Secure and Privacy-Preserving Stored Surveillance Video Sharing atop Permissioned Blockchain

Alem Fitwi, Yu Chen

Dept. of Electrical and Computer Engineering, Binghamton University, Binghamton, NY 13902, USA

Emails: {afitwi1, ychen}@binghamton.edu

Abstract—At present, more than a billion closed-circuit television (CCTV) cameras are watching the world. These cameras garner a lot of visual information that is often processed and stored in remote and centralized cloud servers. Multiple occasions have revealed that this traditional approach is plagued with security and privacy breaches. The breaches could be the interception of raw videos while in transit to distant surveillance analytics centers (SAC), infiltration to cameras and network video records (NVR), or abuse of cameras and stored videos. Hence, the traditional video surveillance system (VSS) cannot guarantee the protection of the privacy of individuals caught on CCTV cameras. Therefore, this paper proposes a Secure and Privacy-preserving Stored surveillance video sharing (SePriS) mechanism for authorized users/nodes based on blockchain (BC), smart contracts, and the enciphering of video frames using DAB, a mechanism developed based on discrete cosine transform (DCT), advanced encryption standard (AES), and a block shuffling (BS) algorithm. The BC-based solution creates an environment auspicious for creating decentralized, reliable SACs and storage sites with secure and privacy-aware sharing of stored surveillance videos across SAC nodes and by law enforcers, police departments, and courts securely connected to the SAC nodes. The experiments and analyses validate that the proposed BC-based SePriS solution achieves the design purpose.

Keywords-Permissioned Blockchain, Video Privacy & Security, Discrete Cosine Transform (DCT), AES, Enciphering.

I. INTRODUCTION

To ensure public safety and physical security, the number of closed circuit television (CCTV) cameras deployed in urban and suburban areas have been increasing quickly over the past decade. As projected by many experts and indicated in recent reports, more than a billion of CCTV cameras are watching the world today [15]. These cameras enable the law enforcers and security personnel to collect tremendous amount of information about individuals without their knowledge and consent while moving along many public and private places. The pros of video surveillance systems (VSS) might outweigh the cons; however, there are two valid arguments raised by two antagonistic groups. On one hand, there are people who advocate the widespread deployment and use of VSS because it helps increase public safety and residents' security, and reduce crime rates. On the other hand, there are a number of people who argue against the practice of VSS in public places because they strongly believe that it could be abused so easily [10].

CCTV cameras have become commonplace around the world where individuals are observed numerous times a day without their consent and knowledge. There are a myriad of reports that substantiate the fear of abuse of CCTV cameras. The German Chancellor, Angela Merkel, was spied while at her apartment by abusing a museum security CCTV camera [2]. Quite recently, on March 9, 2021, a group of hackers claimed to have hacked the security CCTV camera data from Verkada and gained access to the live feeds as well as central storage of 150,000 surveillance CCTV cameras deployed in a number of companies and hospitals [7].

In general, privacy breaches are mainly attributed to the interception of raw video streams that contain visual information about individuals by adversaries/intruders and abuse of videos by people in charge of the surveillance. The abuse of the surveillance system include collecting unauthorized data about individuals by maneuvering the cameras, accessing and leaking collected data or threatening to do so, and blackmailing individuals caught on cameras [20], [26]. Our previous work focused on privacy-sensitive attributes detection and ensuring end-to-end (E2E) privacy [8], [11], [12]. However, all of the aforementioned problems cannot be addressed by introducing good privacy-attributes detection and scrambling schemes alone. The addition of an effective access management is vital to ensure privacy. Stored videos must be accessed with clear authentication, authorization, and accounting policies in place.

A permissioned, private blockchain (PBC) network is envisioned in this work to alleviate the privacy and security problems vis-à-vis access to surveillance videos processed and stored in distributed surveillance analytics centers (SAC) and storage sites, respectively. It employs privacy-preserving video-frame encrypting mechanisms and smart contracts that define privileges and access rules. PBC allows only authorized users to access the videos without violating the privacy of individuals. The existing smart contracts, however, do not preserve the privacy and confidentiality of data when shared to the BC nodes. In our proposal, the smart contract is tailored for better handling of the privacy and confidentiality issues. Users who try to access the stored videos need to prove themselves to the blockchain that they have the required privileges. Besides, correctness of the references are validated by every other node so that only authorized accesses are made and the integrity of the video storage is verifiable. The reference in this paper points to a variable on a mapping table that contains actual references to the videos. On top of that, the video frames are exchanged in scrambled form to prevent spilling of personal information by interception attacks.

To prevent the abuse of stored surveillance videos,

we proposed and experimentally validated a Secure and Privacy-preserving Stored surveillance videos sharing (SePriS) mechanism, a PBC-based solution along with an efficient video-frame scrambling mechanism. Our major contributions are briefly outlined as follows:

- Design of PBC-based video surveillance system that ensures secure and private exchange of stored video frames to prevent leaking and blackmailing of individuals caught on CCTV cameras. SePriS ensures that videos are accessed only in an authenticated, authorized, and accountable way.
- A video-frame enciphering mechanism named DAB is introduced based on discrete cosine transforms (DCT), advanced data encryption standard (AES), and a block shuffling (BS) algorithm to ensure secure exchange of video streams off-BC storage sites and users.
- Extensive experimental study and security analyses substantiate the validity and applicability of the proposed SePriS architecture, mechanisms, and techniques.

The remainder of this paper is organized as ensues: the related work is briefly discussed in Section II. The overall system architecture of SePriS is then introduced in Section III. In Section IV, the blockchain based solutions are formulated followed by the description of DAB, the DCT-AES-BS based video-frame enciphering scheme in Section V. The analysis and discussion of the proposed SePriS scheme are presented in Section VI. Eventually, the conclusions are presented in Section VII.

II. RELATED WORK

A. Video Surveillance Systems and Privacy

Today, more than a billion of CCTV cameras are pervasively deployed around the world in urban areas by governments, companies, and individuals with the main goals of ensuring physical security and public safety. In places like Beijing, London, and New York, an individual is estimated to be caught on CCTV cameras hundreds of times a day [9], [12], [26], [30]. Consequently, a tremendous amount of information about individuals is garnered without their knowledge and consent. This huge data containing privacy-sensitive visual information could be divulged into the wider cyber space where there are almost 4.57 billion active Internet users as of July 2020 that accounts 59% of the global population [4]. The spill of the information is often attributed to interception attacks and abuse of cameras and stored videos for blackmailing, cyber stalking, or extorting. This poses a great risk of breaches and invasions of the privacy of individuals caught on CCTV cameras. The best way to create a video surveillance system that protects the privacy of individuals amid the increased proliferation of CCTV cameras is requiring the camera manufactures to incorporate privacy-preserving methods by design and recommend secure deployment networks [1], [3], [25].

Many incidences have been reported in relation to privacy breaches and CCTV camera approaches. About a quarter of century ago, in August 1995, numerous peeping incidences or voyeurism to observe or record people doing private stuffs at their homes were reported [13]. Unfortunately, those bad practices and abuses did not stop there; rather they have continued in a more sophisticated way. Even government officials' apartments were spied by abusing and directing CCTV cameras via windows [2]. The American Civil Liberties Union (ACLU) have identified and reported multifaceted CCTV camera abuses including criminal abuse, institutional abuse, abuse for personal purposes, discriminatory targeting, and voyeurism [23].

Generally, the public has been repeatedly informed that surveillance cameras are never abused by authorized people in charge of them. Hence, many a person might believe that people who sit in the surveillance operation centers (SOC) can supposedly be trusted not to abuse these CCTV cameras at their disposal, which boost their sighting capability drastically, to engage in despicable or outright illegal behavior. Nonetheless, this understanding has been proven to be glaringly false as the report of literally multiple incidences clearly indicate [18]. A number of protests against the use of CCTV cameras were conducted in the best, where a list of many such protests against surveillance cameras are provided in reports citing the abuses and the ineffectiveness of video surveillance as a "crime-fighting" tool [17]. Even today, CCTV cameras are not secure and they greatly risk the privacy of many individuals.

B. Blockchain Technology

About a decade ago, the Bitcoin has substantiated how the BC technology can enable decentralize trusted computing models [16]. The BC technology as a whole was made popular by the success of Bitcoin. Now it can be employed to make trustworthy and secure transactions across untrusted networks without relying on a trusted centralized third party. The BC is a kind of chronological sequence of blocks including a list of complete and valid transaction records. The blocks that constitute the BC blocks are chained to one another by a hash value, where the block preceding a given block is called its parent block, and the first block is known as the genesis block. Each block comprises a block header and a block body. The block header contains the block version, previous block hash, timestamp, 4-byte nonce, body root hash, and target hash. The block body consists of validated transactions within a specific time period. These features enable the BC technology to have the potential to decentralize many applications that depend on a centralized trusted body.

Moreover, a light-weight blockchain along with the concept of identity-based distributed data possession in multi-cloud storage can be leveraged to ensure privacy and authorized access in many smart applications; additional works are required, though [14], [27], [28]. However, due to concerns on privacy and performance issues, a public blockchain is not an ideal candidate. Instead, a private blockchain has been considered where only authenticated member nodes join [6], [31]. Therefore, a lightweight, closed-group blockchain that supports decentralized applications like surveillance that entails high speed and privacy could meet the requirements [29]. The main issue is speed. Video surveillance is a real-time process but the BC does not allow this yet. As a result, the

BC technology is employed in SePriS mechanism to manage accesses to videos stored in many distributed sites.

C. Video Frame Scrambling Mechanisms

There are a multitude of schemes like *editing, face regions, false color, and JPEG* [21] that can be employed to scramble or mask video frames. However, scrambling/encryption scheme is the only feasible option in the eyes of security/privacy and usability. It securely hides sensitive information on video frames and prevents unauthorized accesses. All other schemes are not able to meet the stringent requirements of video-contents privacy protection as they fail to achieve an optimal balance between privacy, clarity, reversibility, security, and robustness.

Most of the preexisting encryption mechanisms are not suitable for enciphering video frames due to their bulky nature. Public-key cryptographic schemes like Rivest-Shamir-Adleman (RSA) and Elliptical Curve Cryptography (ECC) are too slow to be used for image scrambling due to their heavy reliance on hard factoring, a compute-intensive process. The conventional encryption mechanisms like Rivest Cipher 4 (RC4) and Advanced Data Encryption (AES) are not suitable for video encryption, either. AES is one of the most secure encryption scheme employed in the transport layer security (TLS) in the TCP/IP Network Architecture. It, nonetheless, has some issues with video/image scrambling like inability in breaking the strong correlation amongst adjust pixels. Chaotic schemes are said to be the best mechanisms for video scrambling due to their high randomness, sensitivity to slight change, and ability to be vectorized. Their shortcoming is the fact that they use XOR operator for mixing the chaos and plain image; hence, a separate key for every frame is required to meet perfect secrecy. In this paper, we proposed DAB, a video encryption mechanism that employs DCT, AES, and block shuffling to reduce the number of keys employed in chaotic schemes, and to improve the correlation problems observed in AES ciphers when used for image encryption.

III. SEPRIS SYSTEM ARCHITECTURE

It is feasible to use BC technology to address the problems in distributed access to stored surveillance videos. It enables the construction of a privacy-aware smart surveillance system by integrating the advanced features of BC and smart contracts that define how security, privacy, integrity, authentication, authorization, controllability, auditability, and accountability can be achieved. Our SePriS system comprises three major parts, namely off-BC distributed video storage sites, BC nodes connected to SACs, and users. The off-BC storage refers to secure cloud/fog based storage system for the storage of surveillance videos connected to the BC nodes. The BC network ensures authenticity. Users are assigned with different levels of access privileges to the videos, which are defined in the smart contracts. Users could be security personnel working in SOCs, law enforcers, police department, or courts.

Figure 1 portrays the high-level overview of the proposed SePriS system, where smart cameras function as edge devices.

Authorized users and off-BC storage connected to the BC-nodes through a local area network (LAN) or a wide area network (WAN). Fine-grained access control policies and privileges are set as part of the privacy policies. They can be legitimately updated or revoked at any time with authorization. References to access histories of stored or viewed videos are logged and posted onto the BC based on the details defined in smart contracts. Viewer's identity, access time, privileges, and references of accessed parts are also logged and stored. To discourage leaking of videos or images, information specific to the viewers, like fingerprint, is appended into the log-reference of every watched video and shared with all BC-nodes. The details are presented in Section IV.

Here two type of cryptographic schemes are employed to ensure secure and privacy-conscious exchange of messages and video frames. A digital signature is embedded in the request for access to stored videos or messages sent to any of the BC-nodes by any of the users. For this purpose, an elliptic curve public encryption/decryption (ECPED) is employed. Following identity and security authentication, consensus by the BC-nodes, and the successful granting of access-code, access to videos is granted to the requestor on the off-BC storage site in scrambled form to ensure end-to-end (E2E) privacy. The scrambling is performed by DAB scheme described in Section V.

IV. PERMISSIONED BLOCKCHAIN BASED SECURE ACCESS

In SePriS system, a PBC-based solution is introduced for secure and privacy-aware sharing of stored surveillance videos across different SACs and authorized users. Each of the SAC node backups the BC copy synchronously. The data stored in the BC comprises only access requests, users information, access control list, references to accessed videos associated with the identity information of the user who was granted access, and other activities performed on the video. The actual video frames are stored on distributed off-BC storage clouds as depicted in Fig. 1.

Figure 2 illustrates how stored surveillance videos are securely accessed by authorized users using the PBC-based approach. Primarily, the police department, courts, and other law enforcers are the users of stored surveillance videos for investigative and forensic purposes, or as evidence against criminals in courts of law. Here, in the interest of clear demonstration, we will consider how a court can access stored videos securely from an off-BC storage site. As indicated in Fig. 2, to access a video of specified date and range from an off-BC storage cloud, it takes ten steps executed by the requestor, BC nodes, and the off-BC storage. Each of the steps is briefly described in what ensues:

Step-1: The court first identifies itself to any of the BC-nodes (SAC_2 in this case) as portrayed in Fig. 2. That is, an identity and a security authentications are first performed. The identity authentication involves bio-metrics where the requestor scans any of their fingers whose processed copies are already in the BC-nodes. If the authentication process succeeds, the requestor receives a unique identifying ID (for instance UID = court322874352017640022980892363199962446587) locked
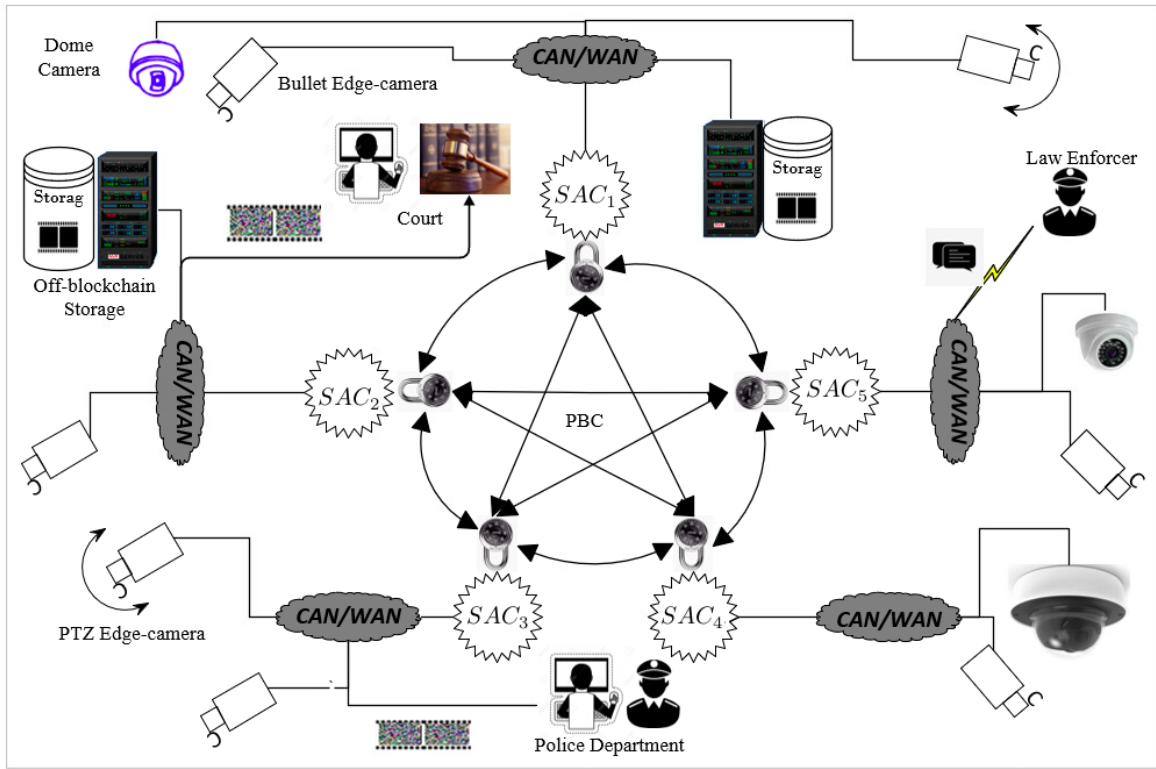
Fig. 1. PBC-based SePriS Architecture for secure and privacy-aware exchange of surveillance videos stored in distributed off-BC sites.
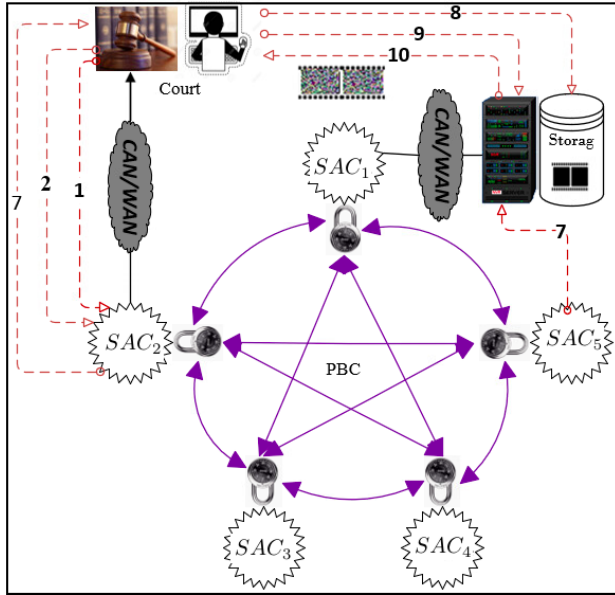

Fig. 2. The work-flow of the PBC-based Solution for secure and privacy-aware exchange of stored surveillance videos.

in a double lock-box as shown by Eq. 1, where E stands for an asymmetrical encryption, key_{pub-R} stands for the public key of the receiver (the court in this case), and key_{pri-S} stands for the private key of the sender (SAC_2 in this case). A copy of the UID is saved in the BC-nodes for later verification. The assumption is that the sender and receiver has each other's public keys. Then, the requestor proceeds to step-2.

$$cipher\_UID = E(key_{pub-R}, E(key_{pri-S}, UID)) \quad (1)$$

Step-2: A request for access to a specific video in the off-BC storage is forwarded to SAC_2 enclosed inside double lock-boxes, described by Eq.1. In other words, the sender initiates a transaction by sending a request signed by its private key and encrypted by receiving BC-node's public key. The request is easily verified by the receiving BC-node (SAC_2) using the sender's public key. Figure 3 shows a sample request that comprises the UID of a sender, ID(s) of the recording camera(s), Date of recording, range or time length of requested video, type that describes whether the sender wants the video with the whole context or specific behavioral activities identified using a machine learning or Deep learning model, and name and address of the off-BC storage site.

Step-3: The request is broadcasted by SAC_2 to all other BC-nodes through the P2P network as shown in Fig. 2.

Step-4: Each BC-node verifies the request in accordance with the predefined smart contract and database of legitimate users along with their access privileges, also called access control list (ACL).

Step-5: Reach consensus and pack the validated request chronologically. That is, if the request is valid, it is appended to the chain as a new block following the solving of the proof of work (PoW) puzzle by a miner.

```
{
    "requester_ID": "court3228743520176400229808923631999962446587",
    "Recording Camera ID": "65FrontStreet123",
    "Date of Recording": "March 09, 2021",
    "Range": "6:00AM to 23:59PM",
    "Type": "With Context",
    "Address of Off-BC Storage Site": "Name = CloudNVR2321, IP = x:x:x:x"
}
```

Fig. 3. A sample request made by court, in JSON file format, sent to a BC-node.

```
{
    "requester_ID": "court32287435201764002298089236319996244 6587",
    "Recording Camera ID": "65FrontStreet123",
    "Date of Recording": "March 09, 2021",
    "Range": "6:00AM to 23:59PM",
    "Type": "With Context",
    "Address of Off-BC Storage Site": "Name = CloudNVR2321, IP = x:x:x:x",
    "Access Code": "courtToCloudNVR232139869614605459"
}
```

Fig. 4. A sample request made by court, in JSON file format, an off-BC storage.

Step-6: Generate an access code for the requestor following consensus. $courtToCloudNVR232139869614605459$ is a sample access code generated for a court to access a video from the off-BC storage specified in the request.

Step-7: The generated $accesscode$ is forwarded to the court wrapped with the private and public keys of SAC_2 and the court, respectively. Likewise, the original request in JSON file format is updated with the access code and sent to the target off-BC storage site in double boxes locked with the private and public keys of SAC_5 and the off-BC storage, respectively.

Step-8: The requestor, court, performs an identity and a security authentication on the off-BC storage.

Step-9: Following a successful authentication, the requestor sends an updated request, shown in Fig. 4, which contains the access code provided by the BC members in addition to the contents of the original request sent to the nodes in Step-2. Just like the previous cases, this request as well is encrypted and signed by the private and public keys of the court agent and the off-BC storage, respectively.

Step-10: If the request sent by the court in Step-9 and the request sent to the off-BC storage by the BC-nodes match, access to the specified video is granted as illustrated in Fig. 2. Unlike the requests and short messages which are enciphered by using computationally expensive asymmetrical encryption mechanism, the video data cannot be encrypted using ECC for it contains bulky information. As a result, the video streams are encrypted using a DCT-AES-BS mechanism designed for this purpose and described in Section V. In parallel, log of activities and references to videos accessed associated with requestor identity and device information are sent to the BC. They are permanently and synchronously stored in the BC.

V. DAB: DCT-AES-BS BASED VIDEO FRAME ENCIPHERING

Asymmetrical encryption schemes like ECC and Rivest–Shamir–Adleman (RSA) are too slow to be employed for video encryption which contains bulky information. Rather they are used for enciphering short messages and creating digital signatures. As a result, DAB, a mechanism convenient for video enciphering is purposed in this section. It's meant for encrypting video frames accessed by authorized users from any of the off-BC storage sites shown in Fig. 1. Figure 5 presents the proposed DAB scheme that comprises four major modules, namely discrete cosine transom (DCT) calculator, quantizer, advanced encryption standard (AES), and a block shuffler (BS). They are briefly described in the following four subsections.
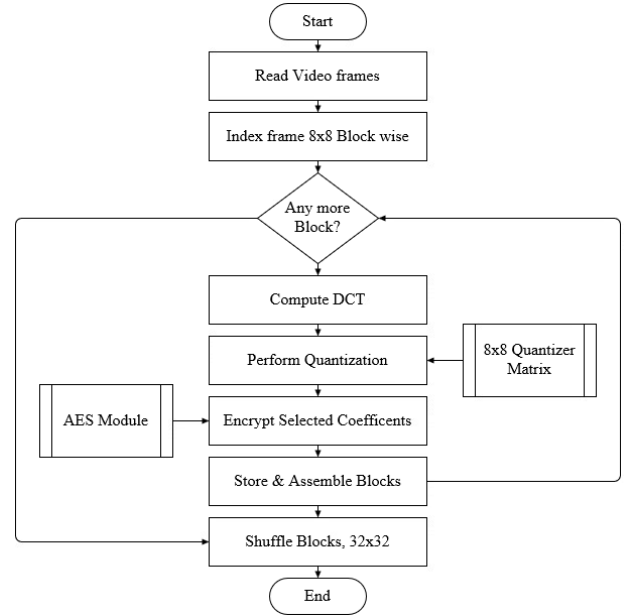

Fig. 5. Video Frame Enciphering Process Flows of DAB.

A. DCT

DCT is a well-known mathematical transformation technique that takes a signal and transforms it from spatial domain into frequency domain. Today, a number of digital image and video compression techniques employ a block-based DCT due to the fact that this technique reduces the amount of data needed to recreate a digitized image. In particular, JPEG and MPEG use the DCT to concentrate image information by removing spatial data redundancies in two-dimensional images [5]. In the process of the DCT, the input video frame is decomposed into 8×8 blocks and the DCT of every 8×8 block of video frame is computed by using Eq. 2. Technically speaking, these blocks are transformed from the spatial domain to the frequency domain representation by the DCT.

$$DCT = T \times M \times T' \qquad (2)$$

where M is an 8×8 block from an input frame, and T is an 8×8 DCT matrix computed by using the following equation,

$$T_{i,j} = \begin{cases} \frac{1}{N}, & \text{if } i = 0. \\ \sqrt{\frac{2}{N}} cos\left[\frac{(2j+1)i\pi}{2N}\right], & \text{if } i > 0. \end{cases} \qquad (3)$$

In the just-above equation, i & j are x and y indices whose values range from 0 to 7, inclusive.

B. Quantization

The 8×8 DCT coefficients are now ready for quantization. Each DCT coefficient is divided by its corresponding constant in a standard quantization matrix, where values are rounded down to the nearest integers. There is currently one standard employed for computing the quantization matrix that has been around for a while ever since JPEG was proposed by the Independent JPEG Group (IJG). It depends on the Quality factor (Q). The basic algorithm is as follows: first a quality

```
[[ 16,  11,  10,  16,  24,  40,  51,  61],
 [ 12,  12,  14,  19,  26,  58,  60,  55],
 [ 14,  13,  16,  24,  40,  57,  69,  56],
 [ 14,  17,  22,  29,  51,  87,  80,  62],
 [ 18,  22,  37,  56,  68, 109, 103,  77],
 [ 24,  35,  55,  64,  81, 104, 113,  92],
 [ 49,  64,  78,  87, 103, 121, 120, 101],
 [ 72,  92,  95,  98, 112, 100, 103,  99]]
```

Fig. 6.   IJG Base Quantization Matrix.

factor Q, which can assume a value from 1 to 100, is selected. 1 is a value of the "poorest" quality while 100 is the value of the "highest" quality. 50 is the default setting. The base IJG quantization matrix (bqm) based on which a desired quantization matrix is derived is provided in Fig. 6.

A quantization matrix with a certain level of quality, Q, is computed by using Algorithm 1. A parameter S is computed based on whether $Q < 50$ or $Q >= 50$ and is used as multiplier to the base quantization matrix to obtain the target quantization matrix.

Algorithm 1 Quantization Matrix

1: *Base Quantization Matrix, bqm* $\leftarrow$ Fig. 6
2: $Q \leftarrow$ Select values: 1 to 100
3: **if** $Q < 50$ **then**
4:      $S = \leftarrow 5000/Q$
5: **else**
6:      $S = \leftarrow 200\text{-}2*Q$
7: $qm = \leftarrow \frac{floor(S \times bqm + 50)}{100}$

C. AES

In each block, there are 64 DCT coefficients set up from the lowest frequency at the upper left corner to the highest frequencies at the lower right corner. The most important visual characteristics of the frame are placed in the low frequencies while the details are situated in the higher frequencies. The Human Visual System (HVS) is most sensitive to lower frequencies than to higher ones [19].

Therefore the AES, the most widely used symmetrical encryption scheme in today's Internet, is employed in this work to encipher selected coefficients of every DCT block. Only those coefficients on locations (indices) [0][0], [0][1], [0][2], [0][3], [1][0], [1][1], [1][2], [1][3], [2][0], [2][1], [2][2], [2][3], [3][0], [3][1], [3][2], and [3][3] with higher HVS sensitivity in every DCT block are encrypted using AES.

D. Block Shuffler

Once all values of the selected locations in every DCT block are encrypted using AES, the whole frame is shuffled by using a simple but secure shuffling algorithm purposed in this section. It further randomizes the outputs of AES in block of size 32×32. AES coupled with the shuffling algorithm described in Algorithm 2. Hence, two keys are employed here: one is AES encryption key, and the other is index_key used to recover shuffled blocks. Both are securely shared with the recipient using the ECC public key cryptographic method.

Algorithm 2 Block Shuffler

1: bs $\leftarrow$ blk_size
2: frame $\leftarrow$ vid.read(0)
3: W, H $\leftarrow$ frame.size
4: **procedure** SHUFFLE_FRAME(frame, bs, H, W)
5:      hw $\leftarrow$ x, y tuples of each 32x32 block
6:      $hws \leftarrow Yates - shuffle(hw)$
7:      $index\_key \leftarrow hws.index()$
8:      $hws \leftarrow array(hws)$
9:      $hws \leftarrow hws.reshape(int(H/bs), \ int(W/bs))$
10:     $imsize \leftarrow frame.shape$
11:     $imgn \leftarrow frame$
12:     $c1 \leftarrow 0$
13:     **for** i in r_[:imsize[0]:bs] **do**
14:         c2=0
15:         **for** j in r_[:imsize[0]:bs] **do**
16:             x, y = hws[c1][c2]
17:             imgn[i:(i + bs),j:(j+ bs)] =
18:                 ch[x:(x + bs),y:(y + bs)]
19:         c1+=1
20:     **return** ch, index_key

VI. EXPERIMENTAL ANALYSIS AND DISCUSSION

A. Functional Test

Figure 7 demonstrates the functionality of the proposed DAB scheme proving that it works as required. The plain image in Fig. 7(a) is completely transformed into a random cipher in Fig. 7(b) by the AES coupled with a BS algorithm as shown by Algorithm 2.

Figure 8 shows sample blocks created when two requests for access to stored surveillance videos were made on two different dates. The request and all associated information are stored in the data part of the blocks. As shown by Fig. 8, the data section of the blocks are stored as cipher-text for security and privacy reasons. The secret keys that are used to unlock the data part are kept in the BC-nodes indexed and encrypted with their private keys.

B. Security of the Enciphering Scheme

To measure the security and computational performance of the proposed DAB scheme, a number of computational security and statistical parameters are considered. The tests or parameters considered include Encryption Quality, Frequency Test, Run Test, Gap Test, Poker Test, Pixel Sensitivity, Key

Fig. 7.   Enciphering: (a) Plain frame/Image, (b) AES Encrypted & Shuffled

```
{'chain': [{'index': 0,
  'timestamp': '01/03/2021',
  'data': 'GenesisBlock',
  'previousHash': '0',
  'hash': '100692994814683281974475180211005660617496449272105605018616585587595325244',
  'nonce': 'SAC_1'},
 {'index': 1,
  'timestamp': '11/03/2021',
  'data': {'1a4d8ec7a3f101ba6182bce0cb70e8181b9f26096882f01dce4105a92dc324a239678faa8c87c0cf9d0bff196ef6b02cd3416
207004cf0e535750276d4cca7f3e6f1d06b874ff78cd63926d08e48fc15a6e48d364236b0f74c5d24f12680cdbfbe9b180036a24b4018a1d2f
d782654d4d659a64e3933e0a45ce600e3a1b6bf26293a0f23bccc31a93f611f8674de9ee8f8991ef38f84511afc03d4d1605c4ae854f7ce175
f1df27bd09c0d7dc1aae1f9f5919645b4ade2309a840fd1a0955fbe174400e3cbe78df47263daf58ad1af61f1961f9b1f1ae9bf568fa453300
d5c3c9d41ed22a9959737c824363fe8657d820a56d89cb8dba1d2d27ea12eb7d0989bd542a9d9d920b147b053b7e4d6ce8d256e94427947e3c
b635247945ff86bbe8cd0dcc25b0baaaee7ec4a3c79dbae2dc7be551cdb38de9cc57b64da819de74ec751218b95dccdf5f944cb9ff651e723e
bb2a7012c6e445e2bbadceeab7e397fd4b1a98e67ff4c25919dada5fcf4bcdcf7e5f6cc4e8b60883c349173becb50'},
  'previousHash': '100692994814683281974475180211005660617496449272105605018616585587595325244',
  'hash': '13527712871399635413174171904063902509138181637848565563598888725569721632',
  'nonce': 'SAC_2'},
 {'index': 2,
  'timestamp': '12/03/2021',
  'data': {'1a4d8ec7a3f101ba6182bce0cb70e8181b9f26096882f01dce4105a92dc324a239678faa8c87c0cf9d0bff196ef6b02cd3416
207004cf0e535750276d4cca7f3e6f1d06b874ff78cd63926d08e48fc15a6e48d364236b0f74c5d24f12680cdbfbe9b180036a24b4018a1d2f
d782654d4d659a64e3933e0a45ce600e3a1b6bf26293a0f23bccc31a93f611f8674de9ee8f8991ef38f84511afc03d4d1605c4ae854f7ce175
f1df27bd09c0d7dc1aae1f9f5919645b4ade2309a840fd1a0955fbe174400e3cbe78df47263daf58ad1af61f1961f9b1f1ae9bf568fa453300
d5c3c9d41ed22a9959737c824363fe8657d820a56d89cb8dba1d2d27ea12eb7d0989bd542a9d9d920b147b053b7e4d6ce8d256e94427947e3c
b635247945ff86bbe8cd0dcc25b0baaaee7ec4a3c79dbae2dc7be551cdb38de9cc57b64da819de74ec751218b95dccdf5f944cb9ff651e723e
bb2a7012c6e445e2bbadceeab7e397fd4b1a98e67ff4c25919dada5fcf4bcdcf7e5f6cc4e8b60883c349173becb50'},
  'previousHash': '13527712871399635413174171904063902509138181637848565563598888725569721632',
  'hash': '65088100624101390014521897311761249347102754518525998946215177313002388300249',
  'nonce': 'SAC_3'}],
 'difficulty': 1}
```

Fig. 8. Creation of sample blocks with the data part enciphered: data comprises requests made and associated identify information and log of activities.

Sensitivity, Peak Signal to Noise Ratio (PSNR), Entropy Test, and Correlation Analysis.

Encryption Quality (EQ), as stated in Eq. 4, is a measure of changes in pixels after a plain frame/image has been encrypted. The higher the number of pixels changed, the better the quality of the enciphering scheme is. The proposed DAB scheme has an Encryption Quality of 99.998%, which means that almost every pixel in the plain image has a different value after encryption was performed. More details of Frequency Test, Run Test, Gap Test, and Poker Test are available to interested readers in the US National Institute of Technology (NIST) randomness test suite [22], [24]. For detailed explanation of Pixel Sensitivity, Key Sensitivity, Peak Signal to Noise Ratio (PSNR), Entropy Test, and Correlation Analysis, please refer to [11]. The results of all tests conducted are shown in Table I, which validate the the proposed DAB scheme.

$$EQ = \frac{Number\ of\ affected\ pixels}{Total\ Number\ of\ pixels} \qquad (4)$$

C. Security & Privacy of SePriS system

In order to ensure a secure and privacy-aware surveillance practice while sharing or accessing stored surveillance videos, the following requirements are set.

1. Security: It is often viewed in terms of the confidentiality, integrity and availability (CIA) Triad. The confidentiality ensures that only authorized users can access the data under protection. The integrity property requires that data must be accurate in transit and be altered only by authorized parties. At last, the availability attribute of security states that the security mechanism in use must allow the data to be accessible to the right users at the right time in the right way.

2. Privacy: It requires that the privacy of individuals caught on CCTV cameras and stored on off-BC sites must be preserved in optimal balance with usability.

TABLE I
SECURITY ANALYSIS

Parameter/Test	Result	Remark
Encryption Quality	99.998%	*Ratio of changed pixels*
Frequency Test	0.643	*P_val > decision rule*
Run Test	0.23	*P_val > decision rule*
Gap Test	*Passed*	*All p_values > 0.05*
Poker Test	*Passed*	*All p_values > 0.05*
Pixel Sensitivity	− − −	*To be secure :*
NPCR	99.151%	*Must be > 99%*
UACI	33.139%	*Must be > 33%*
Key Sensitivity	− − −	*To be secure :*
NPCR	99.634%	*Must be > 99%*
UACI	33.548%	*Must be > 33%*
PSNR Test	11.73dB	*Good if less than 20dB*
Entropy Test	7.945	*Good if closer to 8*
Correlation	− − −	*Good if closer to 0*
Horizontal	0.0027	− − −
Vertical	0.0065	− − −
Diagonal	0.00781	− − −

3. Authenticity: the proposed scheme must have a capability to verify the identities of requestors before any access is granted.

4. Accountability: The scheme must have a capability for auditing users to hold them responsible for any misbehaving.

5. Auditability: The proposed scheme must be auditable, which is an essential component of security. Logging and audit logs are, for instance, vital. The audit logs contain information on who have accessed which videos and what they did on them.

6. Anonymity: This requirement refers to the fact that parties must have no visible identifier for privacy reasons. As our goal is to prevent abuse of surveillance videos by people in

charge, our scheme does not guarantee complete anonymity to users who access stored video. However, individuals on video frames are anonymized!

The proposed SePriS system is designed to meet the aforementioned requirements. As depicted in Table II, SePriS meets all requirements except anonymity, which is partially met. Within the secure group, in order to discourage leaking, some identity information about users are stored as part of the blocks in every BC-node in enciphered form.

TABLE II
SECURITY ANALYSIS

Parameter	Result	Remark
Security	*Yes*	*In terms of CIA Triad*
Privacy	*Yes*	*Privacy is ensured!*
Integrity	*Yes*	*By Double Lock Boxes*
Authenticity	*Yes*	*Required before any access*
Controllability	*Yes*	*Scheme is manageable*
Auditability	*Yes*	*All activities are auditable!*
Accountability	*Yes*	*Ensured by scheme!*
Anonymity	*No*	*Partially*

VII. CONCLUSIONS

Security and privacy are very essential issues in the world of video surveillance. This paper proposes SePriS, a private blockchain based solution coupled with an efficient video frame enciphering mechanism for sharing stored surveillance videos in a secure and privacy-aware way. It illustrates how the blockchain technology can be leveraged to prevent abuse and leaking of stored videos, which have plagued the surveillance practice for years. The experimental analysis show that the video frame enciphering mechanism passes the standard computational and security parameters. Additionally, they corroborate the security, privacy, integrity, authenticity, controllability, auditability, and accountability of the proposed decentralized system for sharing of stored surveillance videos. Overall, the SePriS system achieves the design goal and creates a video surveillance system with good balance of privacy and usability.

REFERENCES

[1] R. Altawy and A. M. Youssef, "Security, privacy, and safety aspects of civilian drones: A survey," *ACM Transactions on Cyber-Physical Systems*, vol. 1, no. 2, p. 7, 2017.

[2] A. Cavallaro, "Privacy in video surveillance [in the spotlight]," *IEEE Signal Processing Magazine*, vol. 2, no. 24, pp. 168–166, 2007.

[3] A. Cavoukian, *Privacy and drones: Unmanned aerial vehicles*. Information and Privacy Commissioner of Ontario, Canada Ontario, 2012.

[4] J. Clement, "Global digital population as of july 2020," *https://www.statista.com/statistics/617136/digital-population-worldwide/*, 2020 (accessed on August 24, 2020).

[5] C. Coconu, V. Stoica, F. Ionescu, and D. Profeta, "Distributed implementation of discrete cosine transform algorithm on a network of workstations," in *Proceedings of the International Workshop Trends & Recent Achievements in IT, Romania*. Citeseer, 2002, pp. 116–121.

[6] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in *2017 IEEE World Congress on Services (SERVICES)*. IEEE, 2017, pp. 90–93.

[7] J. Drees, "150,000 security cameras hacked, exposing footage from halifax health, other hospitals," *Becker's Hospital Review*, 2021.

[8] A. Fitwi and Y. Chen, "Privacy-preserving selective video surveillance," in *2020 29th International Conference on Computer Communications and Networks (ICCCN)*. IEEE, 2020, pp. 1–10.

[9] A. Fitwi, Y. Chen, and N. Zhou, "An agent-administrator-based security mechanism for distributed sensors and drones for smart grid monitoring," in *Signal Processing, Sensor/Information Fusion, and Target Recognition XXVIII*, vol. 11018. International Society for Optics and Photonics, 2019, p. 110180L.

[10] A. Fitwi, Y. Chen, and S. Zhu, "Prise: Slenderized privacy-preserving surveillance as an edge service," in *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*. IEEE, 2020, pp. 125–134.

[11] A. Fitwi, Y. Chen, S. Zhu, E. Blasch, and G. Chen, "Privacy-preserving surveillance as an edge service based on lightweight video protection schemes using face de-identification and window masking," *Electronics*, vol. 10, no. 3, p. 236, 2021.

[12] A. Fitwi, M. Yuan, S. Y. Nikouei, and Y. Chen, "Minor privacy protection by real-time children identification and face scrambling at the edge," *submitted to EAI Endorsed Transactions on Security and Safety*, 2020.

[13] C. Goldberg, "Introduction to the world of peeping toms, binoculars and headset included," *New York Times*, p. 35, 1995.

[14] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecommunications policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[15] L. Lin and N. Purnell, "A world with a billion cameras watching you is just around the corner," *The Wall Street Journal*, 2019.

[16] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[17] N. Org, "Ineffectiveness of surveillance cameras," *Surveillance Camera Players*, 2009.

[18] ——, "Abuses of surveillance cameras," *Surveillance Camera Players*, 2010.

[19] W. B. Pennebaker and J. L. Mitchell, *JPEG: Still image data compression standard*. Springer Science & Business Media, 1992.

[20] Q. M. Rajpoot and C. D. Jensen, "Video surveillance: Privacy issues and legal compliance," in *Promoting Social Change and Democracy through Information Technology*. IGI global, 2015, pp. 69–92.

[21] L. Rakhmawati *et al.*, "Image privacy protection techniques: A survey," in *TENCON 2018-2018 IEEE Region 10 Conference*. IEEE, 2018, pp. 0076–0080.

[22] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen and Hamilton Inc Mclean Va, Tech. Rep., 2001.

[23] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y.-L. Tian, A. Ekin, J. Connell, C. F. Shu, and M. Lu, "Enabling video privacy through computer vision," *IEEE Security & Privacy*, vol. 3, no. 3, pp. 50–57, 2005.

[24] M. J. Strube, "Tests of randomness for pseudorandom number generators," *Behavior Research Methods & Instrumentation*, vol. 15, no. 5, pp. 536–537, 1983.

[25] E. Vattapparamban, İ. Güvenç, A. İ. Yurekli, K. Akkaya, and S. Uluağaç, "Drones for smart cities: Issues in cybersecurity, privacy, and public safety," in *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 2016, pp. 216–221.

[26] J. Wang, B. Amos, A. Das, P. Pillai, N. Sadeh, and M. Satyanarayanan, "Enabling live video analytics with a scalable and privacy-aware framework," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 14, no. 3s, p. 64, 2018.

[27] R. Xu and Y. Chen, "Microchain: A light hierarchical consensus protocol for iot system," *arXiv preprint arXiv:1912.10357*, 2019.

[28] R. Xu, Y. Chen, and E. Blasch, "Decentralized access control for iot based on blockchain and smart contract," *Modeling and Design of Secure Internet of Things*, pp. 505–528, 2020.

[29] R. Xu, S. Y. Nikouei, D. Nagothu, A. Fitwi, and Y. Chen, "Blendsps: A blockchain-enabled decentralized smart public safety system," *Smart Cities*, vol. 3, no. 3, pp. 928–951, 2020.

[30] M. Yuan, S. Y. Nikouei, A. Fitwi, Y. Chen, and Y. Dong, "Minor privacy protection through real-time video processing at the edge," *arXiv preprint arXiv:2005.01178*, 2020.

[31] G. Zyskind, O. Nathan *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*. IEEE, 2015, pp. 180–184.