sensors

MDPI

Article

Smart Privacy Protection for Big Video Data Storage Based on Hierarchical Edge Computing

Di Xiao *, Min Li and Hongying Zheng

College of Computer Science, Chongqing University, Chongqing 400044, China; li_min_1995@163.com (M.L.); zhenghongy@cqu.edu.cn (H.Z.)

* Correspondence: xiaodi_cqu@hotmail.com; Tel.: +86-23-6510-3199

Received: 13 February 2020; Accepted: 9 March 2020; Published: 10 March 2020

Abstract: Recently, the rapid development of the Internet of Things (IoT) has led to an increasing exponential growth of non-scalar data (e.g., images, videos). Local services are far from satisfying storage requirements, and the cloud computing fails to effectively support heterogeneous distributed IoT environments, such as wireless sensor network. To effectively provide smart privacy protection for video data storage, we take full advantage of three patterns (multi-access edge computing, cloudlets and fog computing) of edge computing to design the hierarchical edge computing architecture, and propose a low-complexity and high-secure scheme based on it. The video is divided into three parts and stored in completely different facilities. Specifically, the most significant bits of key frames are directly stored in local sensor devices while the least significant bits of key frames are encrypted and sent to the semi-trusted cloudlets. The non-key frame is compressed with the two-layer parallel compressive sensing and encrypted by the 2D logistic-skew tent map and then transmitted to the cloud. Simulation experiments and theoretical analysis demonstrate that our proposed scheme can not only provide smart privacy protection for big video data storage based on the hierarchical edge computing, but also avoid increasing additional computation burden and storage pressure.

Keywords: smart privacy protection; hierarchical edge computing; color video; low computation complexity; cloud storage

1. Introduction

Cloud computing was introduced in Search Engine Strategies 2006 in order to tackle the constraints of the Internet of Things (IoT) in management, storage, computing and processing, and was formally defined by National Institute of Standards and Technology [1]. Since then, this prominent computing infrastructure has always drawn attentions of increased individuals, enterprises and researchers with its affordable prices, powerful communication facilities, abundant computing and storage resources [2]. These advantages make it possible to offer more services (e.g., cloud storage [3], smart monitoring and forecasting [4]) by integrating plentiful connected sensor devices.

However, cloud computing cannot efficiently support big multimedia data storage in distributed IoT environments because of the following reasons [5]. First, the mobile sensor application facilities require real-time response, location awareness and mobility, but cloud computing fails to satisfy these demands due to being far away from local sensor devices. Second, cloud computing processes huge amounts of raw data directly, which results in inevitable service delays and process blocking. Third, cloud services face substantial unprecedented challenges with exponential rise of user volume. In order to better address the above issues, edge computing [6,7], a new decentralized paradigm, was proposed to extend cloud computing to the edge of networks. This popular technology contains seven features, that is, dense geographical distribution, mobility support, location awareness, context-awareness, low latency, proximity and heterogeneity so that it can improve the efficiency and quality of cloud services and be suitable for strict and smart application scenarios [8].

Generally speaking, edge computing includes three patterns, that is, multi-access edge computing (MEC) [9,10], cloudlets [11] and fog computing [12]. To be brief, MEC is an emergency model that uses mobile base stations as sensor nodes to handle delay-sensitive and context-aware applications. Different from set-top-boxes, road-side units, routers, gateways and other resource-limited devices, cloudlets have powerful CPU and rich storage spaces. Fog computing is regarded as a scenario in which a large number of heterogeneous and decentralized base stations and access points act as fog nodes to communicate and cooperate with each other and perform information processing and storage operations in the absence of the third-party. The overall architecture of edge computing is shown in Figure 1. The outermost layer is the local facilities which are formed by plentiful mobile sensor devices such as smart transportation, medical treatment and wearable services. Original data can be generated or sampled here and transmitted to the middle layer for the next process. The middle layer is the edge layer which contains numerous edge nodes with computing and storage capabilities. It exists for the purpose of providing transient data storage and computing offloading for users and simultaneously alleviating the cloud burden. The central layer is the cloud server which supports further huge data processing and storage.

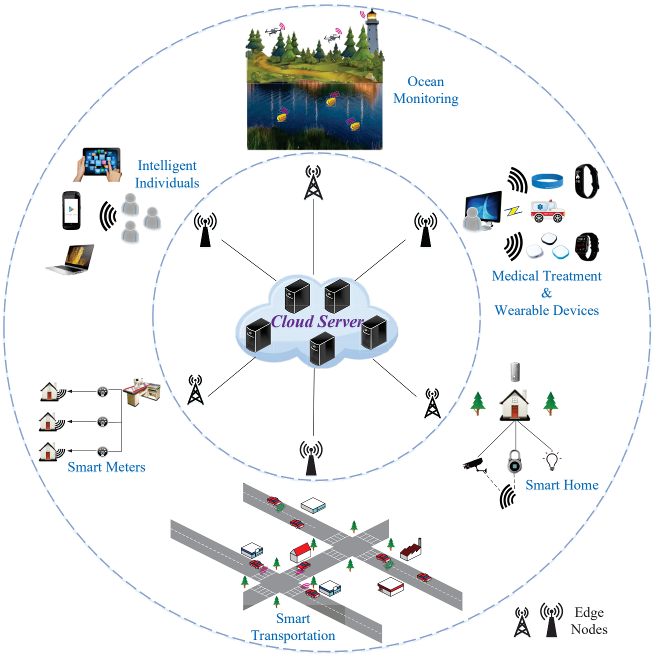


Figure 1. The overall architecture of edge computing.

However, various security issues have always been potential threats to the cloud storage. Each user has his/her own data ranging from GB's to TB's and the local storage fails to achieve this huge demand alone. Thus, deploying a low-complexity and high-secure cloud storage service has become an inevitable trend. In other words, the cloud provider who supports smart edge computing-based IoT applications with higher security degrees will attract more individuals. In this paper, we propose a novel distributed compressive video sensing (DCVS) coding [13] and the hierarchical edge computing architecture-based scheme to offer a low-complexity and high-secure big video data storage service. Our main contributions can be summarized as follows.

- We make full use of the respective advantages of MEC, cloudlets and fog computing to design the hierarchical edge computing architecture to support distributed IoT application environments.
- The most significant bits (MSB) of the key frame (KF) are completely controlled by users so that our proposed scheme has higher degrees of security. Meanwhile, the least significant (LSB) bits of

KF are directly encrypted via MSB to avoid unnecessary computation burden of edge computing and extra storage pressure of local sensor devices.

- The two-layer parallel compressive sensing is used to compress the non-key frame (NKF) so as to minimize the storage burden on cloud services.

The remainder of this paper is organized as follows. Section 2 briefly provides necessary and basic relevant knowledge. Section 3 describes the scheme of smart privacy protection for big video data storage based on the hierarchical edge computing in detail. Section 4 evaluates performance of the proposed scheme from both experiments and theory and Section 5 draws a brief conclusion.

2. Related Work

2.1. Bit Adaptive Diffusion

Diffusion can significantly change statistical characteristics of the input plain-frame and spread the influence of each bit to the cipher-frame. The principle is to diffuse the corresponding pixel of the current frame through the value of the key stream [14]. In order to achieve high communication efficiency of hardware in cloud computing, we adopt bit adaptive diffusion by bit-wise XOR operation. It can be defined as

$$A_{i,j} = \begin{cases} O_{i,j} \oplus O_{I,J} \oplus S_{i,j}, & if\ i = 1, j = 1, \\ O_{i,j} \oplus A_{I,j-1} \oplus S_{i,j}, & if\ i = 1, j \neq 1, \\ O_{i,j} \oplus A_{i-1,j} \oplus S_{i,j}, & if\ i \neq 1, \end{cases} \tag{1}$$

where $\oplus$ is the bit-wise XOR operation. S is the key stream with the same size $(I \times J)$ and data format as the original frame O. The inverse operation in the decryption process can be expressed by

$$O_{i,j} = \begin{cases} A_{i,j} \oplus O_{I,J} \oplus S_{i,j}, & if\ i = 1, j = 1. \\ A_{i,j} \oplus A_{I,j-1} \oplus S_{i,j}, & if\ i = 1, j \neq 1. \\ A_{i,j} \oplus A_{i-1,j} \oplus S_{i,j}, & if\ i \neq 1. \end{cases} \tag{2}$$

2.2. Parallel Compressive Sensing

Compressive sensing (CS) has two promising advantages: compress and sample simultaneously; the sampling rate is much lower than the Nyqvist-Shannon criterion. Both of them facilitate CS to be used in relevant fields widely since its emergence [15]. However, the multidimensional signal has to be transformed to the 1D signal before compression so that the required measurement matrix is tremendous. In order to reduce computation complexity and storage space, the characteristics of 2D signals are combined with the theory of CS to be parallel CS (PCS) [16] is suggested. The mathematical expression is as follows

$$y_i = \Phi x_i, \tag{3}$$

where x_i is the i column of an original 2D signal and y_i is the i column of the measurement value via linear projection of the measurement matrix Φ.

2.3. Researches on Relevant Privacy-Protection Schemes

Lyu et al. proposed a privacy-preservation system for fog-based aggregation in Smart Grid with differential privacy so as to enable the intermediate fog nodes to safely collect data from connected smart meters [17]. Wang et al. presented a three-layer privacy preserving cloud storage scheme in cloud computing to resist possible attacks from the inside of cloud servers [18]. Xue et al. designed verifiable security fine-grained access control in vehicular cloud computing to share latency-sensitive data [19]. Gu et al. provided a dynamic method to protect user privacy during communications between users and multiple fog nodes and meanwhile discussed the payoff and privacy loss in time of the process [20]. Wang et al. proposed an effective dual-chaining watermark scheme for data integrity protection in smart campus IoT applications, and this smart meteorological Internet of Things system can effectively authenticate the integrity of the data with free distortion at low cost [21]. Wang et al. proposed an edge-based model for data collection to provide a general privacy preservation service via the differential privacy algorithm [22]. Wang et al. designed a scheme that attempts to preserve a balance in user privacy, data integrity in edge-assisted IoT devices and the computational cost through a balanced truth discovery approach and a proposed enhanced technique [23]. He et al. proposed a distributed privacy preserving scheme for random linear network coding in smart grid that offers a data confidentiality privacy preserving feature and efficiently thwarts traffic analysis [24]. Xie et al. designed a new efficient privacy preserving compressive data gathering scheme, which exploits homomorphic encryption functions in compressive data gathering to thwart the traffic analysis/flow tracing and possess message flow un-traceability and message content confidentiality [25]. Gu et al. presented a scheme for the privacy protection of location data mining based on the differential privacy mechanism, which protects highly frequent accessing location data or location preference of user by distorting accessing frequencies [26]. It is worth affirming that the above researches have achieved great contributions of privacy protection based on the cloud computing in different aspects.

However, to the best of our knowledge, this study is the first to take full advantage of MEC, cloudlets and fog computing to design the hierarchical edge computing architecture and propose a smart and low-complexity privacy protection scheme for big video data storage based on it. Besides, the cloud space does not mean unlimited storage resources so that we also consider compression.

2.4. Researches on Relevant Edge Computing Schemes

Bonomi et al. argued that the features of fog computing make it suitable for many critical Internet of Things services and applications, namely, connected vehicle, smart grid, cloud computing and wireless sensors networks [27]. Hu et al. showed that MEC enables innovative service scenarios that can ensure enhanced personal experience and optimized network operation, and satisfy the demanding requirements for ultra-low latency and stimulating innovation [28]. A novel vision of mobile computing liberates mobile devices from severe resource constraints by enabling resource-intensive applications to use cloud computing free of jitter, congestion and failures [29]. Unfortunately, longer communication delay is a fundamental obstacle. Rather than relying on a distant "cloud", it is better to address a mobile device's resource poverty through the nearby resource-rich edge computing.

Mora-Gimeno et al. presented a security model for the externalization of application execution in multi-tier MEC environments, which produces a minimal overhead, especially for computationally intensive applications [30]. Lee et al. designed a hierarchical MEC architecture in which MEC servers are arranged in a hierarchical way to provide users with rapid content delivery, higher computing performance, and efficient use of server resources [31]. Dong et al. studied a dynamic and decentralized resource-allocation strategy based on the evolutionary game theory to deal with task offloading to multiple heterogeneous edge nodes and central clouds among multi-users, which could achieve one evolutionary equilibrium, and meet users' quality-of-service requirements under resource constraints of edge nodes [32]. Lee et al. proposed the MEC-based mobility management scheme that arranges MEC server as the concept of Zone so that mobile users can continue to receive content and use server resources efficiently even when they move [33].

The above researches related with the edge computing schemes can be classified as the three-level architecture, including the local individual layer, the edge computing layer and the cloud computing layer. Specifically, the edge computing layer is refined as the MEC layer. However, although MEC brings computing power and storage resources to the edge of the mobile network, limited computation resources of mobile edge nodes may not be sufficient to serve excessive offloading tasks exceeding the computation capacities of themselves. Further, we can take advantage of the lower latency of MEC to distinguish KF from NKF in real time while receiving the video. Meanwhile, all frames are encrypted or compressed by fog computing, which has relatively stronger computing resources compared with

MEC. In addition, considering the local storage resources are limited and individuals do not want the key information of the video to be stored by completely un-trusted cloud, we use the independent encoding - joint decoding DCVS coding to divide the video data into three parts. MSB of KF is stored by local devices while LSB of KF is transmitted to the semi-trusted cloudlets. The rest, NFK, which must be reconstructed better via referring to KF, should be stored to the cloud after a series of processing. This is why we design a novel hierarchical edge computing architecture to provide smart private protection for big video data storage with low latency.

3. Description of the Proposed Scheme

The overall scheme of using the hierarchical edge computing architecture to protect big video data storage privacy is shown in Figure 2. Firstly, local devices transmit video streams to the edge layer through wireless communication. Then, the raw videos are processed by the group of pictures (GOP) selection in MEC. The separated KF and NKF are encrypted and compressed respectively in fog computing. Significant and sensitive KF after processing are stored in local devices and cloudlets equally. The remainders are sent to the cloud server via wire communication. Both procedures and algorithms adopted in our proposed scheme will be described in detail as follows. It is worth noticing that we adopt color videos as objects to better fit the actual environment.

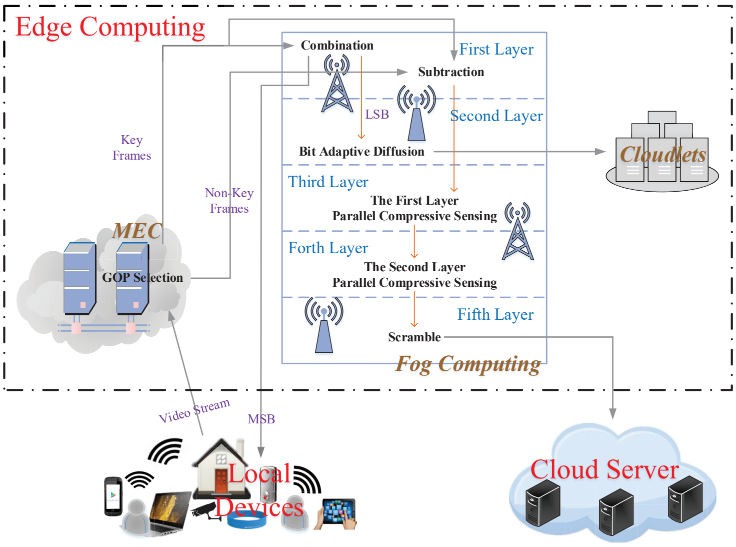


Figure 2. The overall scheme of privacy protection for big video data storage based on the hierarchical edge computing.

3.1. GOP Selection

Video is not a simple combination of pictures, and there are strong correlations among frames. That is, the selection of KF often determines the whole recovery performance of NKF from the same GOP. Thus, GOP selection has profound significance for video sampling. However, service objects of the cloud consist of intelligent users, ocean monitoring and so on, as shown in Figure 1, so we have to combine actual scenarios and computation costs to distinguish KF from NKF .

- Fixed GOP values: If a certain scenario needs to analyze complex or important videos, the small values should be selected to ensure reconstruction performance, while the large values could be considered to reduce the overall sampling rate of videos and handle massive data.
- Adaptive GOP selection: In order to improve encoding efficiency and decoding performance, the adaptive GOP selection based on the perceptual hash algorithm was applied for DCVS [34]. Though the computation complexity of this algorithm is relatively high, the accuracy of selecting KF is raised substantially.

In a word, we should make a concrete analysis of concrete conditions. MEC receives the video stream from the nearest local devices and then the separated KF and NKF are transmitted to different layers of fog computing.

3.2. Encoding and Decoding of Key Frames

Take 1st frame of "News(CIF)" as an example. The whole scheme of encoding KF is shown in Figure 3. The first layer of fog computing receives KF and separates the RGB three-layer of a color frame bit by bit all alone. These bit-layers can be denoted by $\left\{X_{Kj}^{i}\right\}$ where $i \in \{1, 2, \ldots, 8\}$, $j \in \{R, G, B\}$, e.g., X_{KR}^{1} is the first bit-layer of the R layer in the KF. As the operation of the RGB three-layer are the same so that we describe the R layer in particular.

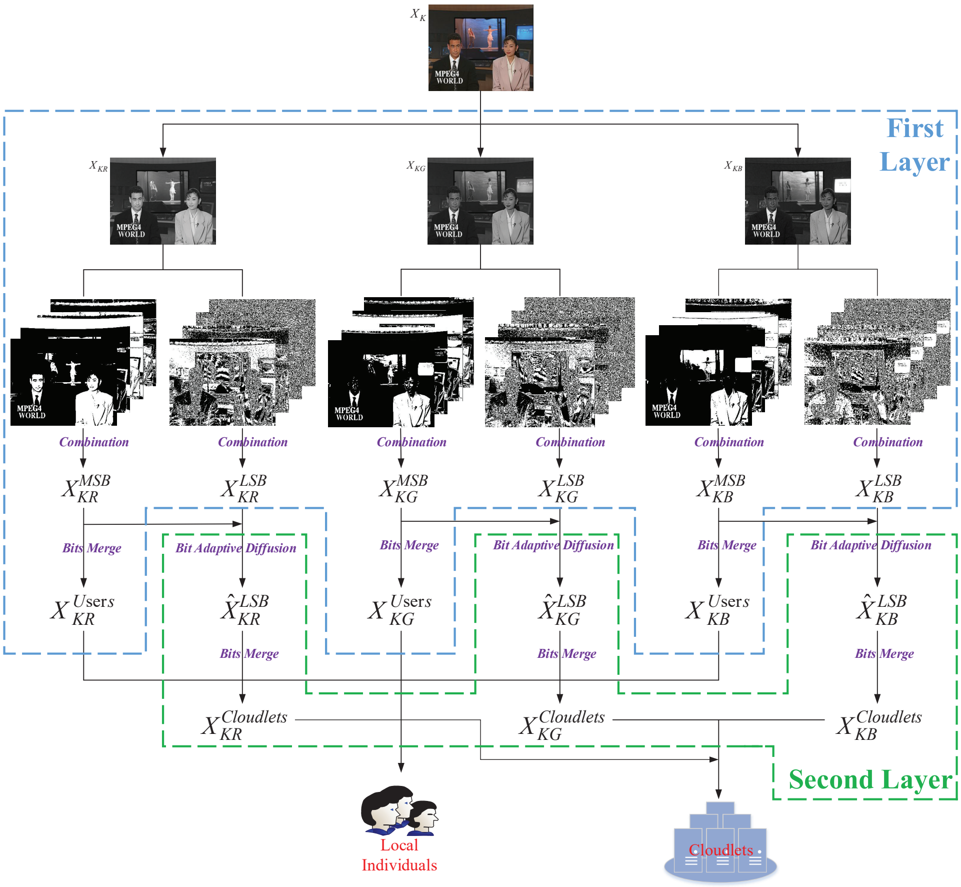


Figure 3. The encoding of key frame (KF) in fog computing.

The MSB $\left\{X_{KR}^{1}, X_{KR}^{2}, X_{KR}^{3}, X_{KR}^{4}\right\}$ and LSB $\left\{X_{KR}^{5}, X_{KR}^{6}, X_{KR}^{7}, X_{KR}^{8}\right\}$ of the original R layer are respectively combined to generate the 1D plane X_{KR}^{MSB} and X_{KR}^{LSB}. Then X_{KR}^{LSB} and the copied X_{KR}^{MSB} are transmitted to the second layer of fog computing. Perform bit adaptive diffusion with X_{KR}^{MSB} by

$$\hat{X}_{KR}^{LSB}(r.c) = \begin{cases} X_{KR}^{LSB}(r.c) \oplus X_{KR}^{LSB}(4M, N) \oplus X_{KR}^{MSB}(r, c), & if\ r = 1, c = 1, \\ X_{KR}^{LSB}(r.c) \oplus \hat{X}_{KR}^{LSB}(N, c) \oplus X_{KR}^{MSB}(r, c), & if\ r = 1, c \neq 1, \\ X_{KR}^{LSB}(r.c) \oplus \hat{X}_{KR}^{LSB}(r-1, c) \oplus X_{KR}^{MSB}(r, c), & if\ r \neq 1, \end{cases} \tag{4}$$

where $r\ (r \in [1, 4M])$ is the abscissa and $c\ (c \in [1, N])$ is the ordinate. M and N are the width and the length of the KF X_K respectively.

Then, the binary matrix X_{KR}^{MSB} and the encrypted $\hat{X}_{KR}^{LSB}$ are merged bit by bit in the first layer and the second layer of fog computing respectively to obtain X_{KR}^{Users} and ciphertext $X_{KR}^{Cloudlets}$. Specifically, the binary matrix merges each 8 bits into a new pixel as shown in Figure 4. Then send X_{KR}^{Users} to local devices and send $X_{KR}^{Cloudlets}$ to cloudlets simultaneously.

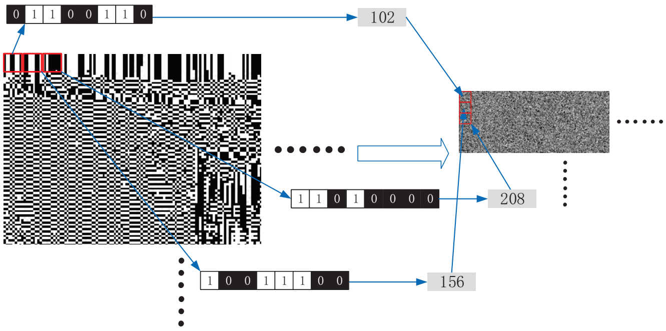


Figure 4. The visual representation of merging a binary matrix to a pixel matrix.

As encoding of KF only involves encryption, decoding is the inverse process of encoding. In brief, X_{KR}^{Users} and $X_{KR}^{Cloudlets}$ are obtained from local devices and cloud servers respectively at first, and then the original LSB are decrypted with the MSB binary stream. Finally, combine MSB with LSB to generate KF. Thus it can be seen KF, as the key information of the video, is further divided into two parts. The most important part of KF is directly stored in local devices, and meanwhile regarded as the key to encrypt the least important part. Considering the local storage resources are limited and individuals do not hope to transmit any data of KF to the un-trusted cloud, we could store LSB of KF with the help of cloudlets in order to obtain higher level of security.

3.3. Encoding and Decoding of Non-Key Frames

To further improve the security level and achieve better accuracy of the NKF reconstruction, we do not directly perform coding but extract deviations between NKF and KF of the same GOP at first in the first layer of fog computing. Then taking the 2nd frame of "News(CIF)" as an example, as shown in Figure 5, the process of the first layer PCS is to compress the RGB three-layer of deviations independently in the third layer of fog computing. It can be represented visually as follows

$$\begin{cases} Y_{NR}^{deviations} = \Phi_{NR} X_{NR}^{deviations}, \\ Y_{NG}^{deviations} = \Phi_{NG} X_{NG}^{deviations}, \\ Y_{NB}^{deviations} = \Phi_{NB} X_{NB}^{deviations}, \end{cases} \tag{5}$$

where $\left\{ X_{Nj}^{deviations} \,|j \in \{R, G, B\} \right\}$ is the RGB three-layer of the original deviations between KF and NKF, and $\left\{ Y_{Nj}^{deviations} \,|j \in \{R, G, B\} \right\}$ is the corresponding measurement values. Let us discuss the generation of the measurement matrix $\{\Phi_{Nj} \,|j \in \{R, G, B\}\}$. To ensure the better reconstruction performance and satisfy the easier implementation of hardware simultaneously, the deterministic binary block diagonal matrix (DBBD) [35] is adopted here. Moreover, considering the level of security, we select different sampling rates to compress each layer of deviations. Then convert $Y_{N}^{deviations}$ to a 1D plane $\hat{Y}_{N}^{deviations}$ and transmit it to the forth layer of fog computing. The process of the second layer PCS is to compress $\hat{Y}_{N}^{deviations}$ with Φ_{DBBD} to obtain $\hat{Y}_N$. For a certain NKF, the total sampling rate is

$$\Gamma = [(\gamma_R + \gamma_G + \gamma_B) \div 3] \times \gamma, \tag{6}$$

where $\gamma_R, \gamma_G, \gamma_B$ denote the sampling rate of the RGB three-layer respectively and γ is that of $\hat{Y}_{N}^{deviations}$. Although we do not directly process the original NKF, the measurement matrix used to reduce computation complexity and storage pressure is not secure, so the information after compression needs to be further encrypted. Send $\hat{Y}_N$ to the fifth layer of fog computing and the steps of scramble are shown below.

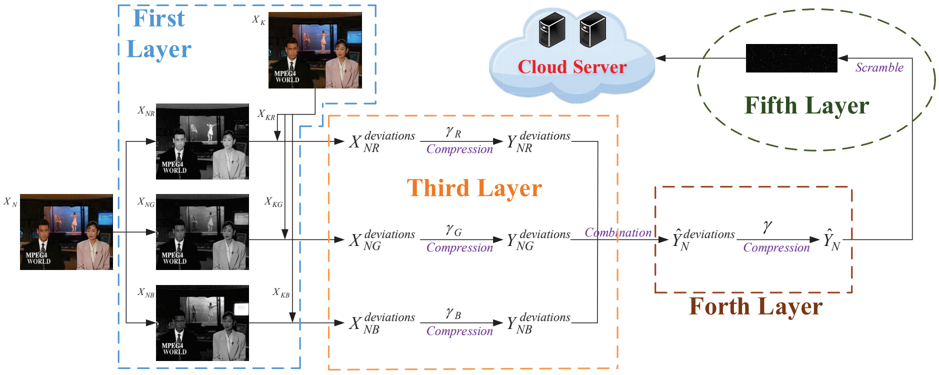


Figure 5. The encoding of non-key frame (NKF) in fog computing.

1. Set initial values α_0, β_0 and a control parameter μ $(\alpha_0, \beta_0, \mu \in (0,1))$.
2. Iterate $H \times W + l$ rounds by 2D logistic-skew tent map with α_0, β_0, μ and discard first l iterated values to avoid transient effects by

$$\begin{cases} \alpha_{i+1} = 4 \times \beta_i \times (1 - \beta_i)\,, \\ \beta_{i+1} = \begin{cases} \alpha_i / \mu, & 0 < \alpha_i < \mu, \\ (1 - \alpha_i)/(1 - \mu), & \mu \leq \alpha_i < 1, \end{cases} \end{cases} \tag{7}$$

   where $H \times W$ is the size of $\hat{Y}_N$.
3. Discretize α, β and obtain two sequences α', β' $(j \in [1, H \times W])$,

$$\begin{cases} \alpha'_j = \left\lfloor \alpha_j \times 10^{14} \right\rfloor & \bmod H + 1. \\ \beta'_j = \left\lfloor \beta_j \times 10^{14} \right\rfloor & \bmod W + 1. \end{cases} \tag{8}$$

4. Rearrange α', β' into two matrices with the size $[H, W]$ respectively.
5. Exchange the pixel $\hat{Y}_N\,(h, w)$ and $\hat{Y}_N \left(\alpha'_{h,w}, \beta'_{h,w} \right)$ from the top left corner to the bottom right corner in order where $h \in [1, H]$, $w \in [1, W]$, $\alpha'_{h,w}$ and $\beta'_{h,w}$ are values in matrices α', β' respectively.

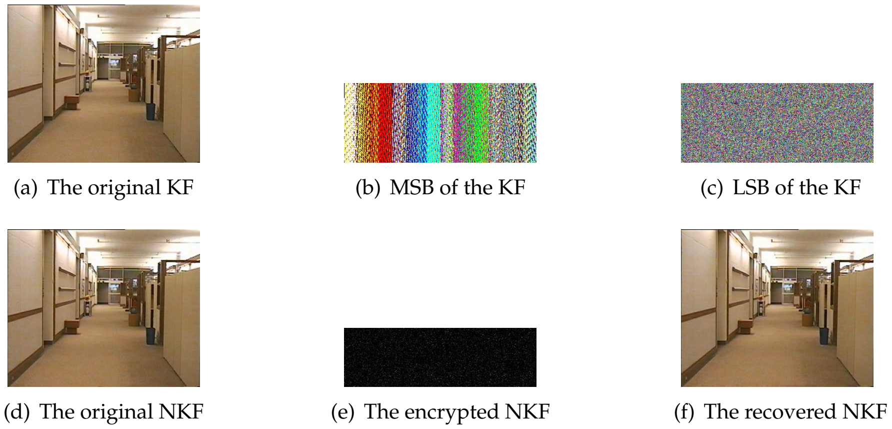
Finally, transmit the encrypted NKF to the cloud.

The decoding process of NKF is decryption-then-reconstruction. Decryption and encryption are inter-reversible and the secret key α_0, β_0, μ must be unified. The total variation minimization by augmented Lagrangian and alternating direction algorithm (TVAL3) [36] is used for reconstruction. At last, the recovered deviations plus the decrypted KF can obtain the corresponding decoded NKF.

4. Simulation Results and Performance Evaluations

4.1. Experimental Results

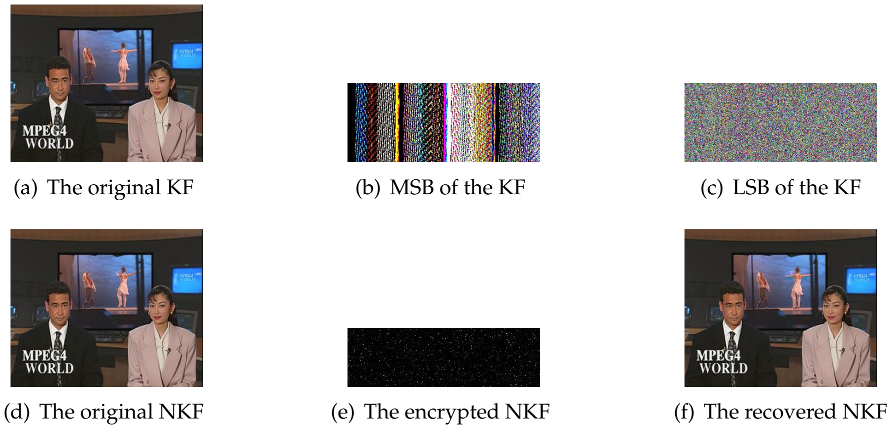
In this paper, our proposed scheme is encoded and decoded by MATLAB 2016a programming software. Hall(CIF), News(CIF) and Foreman(CIF) with different motion types are applied to simulate our scheme reliably. Figure 6a,d show the original 1st KF and 2nd NKF of Hall(CIF), respectively. Figure 6b denotes MSB of the KF and Figure 6c is LSB of that. Figure 6e is the encrypted NKF. The first-layer PCS adopts $\gamma_R = 0.3$, $\gamma_G = 0.25$ and $\gamma_B = 0.2$ while the second-layer PCS employs $\gamma = 0.5$. Figure 6f is the reconstructed NKF and the peak signal to noise ratio (PSNR) value reaches up to 35.68. It can be seen that the reconstruction performance is satisfying with the overall sampling rate 0.125. Similarity, Figure 7 represents simulation results of KF and NKF in the first GOP of News(CIF), and Figure 8 shows simulation results of KF and NKF in the first GOP of Foreman(CIF).



(a) The original KF (b) MSB of the KF (c) LSB of the KF

(d) The original NKF (e) The encrypted NKF (f) The recovered NKF

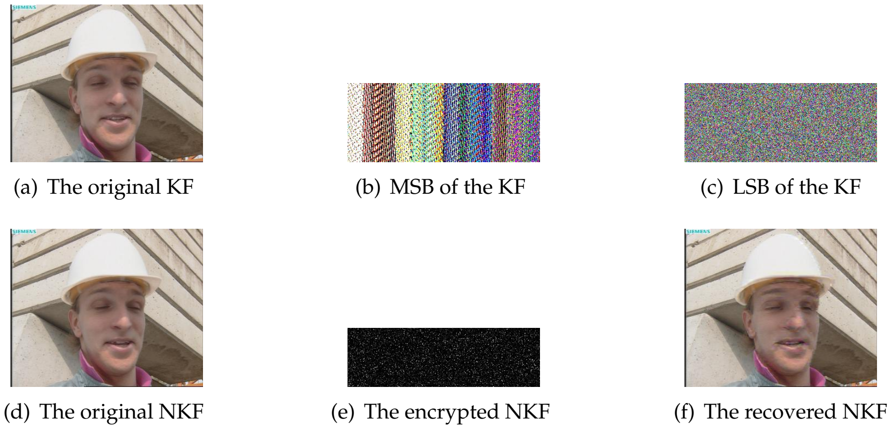
Figure 6. The simulation results of Hall(CIF).



(a) The original KF (b) MSB of the KF (c) LSB of the KF

(d) The original NKF (e) The encrypted NKF (f) The recovered NKF

Figure 7. The simulation results of News(CIF).



(a) The original KF (b) MSB of the KF (c) LSB of the KF

(d) The original NKF (e) The encrypted NKF (f) The recovered NKF

Figure 8. The simulation results of Foreman(CIF).

4.2. Theoretical Security Analysis

The security analysis of video data storage based on the hierarchical edge computing can be analyzed from two aspects. From the perspective of KF, although the local individuals have full control over the edge computing devices and can rely on the cloudlets to manage data, cipher-data are stored to prevent an attacker who obtains the data by force. In the field of reversible data hiding, the LSB layers of the cover image are usually replaced by significant information to ensure that no change in the cover image is visible to the naked eye. It indicates that the important data of an image is located in the MSB layers. Based on this principle, we divide KF into the MSB layers and LSB layers equally.

Compared with the random matrix generated by the key to diffuse the LSB layers, directly regarding the MSB layers as the key stream is far more secure and even does not need to provide the extra space to store the key. Besides, two secret keys with only one bit difference can encrypt a certain frame into two different cipher-frames by bit adaptive diffusion. So our secure scheme for KF has strong capability of resisting famous attacks, such as differential attack and chosen-plaintext attack.

The NKF, which occupies a large part of videos, have to be stored in the completely untrusted public cloud. So the privacy and compression should be considered at the same time. In order to achieve the above goal without increasing computation complexity, we directly adopt the two-layer PCS with controlled sampling rates. To be more specific, in the first compression process, the three-layer RGB employs different sampling rates so that the correct composition proportion of the 1D plane formed by combination could not be known absolutely. To further reduce the storage, the second compression is adopted. Besides, instead of processing NKF directly, the main information is removed by subtraction in order to avoid the sensitive data leakage. We also use 2D logistic-skew tent map to encrypt measurement values further to improve the performance of privacy preservation.

In short, our proposed scheme not only provides effective and efficient privacy protection for big video storage based on the hierarchical edge computing, but also does not add additional burden from both computation and storage aspects of edge computing and the public cloud.

4.3. Computation Complexity

Table 1 shows that the average encoding time required for MSB is 0.106 s and for LSB is 0.841 s of any KF in News(CIF). As part encoding stages of MSB and LSB can be carried out parallelly, the total encoding time of KF is generally less than 0.7 s. Besides, the average decoding time of KF is about 1 s. For NKF, as shown in Tables 2 and 3, the average run-time of the whole encoding is only 0.113 s, but the decoding time is long due to higher iterative complexity of CS reconstruction. But the performance of existing non-iterative reconstruction algorithm can be optimized to greatly reduce the run-time. Most importantly, all frames of the video stream can be encoded simultaneously, that is to say, the total encoding time of the video stream is no more than 1 s in our proposed scheme, which indicates that our scheme has higher efficiency and low complexity.

Table 1. Average run-time (s/frame) performance of KF in our proposed scheme.

	Encoding	**Decoding**
MSB	0.106	0.123
LSB	0.841	0.905

Table 2. Average run-time (s/frame) performance of encoding NKF in our proposed scheme.

The First PCS	**The Second PCS**	**Encryption**
0.017	0.035	0.061

Table 3. Average run-time (s/frame) performance of decoding NKF in our proposed scheme.

Decryption	**The First Reconstruction**	**The Second Reconstruction**
0.05	29.09	31.72

4.4. Comparison

Table 4 shows the performance comparison among our proposed scheme and other relevant ones. It can be clearly seen that the proposed scheme has its unique merits.

Table 4. Compared with the relevant privacy protection schemes.

Schemes	Produce Redundant Data	Compression	Complexity	Application Scenarios
Ours	No	Yes	Low	Cloud storage
[17]	No	No	Medium	Date aggregation
[18]	Yes	No	Low	Cloud storage

5. Conclusions

In this paper, we take full advantage of three patterns (MEC, cloudlets and fog computing) of edge computing to design the hierarchical edge computing. Based on this architecture, we further propose a novel smart privacy preservation scheme for big video data storage. For KF, MSB are stored directly in local sensor devices while LSB are encrypted by MSB and then sent to cloudlets. For NKF, two-layer PCS and encryption are performed at first, and finally transmitted to the cloud service. Experimental results and theoretical analysis prove that our proposed scheme is effective, efficient and lower-complexity, which provides smart privacy-protection for video contents.

Author Contributions: D.X., M.L. and H.Z. conceived the mechanism design; D.X. and M.L. wrote and revised the paper. All authors have read and agreed to the published version of the manuscript.

Funding: The work was funded by the National Natural Science Foundation of China (Grant Nos. 61572089, 61633005), the Chongqing Research Program of Basic Research and Frontier Technology (Grant No. cstc2017jcyjBX0008) and the Chongqing Postgraduate Education Reform Project (Grant No. yjg183018).

Acknowledgments: We thank the editor and anonymous reviewers for their diligent work on our paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Mell, P.; Grance, T. The NIST Definition of Cloud Computing (Draft). *NIST Spec. Publ.* **2011**, *800*, 145.
2. Zhu, W.; Luo, C.; Wang, J.; Li, S. Multimedia cloud computing. *IEEE Signal Process. Mag.* **2011**, *28*, 59–69. [CrossRef]
3. Deng, Z.; Ren, Y.; Liu, Y.; Yin, X.; Shen, Z.; Kim, H.J. Blockchain-based trusted electronic records preservation in cloud storage. *Comput. Mat. Contin.* **2019**, *58*, 135–151. [CrossRef]
4. Wang, B.; Kong, W.; Guan, H.; Xiong, N.N. Air Quality Forecasting Based on Gated Recurrent Long Short Term Memory Model in Internet of Things. *IEEE Access* **2019**, *7*, 69524–69534. [CrossRef]
5. Liu, D.; Yan, Z.; Ding, W.; Atiquzzaman, M. A Survey on Secure Data Analytics in Edge Computing. *IEEE Internet Things J.* **2019**, *6*, 4946–4967. [CrossRef]
6. Shi, W.; Cao, J.; Zhang, Q.; Li, Y.; Xu, L. Edge computing: Vision and challenges. *IEEE Internet Things J.* **2016**, *3*, 637–646. [CrossRef]
7. Wang, T.; Wang, P.; Cai, S.; Ma, Y.; Liu, A.; Xie, M. A Unified Trustworthy Environment based on Edge Computing in Industrial IoT. *IEEE Trans. Ind. Inform.* **2019**. [CrossRef]
8. Khan, W.Z.; Ahmed, E.; Hakak, S.; Yaqoob, I.; Ahmed, A. Edge computing: A survey. *Futur. Gener. Comp. Syst.* **2019**, *97*, 219–235. [CrossRef]
9. Mao, Y.; You, C.; Zhang, J.; Huang, K.; Letaief, K.B. A survey on mobile edge computing: The communication perspective. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2322–2358. [CrossRef]
10. Jo, B.; Piran, M.J.; Lee, D.; Suh, D.Y. Efficient Computation Offloading in Mobile Cloud Computing for Video Streaming Over 5G. *Comput. Mat. Contin.* **2019**, *61*, 439–463. [CrossRef]
11. Shaukat, U.; Ahmed, E.; Anwar, Z.; Xia, F. Cloudlet deployment in local wireless networks: Motivation, architectures, applications, and open challenges. *J. Netw. Comput. Appl.* **2016**, *62*, 18–40. [CrossRef]
12. Bao, W.; Yuan, D.; Yang, Z.; Wang, S.; Li, W.; Zhou, B.B.; Zomaya, A.Y. Follow me fog: Toward seamless handover timing schemes in a fog computing environment. *IEEE Commun. Mag.* **2017**, *55*, 72–78. [CrossRef]
13. Kang, L.W.; Lu, C.S. Distributed compressive video sensing. In Proceedings of the 2009 IEEE International Conference on Acoustics, Speech and Signal Processing, Taipei, Taiwan, 19–24 April 2009.
14. Hua, Z.; Yi, S.; Zhou, Y. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process.* **2018**, *144*, 134–144. [CrossRef]

15. Laue, H.E.A. Demystifying compressive sensing [Lecture notes]. *IEEE Signal Process. Mag.* **2017**, *34*, 171–176. [CrossRef]
16. Fang, H.; Vorobyov, S.A.; Jiang, H.; Taheri, O. Permutation meets parallel compressed sensing: How to relax restricted isometry property for 2D sparse signals. *IEEE Trans. Signal Process.* **2013**, *62*, 196–210. [CrossRef]
17. Lyu, L.; Nandakumar, K.; Rubinstein, B.; Jin, J.; Bedo, J.; Palaniswami, M. PPFA: Privacy preserving fog-enabled aggregation in smart grid. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3733–3744. [CrossRef]
18. Wang, T.; Zhou, J.; Chen, X.; Wang, G.; Liu, A.; Liu, Y. A three-layer privacy preserving cloud storage scheme based on computational intelligence in fog computing. *IEEE Trans. Emerg. Top. Comput. Intell.* **2018**, *2*, 3–12. [CrossRef]
19. Xue, K.; Hong, J.; Ma, Y.; Wei, D.S.; Hong, P.; Yu, N. Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing. *IEEE Netw.* **2018**, *32*, 7–13. [CrossRef]
20. Gu, B.; Wang, X.; Qu, Y.; Jin, J.; Xiang, Y.; Gao, L. Context-Aware Privacy Preservation in a Hierarchical Fog Computing System. In Proceedings of the 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 20–24 May 2019.
21. Wang, B.; Kong, W.; Li, W.; Xiong, N.N. A dual-chaining watermark scheme for data integrity protection in Internet of Things. *Comput. Mat. Contin.* **2019**, *58*, 679–695. [CrossRef]
22. Wang, T.; Mei, Y.; Jia, W.; Zheng, X.; Wang, G.; Xie, M. Edge-based differential privacy computing for sensor–cloud systems. *J. Parallel Distrib. Comput.* **2020**, *136*, 75–85. [CrossRef]
23. Wang, T.; Bhuiyan, M.Z.A.; Wang, G.; Qi, L.; Wu, J.; Hayajneh, T. Preserving Balance between Privacy and Data Integrity in Edge-Assisted Internet of Things. *IEEE Internet Things J.* **2019**. [CrossRef]
24. He, S.; Zeng, W.; Xie, K.; Yang, H.; Lai, M.; Su, X. PPNC: Privacy Preserving Scheme for Random Linear Network Coding in Smart Grid. *KSII Trans. Internet Inf. Syst.* **2017**, *11*, 1510–1532.
25. Xie, K.; Ning, X.; Wang, X.; He, S.; Ning, Z.; Liu, X.; Wen, J.; Qin, Z. An efficient privacy-preserving compressive data gathering scheme in WSNs. *Inf. Sci.* **2017**, *390*, 82–94. [CrossRef]
26. Gu, K.; Yang, L.; Yin, B. Location Data Record Privacy Protection based on Differential Privacy Mechanism. *Inf. Technol. Control.* **2018**, *47*, 639–654. [CrossRef]
27. Bonomi, F.; Milito, R.; Zhu, J.; Addepalli, S. Fog computing and its role in the internet of things. In Proceedings of the First Edition of The MCC Workshop on Mobile Cloud Computing, Helsinki, Finland, 13–16 August 2012.
28. Hu, Y.C.; Patel, M.; Sabella, D.; Sprecher, N.; Young, V. Mobile edge computing—A key technology towards 5G. *ETSI White Paper* **2015**, *11*, 1–16.
29. Satyanarayanan, M.; Bahl, P.; Caceres, R.; Davies, N. The case for vm-based cloudlets in mobile computing. *IEEE Pervasive Comput.* **2009**, *8*, 14–23. [CrossRef]
30. Mora-Gimeno, F.J.; Mora-Mora, H.; Marcos-Jorquera, D.; Volckaert, B. A secure multi-tier mobile edge computing model for data processing offloading based on degree of trust. *Sensors* **2018**, *18*, 3211. [CrossRef]
31. Lee, J.; Lee, J. Hierarchical mobile edge computing architecture based on context awareness. *Appl. Sci.* **2018**, *8*, 1160. [CrossRef]
32. Dong, C.; Wen, W. Joint optimization for task offloading in edge computing: An evolutionary game approach. *Sensors* **2019**, *19*, 740. [CrossRef]
33. Lee, J.; Kim, D.; Lee, J. Zone-based multi-access edge computing scheme for user device mobility management. *Appl. Sci.* **2019**, *9*, 2308. [CrossRef]
34. Chen, C.; Ding, F.; Zhang, D. Perceptual hash algorithm-based adaptive GOP selection algorithm for distributed compressive video sensing. *IET Image Process.* **2017**, *12*, 210–217. [CrossRef]
35. Ravelomanantsoa, A.; Rabah, H.; Rouane, A. Compressed sensing: A simple deterministic measurement matrix and a fast recovery algorithm. *IEEE Trans. Instrum. Meas.* **2015**, *64*, 3405–3413. [CrossRef]
36. Li, C. An Efficient Algorithm for Total Variation Regularization with Applications to the Single Pixel Camera and Compressive Sensing. Ph.D. Thesis, Rice University, Houston, TX, USA, 2010.

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).