S_n]$
SK_i /PK_i	The private/public key of S_i
$ESK_i()$ /$DPK_i()$	The signature/verification operation by SK_i/PK_i
$H()$	One-way hash function
bf	The batch file
t_{start} /t_{end}	The start/end timestamp of a bf
T	Time threshold of one round aggregation
TL	Time threshold of one surveillance camera for aggregation

3 BPCS: Blockchain-based Pipeline Custody System

The flowchart of BPCS is displayed in Figure 3, including the critical frame determination (CFD), aggregation phase, recording phase, and verification phase. The first phase is to determine if the captured frame is potential evidence or not. The potential evidence is then aggregated to a batch file in the second phase according to the pipeline and directional ring strategy. Hereafter, a surveillance camera hitting the eventual aggregation uploads the data to the blockchain network. Once a suspicion occurs to any specific data, the final phase can help an investigator verify if the data have been tampered or not. Notations used in BPCS are displayed in Table 1.

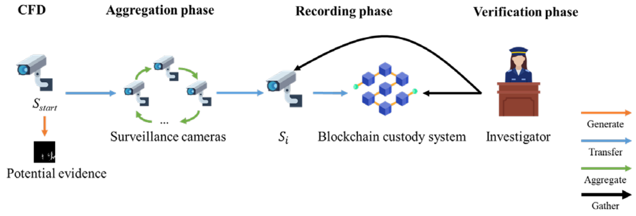


Figure 3. The flowchart of BPCS

3.1 Critical Frame Determination (CFD)

The CFD is to examine whether a frame has the region of interesting (ROI) or not. The outcome relies on the concept of critical motion detection. CFD consists of four operations, average filter, discrepancy processing, binary transformation, and characteristics extraction. Here we use an example to give an overview of CFD and the gradual outcomes are shown in Figure 4. Note that CFD randomly selects one frame from video per second.

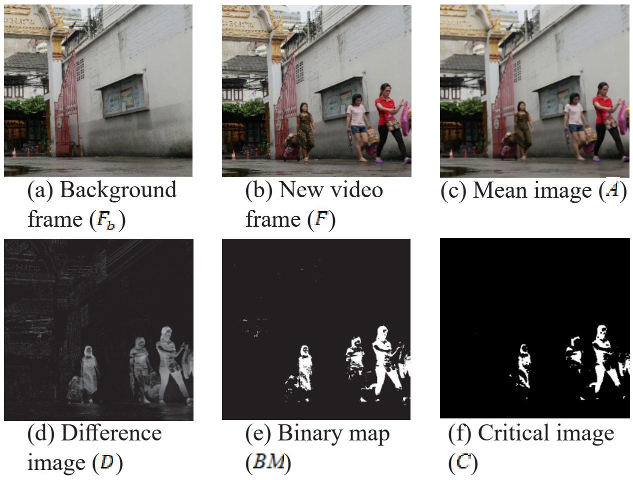

(a) Background frame (F_b)
(b) New video frame (F)
(c) Mean image (A)
(d) Difference image (D)
(e) Binary map (BM)
(f) Critical image (C)

Figure 4. Gradual outcomes of CFD

Step 1. Average filter: this step is to filter the noise in a frame.

Firstly, we have to decide a clear video frame, which is the background frame F_b, as shown in Figure 4(a). CFD continuously detects whether there is a new frame F or not, as shown in Figure 4(b). If it is a new frame, it will be captured. Here a 3*3 mask M_A is used to convolve the new video frame F from left to right and top to bottom according to (1) and (2). An average image A is then generated, as depicted in Figure 4(c).

$$A(x,y) = M_A(i,j) * F(x,y). \quad \textbf{(1)}$$

$$M_A(i,j) = \begin{bmatrix} 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \\ 1/9 & 1/9 & 1/9 \end{bmatrix}. \quad \textbf{(2)}$$

Step 2. Discrepancy processing: this step is to distinguish the foreground and background to obtain a difference image D.

Following the example of step 1, the difference image D is illustrated in Figure 4(d). Based on (3), all the pixels of A subtract from the corresponding pixel values from the background frame F_b are the ones of D.

$$D(x,y) = |\, A(x,y) - F_b(x,y) \,|. \quad \textbf{(3)}$$

Step 3. Binary transformation: this step is to transform the frame into binary image for capturing the ROI, which is called binary map (BM).

The BM of the example is displayed in Figure 4(e), which is obtained from the difference image D by (4). The value 255 is set to indicate the moving objects when the pixel value of D is non-zero. Otherwise, the value equals to 0.

$$BM(x,y) = \begin{cases} 255, \text{ if } D(x,y) \neq 0, \\ 0, \text{ otherwise.} \end{cases} \quad \textbf{(4)}$$

Step 4. Characteristics extraction: this step is to strengthen the characteristics of the captured ROI and output a critical frame C.

The critical frame C is calculated by (5), as shown in Figure 4(f), where the 3*3 structuring element M_C is depicted in (6), and the dilation operation and erosion operation are defined in (7) and (8), respectively.

$$C(x,y) = (B(x,y) \oplus M_C(i,j)) \Theta \ M_C(i,j). \quad \textbf{(5)}$$

$$M_C = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}. \quad \textbf{(6)}$$

$$A \oplus B = \{z|(B)_z \cap A \neq \emptyset\}. \quad \textbf{(7)}$$

$$A \Theta \ B = \{z|(B)_z \cap A^c \neq \emptyset\}. \quad \textbf{(8)}$$

Step 5. According to (9), if any pixel value in the critical image C is non-zero, which means that there exists a moving target in C, C is judged as potential evidence, $P = 1$; otherwise, it is determined as non-potential evidence, $P = 0$. Once $P = 1$ occurs, the target C is carried to aggregation for further custody.

$$P = \begin{cases} 1, \exists C(x,y) \neq 0, \\ 0, \text{ otherwise.} \end{cases} \quad \textbf{(9)}$$

3.2 Aggregation Phase

Suppose that Figure 5 has six surveillance cameras and three rounds for example. A directed ring is formed from S_1 to S_6 along the arrow direction to run the strategy. A round includes three actions: start, aggregation, and end, as shown in the columns. Time is indicated by the color, and one color represents one second. The table with the same color represents the same time. For the third second, said the yellow block, round one and round two stay in aggregation phase, and the round three is in start section.

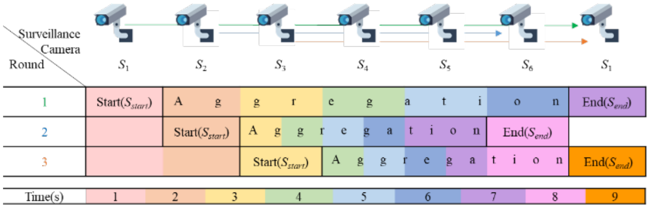


Figure 5. The scenario of pipeline and ring strategy

Take the first round for illustration, the first camera generating critical evidence, said S_1, is defined as S_{start}. After it transmits data to S_2, the strategy entering into aggregation. And a batch file is generated by S_2 to aggregate evidences of S_1. Once a critical evidence has been laid out by S_2, the latest evidence has been added into the batch file and delivered to S_3, and so on until it is passed to the final camera S_{end}. Note that all the cameras could be the beginning node to independently launch the aggregation ring based on the concept of pipeline strategy, and two thresholds, T and TL, are designed to prevent endless waiting time. For example, T sets six seconds and TL sets two seconds in Figure 5. At the second second, S_2 not only aggregates the data of the first round, but also starts the second round at the same time. In addition, in the second round, starting from S_{start} to aggregate data from different monitors to S_{end} in every two seconds, until the time of aggregation reaches the T threshold of six seconds, and so on for the third round.

Step 1. Data aggregation

(1) While S_i generating a critical frame F_i:

S_i applies SK_i to compute $ESK_i(F_i)$ and checks if there exists a batch file bf. If it is positive, the new frame is concatenated to the bf; otherwise, F_i is transmitted to S_{i+1}.

(2) While S_{i+1} receiving $ESK_i(F_i)$:

S_{i+1} checks if there exists a batch file bf. If it is positive, the frame is concatenated to the bf; otherwise, S_{i+1} generates a new bf to record the frame based on (10) and sets S_i as a S_{start} to be the beginning node of a new round. Before generating a new frame by itself, S_{i+1} keeps appending the received data to the bf according to (11).

$$bf = ESK_{start}(F_{start}) \quad . \quad \textbf{(10)}$$

$$bf = (ESK_{start}(F_{start}) \ || \ ESK_i(F_i')). \quad \textbf{(11)}$$

(3) While S_i receiving a batch file bf:

S_i checks if the round time has reached T. If yes, BPCS is switched to recording phase. Otherwise, S_i keeps aggregating frames. In case that the batch file has been occupied at the node for more than TL, S_i packages and sends the current file including an empty record to S_{i+1} based on (12).

$$bf = (ESK_{start}(F_{start})|| \ldots || \ ESK_{i-1}(F_{i-1})|| \ ESK_i(\ )). \quad \textbf{(12)}$$

Step 2. Termination conditions

Termination criteria in BPCS include the number of batch file relay and the total delivery time. The number of a bf relay is limited to the total number of surveillance cameras n, while the total delivery time is bound to a predefined time threshold T. If one of the two conditions holds, t_{start} and t_{end} are recorded in the bf to complete the aggregation according to (13).

$$(ESK_{start}(F_{start})||ESK_1(F_1)|| \ldots ||t_{start}||t_{end}). \quad \textbf{(13)}$$

3.3 Recording Phase

When one of the termination conditions happens to a surveillance camera, it is set to be the S_{end} of this round. Later on, S_{end} randomly chooses another surveillance camera S_i to backup the data. It further computes and uploads the hash value of bf to the blockchain.

Step 1. S_i computes $h(bf)$ based on (14)

$$h(bf) = Hash(ESK_{start}(F_{start})||ESK_1(F_1)|| \ldots ||t_{start}||t_{end}) \ . \quad \textbf{(14)}$$

Step 2. S_i packages and uploads t_{start}, t_{end}, $h(bf)$, and the file name to the blockchain.

3.4 Verification Phase

Once the integrity of video suffers from a question, an investigator can perform the following to verify and restore the video data.

Step 1. The investigator access all frames stored on the target S_i according to the incident time. Note that the integrity of critical frames during the period is the verification target.

Step 2. The investigator applies t_{start} and t_{end} to figure out the block to obtain $h(bf)$.

Step 3. The investigator captures the file name from the block to ask the backup of *bf* from other nodes. After receiving the backup data, the investigator computes the corresponding hash value and compares it with the one stored in the block. If they are the same, the received batch file is perfect to carry on the next step. The opposite means that the file has been polluted.

Step 4. The investigator employs PK_i to extract F_i from $ESK_i(F_i)$ and compares the result with that kept in S_i. If they are equal, F_i is complete. Otherwise, the data of S_i has been polluted. Here, F_i could be recovered according to the backup data passing above step examination.

4 Results and Analysis

Property achievements of related works and BPCS are compared in subsection 4.1, including integrity, confidentiality, availability, scalability, and storage overhead. The storage overhead simulation is examined in subsection 4.2, while the performance discussion of BPCS is explained in subsection 4.3. In the following, experiments under one-hour monitor based on 720P resolution are completed to highlight the contribution of BPCS. The proposed scheme was implemented in Python with a personal computer running Windows 10 64-bit. It is equipped with an Intel Core i7-10510U 2.3-GHz with 8G RAM.

4.1 Property Achievements of BPCS

Achievements of different protection methods are shown in Table 2. In a traditional architecture, the content of the monitor image is only stored without the protection of evidence credibility. Once people are suspicious of the surveillance camera security, the integrity and credibility of the recorded images cannot be trusted anymore. As to a blockchain-based framework, the image credibility can be confirmed definitely. Nevertheless, the transparency and storage overhead have led to the potential risk of confidentiality and high maintenance cost. Compared with above-mentioned works, BPCS relies on the blockchain architecture to possess the advantages of integrity and credibility confirmation. Specifically, CFD has been used to lower down storage overhead of the full video to achieve availability. The symbol “Weak” listed in Table 2 means that the property cannot be firmly confirmed, while “Robust” denotes that it can be ensured definitely.

Table 2. Comparisons of property achievement

Methods Achievements	Traditional	Blockchain	BPCS
Integrity	Weak	**Robust**	**Robust**
Confidentiality	**Robust**	Weak	**Robust**
Availability	Weak	**Robust**	**Robust**
Scalability	**Robust**	Weak	**Robust**
Low storage overhead	**Robust**	Weak	**Robust**

- Integrity

The property of integrity is to guarantee that no one is able to tamper the evidence data. In a traditional architecture, the monitor video is stored in database equipment without the assistance of other devices. In case that the surveillance or storage device suffer from hackings, a slice of intrusion vestige must cause the challenge of evidence credibility. No doubt that the integrity is hard to be ensured in traditional methods. On the other hand, this property can be firmly confirmed in a blockchain-based method and BPCS. It is due to the fact that both of them have inherited the non-tampering characteristics from blockchain technique. Taking a deep insight into BPCS, recorded data could be divided into off-chain and on-chain types. The off-chain data focus on the preservation of potential evidence, while the on-chain data concentrate on the integrity of evidence. Regarding the preservation of evidence, the aggregation ring based on the pipeline strategy has been adopted to lay out multiple $ESK_i(F_i)$ to reach the target in subsection 3.2. As to the integrity guarantee, all the aggregated data are hashed and uploaded to the blockchain network. A successful modification behavior shall depend on the assumption that a malicious user is able to tamper with more than 51% of the data on the whole blockchain network, which is regarded as an infeasible task.

- Confidentiality

The property of confidentiality is to ensure that no one is able to learn the video content without delegation. Since the distributed storage is adopted in blockchain architecture, all the nodes can read the data content. But in fact, the surveillance video contains lots of private information. The lack of a well-protected auxiliary may cause the disclosure of confidentiality. As to the confidentiality consideration in BPCS, the recorded data uploading to the chain have to be input into the one-way hash function to obtain an average hash value in the aggregation phase of subsection 3.2. Although the data on the blockchain are public and transparent to all, it is computationally infeasible to recover the original image via the hash value according to the security assumption of one-way hash function [28]. Therefore, the confidentiality can be definitely ensured in BPCS. Regarding the confidentiality in a traditional architecture, a trusted centralization node is assumed to secure the video management. Thus, the confidentiality is also confirmed in the traditional method.

- Availability

The property of availability is to guarantee the credibility even when the video content has been challenged owing to the intrusion suspicion of surveillance camera. Traditional cctv data storage adopts single-point storage mode. As the video content has been questioned somehow, the central node in the traditional architecture cannot prove that it has not been contaminated neither. That is, the property is hard to be ensured in a traditional centralized architecture. Therefore, the availability of its evidence validity is questionable. Concerning to the decentralized architecture, including the blockchain-based method and BPCS, a single node video challenging does not matter much in credibility. The suspicious data content can be certified and corrected according to the help of distributed nodes. Thus, the availability can be preserved definitely in these two methods.

- Scalability

Scalability refers to the ability of a framework to meet increasing storage demands effectively. In blockchain architecture, all users are required to maintain the same data. Over time, the amount of data stored by all users becomes difficult to estimate, and the mining profitability decreases, leading to discouragement among miners to continue working on the blockchain platform. This situation categorizes the scalability as "Weak."

As to BCPS is described in chapter 3. The CFD seamlessly address the challenge of storage burden. Thus, the method significantly reduces the high cost of traditional blockchain based on the analytical result of subsections 4.2. Consequently, the proposed method definitely solves the problem of disintegration of the traditional blockchain when the contribution of the participants in the chain is not proportional to the profit; thus, fulfilling the scalability requirement.

- Low storage overhead

This characteristic is to ensure that only a lightweight storage cost is required in recording the evidence. In a centralized method, a record copy is kept for future investigation. Namely, it achieves the low storage overhead. Considering a blockchain-based method, each node has to maintain a ledger containing a full copy of surveillance video. As all blockchain nodes have to spend a large scale of storage space for evidence credibility, the property of lightweight storage overhead comes to grief. Regarding BPCS in this field, CFD is developed to tell potential critical evidence images from surveillance video. The fact is that most of images in a 24-hour video are meaningless, while CFD can be applied to filter those non-potential images to lower down the storage overhead. The details of storage examination are explained in subsection 4.2. Additionally, the retrieved potential images are compressed through an average hash operation in BPCS. Aside from confidentiality, the storage overhead can be further decreased to comply with the characteristic of low storage overhead.

4.2 Storage Overhead Simulation

To highlight the contribution, we examine and compare the storage overhead between blockchain-based method and BPCS. The storage space for a one-hour surveillance video is 6,338.56MB. It is impractical for all blockchain nodes to spend such a huge amount of space. For a 24-hour continuous surveillance video, each node has to take 148.56GB for chain maintenance. Even the video could be compressed via an average hash operation before uploading to the chain, a one-hour storage cost can be decreased to 140.67MB. The amount of data size is reduced by about 45 times. Nevertheless, most of images in a video is meaningless and unrelated to the evidence credibility. BPCS follows this regulation to find out the potential critical images by the help of CFD and further reduces the space overhead.

For a one-hour monitoring, the ratio of potential evidence located in video is set to 20%, 40%, …, 100%. A blockchain-based method and BPCS are used to examine the overhead for recording these potential evidences. As illustrated in Figure 6, it requires 28.14MB for BPCS to store potential evidences under the scenario of 20%. It is only one-fifth of the blockchain-based method, while the main reasons include the contribution of CFD in telling potential critical images and the compression of average hash operation. In addition, it is easy to observe the fact that CFD is able to distinguish potential critical images and filter the meaningless ones no matter how many evidence ratios we increase. These examination outcomes have demonstrated the contribution that BPCS can efficiently integrate the blockchain concept and CFD to secure the evidence credibility with a lightweight storage overhead.

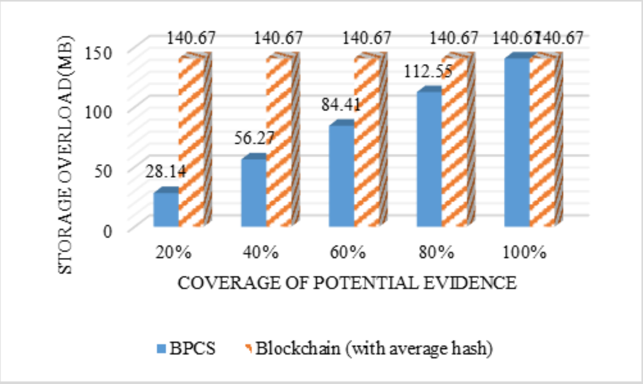


Figure 6. Storage overhead under different ratios of potential evidence

4.3 Performance Discussions

To lower down the risk of data pollution and guarantee the efficiency of BPCS, the batch file data shall not be occupied in a single node for a long time. In the following, the average execution time of BPCS under one hundred examinations is used to help determine the settings of *TL* and *T*. For a single monitor, it takes 20.575ms in average to obtain a critical evidence frame, as shown in subsection 3.1. A signature verification requiring 0.0004ms is then performed to confirm the source correctness of the batch file. After that, the monitor has to spend 47.9297ms to execute a signing procedure for aggregated data, followed by a 0.0013ms concatenation operation. To sum up, it averagely costs 68.5047ms for the beginning monitor to complete an aggregation of critical frame, while it takes 68.5064ms for other nodes. Figure 7 has displayed the execution time of BPCS under different numbers of monitors.

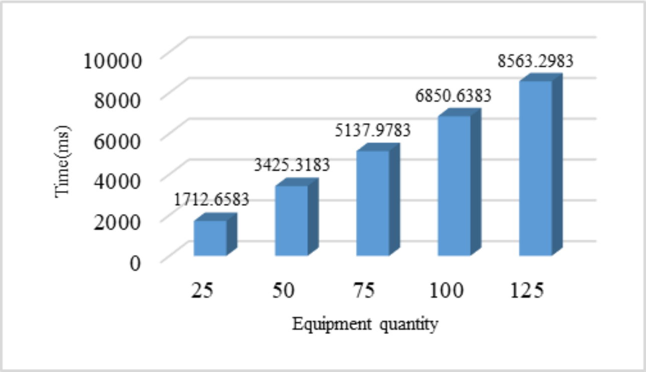


Figure 7. Execution time

Considering the minimum execution time of evidence frame generation and aggregation, which is 68.5064ms in average, TL is set to be 90ms. As to the determination of T, two main factors have to be taken into consideration, including the single node execution time and the buffering time. In case of 25 surveillance cameras, the minimum execution time without buffering is 1712.6583ms, while the maximum execution time concerning all factors takes 68.5047+(25-1)x(90)ms = 2228.5047ms. To achieve a satisfactory trade-off between block overhead and BPCS efficiency, the mean value of the two execution periods is determined to be the T = 1970.5815ms. Accordingly, the setting of T = 9895.9015ms is obtained in the case of 125 surveillance cameras

5 Conclusions

In this article, the blockchain concept and a developed CFD technique are integrated to realize a critical evidence custody system. The CFD can be used to lower down the storage overhead of surveillance camera, while the tamper-free achievement can be confirmed based on the blockchain adoption. In particular, simulations have demonstrated that the pipeline and ring strategy of BPCS can reduce the block consumption on the blockchain network and guarantee the efficiency simultaneously.

References

[1] E. L. Piza, B. C. Welsh, D. P. Farrington, A. L. Thomas, CCTV Surveillance for Crime Prevention: A 40-Year Systematic Review with Meta-Analysis, *Criminology & Public Policy*, Vol. 18, No. 1, pp. 135-159, February, 2019. https://doi.org/10.1111/1745-9133.12419

[2] M. P. J. Ashby, The Value of CCTV Surveillance Cameras as an Investigative Tool: An Empirical Analysis, *European Journal on Criminal Policy and Research*, Vol. 23, No. 3, pp. 441-459, September, 2017. https://doi.org/10.1007/s10610-017-9341-6

[3] F. Brookmamn, H. Jones, Capturing Killers: The Construction of CCTV Evidence during Homicide Investigations, *Policing and Society*, Vol. 32, No. 2, pp. 125-144, 2022. https://doi.org/10.1080/10439463.2021.1879075

[4] P. Bischoff, Surveillance Camera Statistics: Which Cities Have the Most CCTV Cameras?, *Comparitech*, Jul. 2022.

[5] J. Cropley, Top Video Surveillance Trends for 2017, *IHS Markit*, 2017.

[6] T. He, R. M. Aronce, L. Dampanaboina, J. Jose, M. King, E. Cohen, SonicWALL Cyber Threat Report, *SonicWALL*, 2021.

[7] ISO/IEC 27037:2012 Information Technology-Security Techniques-Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence, *International Organization for Standardization*, October, 2012.

[8] S. Higgins, Vermont is Close to Passing a Law That Would Make Blockchain Records Admissible in Court, *Coindesk*, May, 2016.

[9] The French National Assembly Says Proofs on Blockchain are Admissible in Court, *ReCheck*, January, 2020.

[10] W. Zhao, China's Supreme Court Recognizes Blockchain Evidence as Legally Binding, *CoinDesk*, September, 2018.

[11] S. Seth, UK Courts Start Pilot Blockchain Evidence System, *Investopedia*, August, 2018.

[12] D. Berdik, S. Otoum, N. Schmidt, D. Porter, Y. Jararweh, A Survey on Blockchain for Information Systems Management and Security, *Information Processing & Management*, Vol. 58, No. 1, Article No. 102397, January, 2021. https://doi.org/10.1016/j.ipm.2020.102397

[13] W. Liang, Y. Fan, K. C. Li, D. Zhang, J. L. Gaudiot, Secure Data Storage and Recovery in Industrial Blockchain Network Environments, *IEEE Transactions on Industrial Informatics*, Vol. 16, No. 10, pp. 6543-6552, October, 2020. DOI: 10.1109/TII.2020.2966069

[14] N. Z. Benisi, M. Aminian, B. Javadi, Blockchain-based Decentralized Storage Networks: A Survey, *Journal of Network and Computer Applications*, Vol. 162, Article No. 102656, July, 2020. https://doi.org/10.1016/j.jnca.2020.102656

[15] H. Shafagh, L. Burkhalter, A. Hithnawi, S. Duquennoy, Towards Blockchain-based Auditable Storage and Sharing of IoT Data, *Proceedings of the 2017 on Cloud Computing Security Workshop*, pp. 45-50, November, 2017. https://doi.org/10.1145/3140649.3140656

[16] Q. Chen, G. Srivastava, R. M. Parizi, M. Aloqaily, I. A. Ridhawi, An Incentive-aware Blockchain-based Solution for Internet of Fake Media Things, *Information Processing & Management*, Vol. 57, No. 6, Article No. 102370, November, 2020. https://doi.org/10.1016/j.ipm.2020.102370

[17] L. Liu, W. H. Zhang, C. Q. Han, A Survey for The Application of Blockchain Technology in The Media, *Peer-to-Peer Networking and Applications*, Vol. 14, No. 5, pp. 3143-3165, September, 2021. https://doi.org/10.1007/s12083-021-01168-5

[18] Y. F. Chang, Research on De-Motion Blur Image Processing based on Deep Learning, *Journal of Visual Communication and Image Representation*, Vol. 60, pp. 371-379, April, 2019. https://doi.org/10.1016/

j.jvcir.2019.02.030

[19] I. Lissner, J. Preiss, P. Urban, M. S. Lichtenauer, P. Zolliker, Image-Difference Prediction: From Grayscale to Color, *IEEE Transactions on Image Processing*, Vol. 22, No. 2, pp. 435-446, February, 2013. DOI: 10.1109/TIP.2012.2216279

[20] F. Y. Li, L. M. Zhang, W. M. Wei, Reversible Data Hiding in Encrypted Binary Image with Shared Pixel Prediction and Halving Compression, *EURASIP Journal on Image and Video Processing*, Vol. 2020, Article No. 33, August, 2020. https://doi.org/10.1186/s13640-020-00522-6

[21] R. Mondal, M. S. Dey, B. Chanda, Image Restoration by Learning Morphological Opening-Closing Network, *Mathematical Morphology-Theory and Applications*, Vol. 4, No. 1, pp. 87-107, January, 2020. https://doi.org/10.1515/mathm-2020-0103

[22] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, October, 2008.

[23] K. Fanning, D. P. Centers, Blockchain and Its Coming Impact on Financial Services, *Journal of Corporate Accounting & Finance*, Vol. 27, No. 5, pp. 53-57, July/August, 2016. https://doi.org/10.1002/jcaf.22179

[24] J. W. Leng, G. L. Ruan, P. Y. Jiang, K. L. Xu, Q. Liu, X. L. Zhou, C. Liu, Blockchain-empowered Sustainable Manufacturing and Product Lifecycle Management in Industry 4.0: A Survey, *Renewable and Sustainable Energy Reviews*, Vol. 132, Article No. 110112, October, 2020. https://doi.org/10.1016/j.rser.2020.110112

[25] M. Mettler, Blockchain Technology in Healthcare: The Revolution Starts Here, *2016 IEEE 18th International Conference on E-health Networking, Applications and Services*, Munich, Germany, 2016, pp. 1-3. DOI: 10.1109/HealthCom.2016.7749510

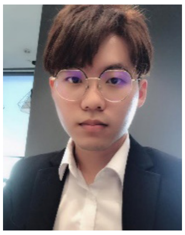
[26] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, A. Faxvaag, Blockchain in Healthcare and Health Sciences-A Scoping Review, *International Journal of Medical Informatics*, Vol. 134, Article No. 104040, February, 2020. https://doi.org/10.1016/j.ijmedinf.2019.104040

[27] S. Y. Huh, S. G. Cho, S. H. Kim, Managing IoT Devices using Blockchain Platform, *2017 19th International Conference on Advanced Communication Technology*, Pyeong Chang, Korea (South), 2017, pp. 19-22. DOI: 10.23919/ICACT.2017.7890132

[28] R. C. Merkle, One Way Hash Functions and DES, *Conference on the Theory and Application of Cryptology*, Santa Barbara, California, USA, 1989, pp. 428-446. https://doi.org/10.1007/0-387-34805-0_40

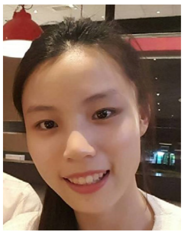
Biographies

Yun-Yi Fan is pursuing her PhD degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan. Her current research interests include image processing and blockchain applications.

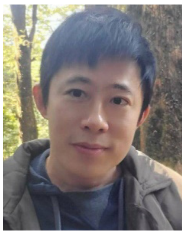


Chit-Jie Chew is pursuing his PhD degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan. His current research interests include information security and blockchain applications.

Wei-Che Hung has received his MS degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan in 2022. His current research interests include network security and image processing.



Ying-Chin Chen is pursuing her PhD degree in information engineering and computer science in Feng Chia University, Taichung, Taiwan. Her current research interests include information security and visual secret sharing.



Jung-San Lee received his Ph.D. degree in computer science and information engineering in 2008 from National Chung Cheng University, Chiayi, Taiwan. Since 2017, he has worked as a professor in the Department of Information Engineering and Computer Science at Feng Chia University, Taichung, Taiwan. His current research interests include network management, electronic commerce, and blockchain.