Hindawi
Complexity
Volume 2019, Article ID 1625678, 11 pages
https://doi.org/10.1155/2019/1625678

Research Article

An Efficient Cryptosystem for Video Surveillance in the Internet of Things Environment

Rafik Hamza,[1,2] **Alzubair Hassan**,[1] **Teng Huang**,[1] **Lishan Ke**,[3] **and Hongyang Yan**[1]

[1]*School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou, China*
[2]*Peng Cheng Laboratory, Shenzhen, 518055 Guangdong, China*
[3]*Department of Mathematics, Guangzhou University, Guangzhou, China*

Correspondence should be addressed to Rafik Hamza; rafik.hamza@hotmail.com

Received 17 August 2019; Accepted 11 November 2019; Published 9 December 2019

Guest Editor: Xuyun Zhang

Surveillance systems paradigm envisions the pervasive interconnection and cooperation of interactive devices over the Internet infrastructure. Nevertheless, dissemination and processing of surveillance video amid the Internet of Things (IoT) applications become a susceptible issue due to the large volume and the significant information of these data. Moreover, surveillance devices on IoT have very limited resources such as memory and storage. The actual security methods are not quite appropriate for surveillance IoT systems. Thus, a particular cryptosystem technique is required for surveillance data security. In this paper, we propose an efficient cryptosystem to secure IoT-based surveillance systems. The proposed cryptosystem framework contains three parts. First, a lightweight automatic summarization technique based on a fast histogram-clustering approach is used to extract the keyframes from the surveillance video. Then, we employ a discrete cosine transform (DCT) technique to compress the extracted data size. Finally, the proposed framework performs an efficient image encryption algorithm by employing a discrete fractional random transform (DFRT). The testing results and analysis confirm the features of the proposed cryptosystem on surveillance systems. The proposed framework is fast and ensures secure and efficient real-time processing by minimizing the transmission cost and storage.

1. Introduction

Digital technology IoT-based becomes an integral part of strategy formulations in human life [1]. In this regard, IoT systems have high operating costs with limited resources. IoT systems generate large volumes of data although only small parts from these data contain really useful information, especially with video data such as surveillance systems. IoT-based machine learning and cryptography techniques are receiving a lot of attention because IoT needs to be distrusted and complemented by new smart frameworks [2, 3]. Accordingly, the researchers have proposed different machine learning techniques such as smart mobile devices [4–6], blockchain-based smart vehicles [7], and analytics techniques in big data such as anomaly detection [8]. Mainly, the idea is to collect smart data with efficiency using machine learning techniques within different environments [9, 10].

Surveillance video data impose large processing computations, especially to identify the informative scenes and objects. The surveillance system needs to inform the data center monitoring in real-time or execute an automatic action such as turn on the light. On the one hand, surveillance devices on IoT have very limited resources such as memory and storage. On the other hand, the surveillance system generates a huge amount of data that require real-time processing. To deal with computational complexity, some researchers propose several contributions such as video summarization techniques [11, 12]. The main task of these techniques is to summarize the most informative parts of video data. Video summarization techniques pick out image-based branches in order to identify abbreviated keyframes [13, 14].

The fast growth of cloud computing boosts a broad deployment of data and computation outsourcing to cloud

providers by resource-limited devices [15–17]. Thus, an efficient cryptosystem scheme is highly recommended to encrypt the sensitive data before outsourcing [18]. In this regard, several encryption techniques have been proposed using various approaches [12, 19–21]. Yet, some techniques lack robustness resistant. For example, a symmetric encryption scheme [22] is proposed to secure IoT surveillance systems using stream cipher with chaotic-PRNG. However, in a case of losing some pixels of the encrypted image (due to noise and cropping attacks), retrieving the plain image could be impossible. Another aspect is using mathematical transformation for image encryption which can resist the noise and cropping attacks. So, further in-depth analyses to select the appropriate cryptosystem for a surveillance system are necessary.

The researchers use DFRNT for image encryption [12, 23, 24], providing a secure scheme to encrypt the digital image. Yet, some techniques failed to eliminate the correlation coefficients of adjacent pixels in the encrypted images. The presented related works' performances illustrate the lack of efficiency, especially with the space of keys and security properties. Motivated by the abovementioned research, an efficient and secure encryption-compression scheme for secure IoT surveillance systems is proposed in this paper. We extend the DCT-DFRT algorithm from our previous work [25] by giving detailed algorithms that guarantee a high level of security with excellent performances for secure IoT surveillance environments.

This paper proposes a cryptosystem framework based on the summarization technique using compression and encryption schemes. A video summarization technique is used to identify the informative keyframes and reduce the video redundancy based on the presented technique in Wu et al. [11]. Accordingly, we compress the extracted frames by applying DCT. It is possible to compress multiple frames by reconstructing the keyframes into spectra by applying DCT. Then, the spectra are cut and divided using Zigzag scanning into a composite spectrum [26]. After compressing the keyframes, the proposed framework encrypts the compressed data using a lightweight image encryption scheme. In this part, Chen's chaotic map is employed to generate two random keys: one key is to confuse the image pixels (a permutation process) and the second key is a random matrix employed in a discrete fractional random transform. The proposed cryptosystem has the ability to compress-encrypt multiple images once. The main secret keys of the proposed cryptosystem are the initial values and parameters of the PRNG and the order of DFRT.

To sum up, we listed the main contributions of this work as follows:

(i) This paper proposes a cryptosystem framework based on a cluster summarization technique with compression and encryption algorithms

(ii) The proposed cryptosystem requires low computational power and decreased bandwidth and storage terms

(iii) The proposed cryptosystem uses randomized keys (instead of a static block cipher) based on Chen's chaotic map

(iv) The proposed cryptosystem can encrypt multiple frames once instead of one-to-one traditional encryption

This paper is organized as follows. Section 2 presents the proposed IoT surveillance cryptosystem. Section 3 explains the evaluation and experimental results. Finally, Section 4 presents a conclusion and some perspectives for future research.

2. The Proposed Framework for Surveillance Systems

In this work, we take into consideration the requirements of modern cryptographic application including the level of security, implementation, and the cost of the proposed framework. The main aim is to guarantee an efficient framework to secure the transmission of extracted keyframes. Thus, we employ a video summarization technique to eliminate the redundancy and identify the informative keyframes. The proposed framework reduces the extracted keyframe size and encrypts them using a lightweight cryptosystem scheme. This will minimize the waste of time to skim the surveillance video to identify the actions and events such as fire detection and unusual activities. Hence, the cryptosystem guarantees data security prior to transmission and minimizes the resource used by the system.

2.1. Keyframes Extraction Technique. Dissemination of video data over the Internet is a susceptible issue due to the large volume and its significant information among these data. Video confidentiality becomes one of the challenging problems nowadays [22]. One of the common ways to record videos is by using surveillance camera systems. As known, most of the video surveillance contain sensitive data with distinguishing visual representations for almost everything in our life. Industrial surveillance systems capture visual images using sensors, producing a large volume of video with high-resolution frames [27]. Furthermore, these surveillance systems could capture noninformative data [14]. For example, most of the video data during the night have noninformative data with a large amount of redundant information. However, sometimes the captured video data contain a significant amount of redundant and noninformative images. Furthermore, modern surveillance cameras require high bandwidth and power. Video surveillance systems have limited processing capabilities and lack to be adaptive for IoT systems [28].

Principally, the modern surveillance systems transfer the video data to intermediary servers and storage systems via the Internet [28]. For instance, Figure 1 depicts a network of different cameras which capture video data with devices such as user camera, adapted from Rajpoot and Jensen [28].

Most of the surveillance systems send the captured video data through the communication channels for real-time monitoring and processing or send them directly to a cloud host. However, video processing is impractical due to the fact of the huge data volume. Furthermore, energy and

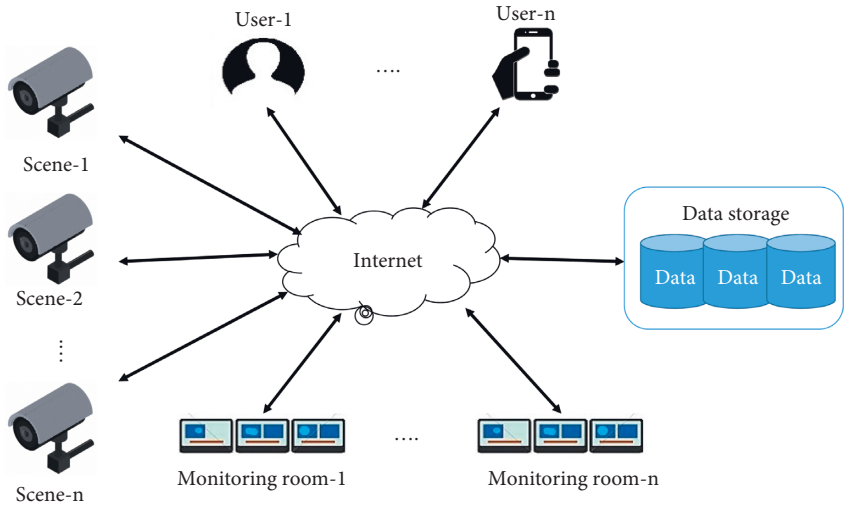


Figure 1: The architecture of a video surveillance system.

bandwidth constraints cannot allow for real-time processing because of video processing complexity [22]. For example, the size of an uncompressed RGB video is around 82.9 GB (contains [640, 480] pixels with a duration of 60 minutes and 25 fps). Even with small volume video data, there will be additional employment of the network resources to process and send the video data. Thus, it is highly recommended employing an automatic technique to reduce the volume and quantity of the collected video from a surveillance system.

To overcome these tackles, we employ a video summarization technique based on the K-means algorithm and histogram values of the frames. A fast data extraction based on an automatic video summarization technique is proposed in this part based on the related work [11]. The aim is to detect the important frames and preview a summarized version of a long video. This will enhance the efficiency of detecting real-time events and make decisions at the right time. K-means algorithm divides the frames into separated clusters using their color histogram. The proposed extraction starts with the presampling of the frames and then frame representation. Finally, cluster and identify the keyframes using K-means clustering. Figure 2 presents the steps of the keyframe extraction technique using K-means clustering and HSV Histograms.

Recently, several research studies have been proposed to extract keyframes based on different techniques such as the clustering algorithm [11]. The keyframes represent the summary of a video by formulating a video summarization task as a clustering problem. Similarly, the work of frame extraction is obtained by K-Means clustering with histograms in HSV color space. Despite the challenges of frames detection, this approach can identify keyframes that are extremely important and produce representative clusters automatically. As mentioned above, Figure 2 shows the frame detection framework based on the HSV clustering.

The following points sum up the steps to extract the keyframes from a video. Accordingly, the input is an original video and the output will be set of frames denoted as keyframes.

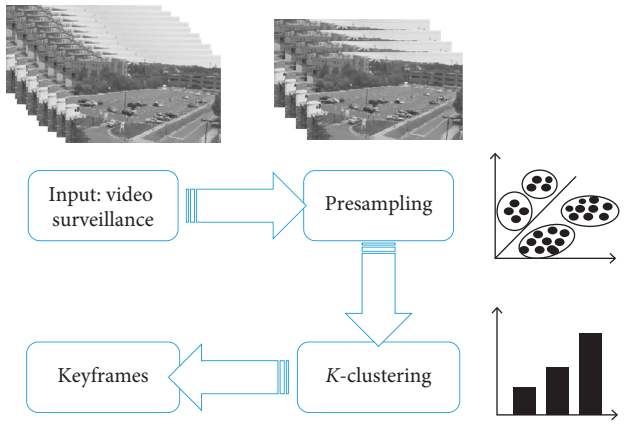


Figure 2: Keyframe extraction technique using K-means clustering and HSV histograms.

(i) Since the video contains large number of frames per second (25 f/s), we first reduce this number to 8. According to Ref [29], it requires at least 8 frames per second to observe the impact of frame rates in a CCTV task.

(ii) We analyze every 100 frames uniformly from the video. This means that we sample 100 frames for each summary process. Obviously, if we decrease the sampling number, we would get better results. However, it will consume more time and the proposed framework will be of higher complexity. The sampling number can be modified depending on the frames number.

(iii) We employ the K-means clustering to extract the keyframes from the input video. First, it is required to perform the K-means clustering inputs.

Thus, we need to create feature vectors based on HSV Histograms. Thus, we convert the space of extracted frames from step one to HSV space. We perform three histograms

for each frame, resembling the hue, saturation, and intensity values.

Now, we compute the value of K for the clustering algorithm for the video. We determine a threshold value between each pair of frames based on pairwise Euclidean distance. Also, the peak number represents the number of significant changes in a frame. To compute the value of K, we add one to the number of peaks above the threshold value.

We use HSV space due to the fact that this color space is a better image descriptor compared to other colors' space such as RGB.

In the proposed framework, a clustering-based method used different low-level features to differentiate between the frames and extract keyframes. This technique is fast and gives accurate results according to previous works. The clustering algorithm used to create clusters of frames based on colors histogram (feature vectors), including hierarchical clustering. However, it is hard to guarantee the video security due to its special features such as huge size and volume. Thus, we employ fast selective compression-encryption technique, reducing the size of frames, and ensure fast transmission.

2.2. A Lightweight Cryptosystem. Visual surveillance networks become widespread, generating enormous amounts of data daily. Due to the high requirements of video data, most of the existing security techniques cannot perform complex data processing in real-time. The existing projects show that it is required to adjust the existing security schemes and techniques for use in IoT systems [30]. Thus, surveillance IoT applications are required to employ compression techniques to minimize the restrictions of bandwidth, energy, and data storage. Generally, the compression technique requires higher computational power and higher energy consumption to achieve a high-compression rate [31]. Nevertheless, the DCT techniques have decreased the amount of computation and enhance energy performance by minimizing some accuracy in the compression [31, 32], resulting in decreased bandwidth and storage requirement for the surveillance IoT systems.

The following steps illustrate the cryptosystem mechanism using the chaotic system and DFRT. The Chen chaotic system is used to encrypt keyframes with the confusion and diffusion process. First, we compress the keyframes using DCT and the spectrum is compressed by spectrum cutting. We employ the DCT due to its energy properties with limited resources devices [31]. Next, we employ a secure and fast pseudorandom number algorithm [33] to produce a random matrix for the discrete fractional random transform (DFRT) [34]. Figure 3 illustrates the steps of the proposed cryptosystem framework in detail.

Note that the proposed cryptosystem can compress multiple frames as follows. The frames are transformed into spectra via the discrete transform (cosine or sine). Then, the cryptosystem should cut the spectra and splice into a combined spectrum using Zigzag scanning.

To sum up, we listed the steps of the proposed framework after getting the keyframe as follows.

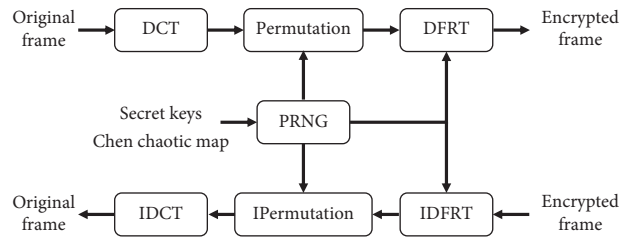


Figure 3: The proposed cryptosystem based on DFRT and PRNG.

(i) Step 1. Collect the keyframe and input the secret keys of the proposed cryptosystem. Note that an RGB keyframe can be encrypted using the proposed cryptosystem in Section 2 by reshaping the matrices [N, M, 3] into two-dimensional formats [3 ∗ N, M]. Next, we apply the following compression-encryption steps.

(ii) Step 2. The obtained keyframe is transformed into a spectrum by the DCT algorithm. The front part of the elements implies the main information to be encrypted is contained in the DC component (such as the low-frequency part of the image). The compressed spectrum will be encrypted using DFRT in step 5 after applying the permutation step.

(iii) Step 3. Produce two sets of random numbers (S_1 and S_2) using a secure PRNG [33]. The Chen chaotic system is elaborated mathematically by the following equations:

$$\begin{cases} \dot{x} = ay - ax, \\ \dot{y} = cx - ax + cy - xz, \\ \dot{z} = xy - bz, \end{cases} \tag{1}$$

where x, y, and z are the random sequences of this map, and a, b, and c are the control parameters. We use Runge–Kutta step 0.01, with iteration of the chaotic map for $1 + (n/3)$ times to obtain x_i, y_i, and z_i. Accordingly, the length of each sequence should around to $k = (n/3)$. The proposed PRNG get three random sequences denoted as S_1, S_2, and S_3:

$$\begin{cases} P(3 \cdot i) = \gamma_1 \cdot 221 \cdot x, \\ P(3 \cdot i + 1) = \gamma_2 \cdot 213 \cdot y, \\ P(3 \cdot i + 2) = \gamma_3 \cdot 231 \cdot z, \\ i = 0, 1, 2, 3, \ldots, k, \end{cases} \tag{2}$$

where $x(i)$, $y(i)$, and $z(i)$ are the samples from the Chen chaotic system, γ_1, γ_2, and γ_3 are arithmetic mean for the absolute values of chaotic sequences x_i, y_i, and z_i, respectively, k is length of one of the orbits x, y, and z. The one-dimensional sequence P_i has real numbers. Now, we transform P_i into integer sequences S using the following equation:

$$S = \text{round}|P| \bmod 255. \tag{3}$$

(iv) Step 4. The permutation step is based on an index sort of generated sequence, allowing to confuse the

pixels. It is possible to perform Zigzag scanning to compress multiple frames after this step. However, this step is not necessary for the cryptosystem process.

(v) Step 5. A discrete fractional random transform is performed after step 4 with the fractional order as the key of DFRT. The discrete fractional random transform of a two-dimensional signal I is

$$E_R = H^{\alpha} I \left(H^{\alpha}\right)^T. \tag{4}$$

Here, the fractional order is α, E_R is the kernel transform of DFRT, and the transpose of (H^P) is $(H^P)^T$.

The transform kernel is pseudorandom due to the use of the chaotic matrix I from S_1.

The kernel transform (H^P) is defined as follows:

$$H^{\alpha} = \Gamma D^{\alpha} (\Gamma)^T, \tag{5}$$

where Γ is the eigenvector basis, while, Γ^T is the transpose of Γ. Note that $\Gamma(\Gamma^T) = I.D^P$ is an $N \times N$ diagonal matrix:

$$\mathbf{D}^{\alpha} = \operatorname{diag}\left\{1,\ \exp\left(-\frac{i2\pi\alpha}{T}\right),\ \exp\left(-\frac{i4\pi\alpha}{T}\right), \ldots,\ \exp\left[-\frac{i2(N-1)\pi\alpha}{T}\right]\right\}. \tag{6}$$

In this part, the positive number $T$is the period of DFRT:

$$E = \frac{P + P^t}{2}. \tag{7}$$

The final encryption image C can be obtained by performing a discrete fractional random transform which is expressed as follows:

$$C = \arg\left(\exp\frac{R^{\alpha} i\pi C}{255}\right), \tag{8}$$

where C is the final encrypted image and R^{α} is the kernel transform matrix of the DFRT by equations (4)–(8) and the generated sequences of PRNG based on Chen's chaotic map.

Note that the decryption algorithm is similar to the encryption process with the reverse order. The inverse DFRT step can be obtained with fractional orders $-\alpha$ using the following equation:

$$D = 255 \times \left(\arg\frac{\exp(R^{-\alpha} iC)}{\pi}\right). \tag{9}$$

Due to the use of the chaotic matrix in encrypting the keyframes, the transform kernel of DFRT will produce random output. The architecture of the proposed cryptosystem based on PRNG and DFRT is shown in Figure 3.

3. Evaluation

We list the experimental results based on different tests and analyses in this section. We evaluate the performances of the proposed cryptosystem using various images [35, 36] with Matlab (R2017b). Based on the results of the related work [11], the precision of extracting the keyframes are varied depending on the databases. The efficiency of extracting the keyframes depends on the surveillance video. So, precision can be low with similar scenes videos and high with different scenes. The proposed algorithm has the ability to compress and encrypt multiple keyframes together (three frames once). First, the extracted frames from the surveillance system are reconstructed into spectra by applying DCT. Then, the spectra are cut and divided using Zigzag scanning into a composite spectrum [26]. The following values have been used as secret keys for the proposed cryptosystem $\alpha = 0.2, x_0 = -1.2, y_0 = 0.7, z_0 = 14, a = 35, b = 3$, and $c = 28$.

Table 1: Keyspace comparison.

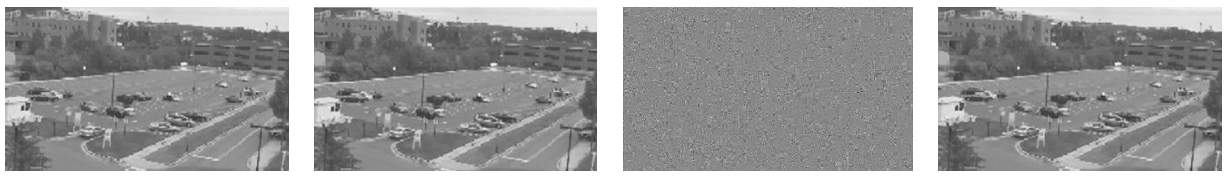
Algorithm	Keyspace
Our cryptosystem	2^{300}
Gong et al. [12]	2^{187}
Zhou et al. [23]	2^{300}
Zhang and Tong [37]	2^{256}
Zhu and Zhu [38]	2^{280}

3.1. Security Analysis. The fractional order in DFRT and the initial parameters of the Chen chaotic system are selected as secret keys. The chaotic maps are known by the sensibility of its initial values and controlling parameters. Accordingly, we can estimate the keyspace based on this sensibility evaluation of the selected secret keys (α, x_0, y_0, z_0, a, b, and c). The keys should be sensitive enough to change the encrypted data. This means that any adjustment of the secret keys (equal to or larger than 10^{-15}) should change completely the encrypted data. Thus, we can estimate that the keyspace for a chaotic sequence is around $10^{90} \simeq 2^{300}$. This is the minimum space key that can be considered in our proposed framework. For example, if the system selects generating two sequences S_1 and S_2 with two different secret keys, the keyspace, in this case, will be more than 2^{600}. The keyspace is large enough to withstand any brute force attack to detect the secret keys and can resist all exhaustive attacks [37]. Table 1 presents the comparison result. The keyspace in our cryptosystem is larger than the existing state-of-art cryptosystem [12, 23, 37, 38].

In this part, we present the visual results based on our implementation. Figure 4 shows the extracted keyframe from the surveillance video followed by the compressed frames and the encrypted keyframe. We employed this simulation to demonstrate the ability of our proposed cryptosystem of securing keyframes and maintain its visual representation.

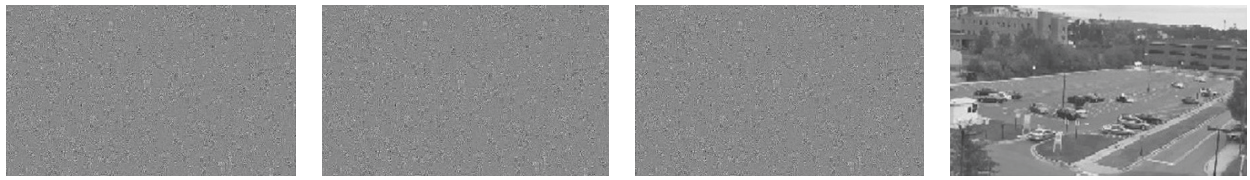
Figure 5 present a scenario of attacks, attempting to decrypt the encrypted data with different secret keys. In this scenario, we adjusted the original secret keys with a small change in one of the secret keys. So, the wrong secret keys' values close to the correct one differs only in one value and with a small number. The results show that any adjustment of any part of the secret keys will change completely the encrypted data. As a result, we can ensure that the proposed cryptosystem can withstand different attacks.

3.2. Compression Ratio. It is well known that the compression ratio measures the relative reduction in data size based on the compression technique [31, 32]. In this case, the compression ratio can be computed by comparing the uncompressed size



(a) (b) (c) (d)

Figure 4: Sample results of the proposed framework: keyframe (a), compressed keyframe without encryption step (b), encrypted keyframe (c), and the decrypted keyframe (d).



(a) (b) (c) (d)

Figure 5: Sample results of decryption with incorrect keys $(+10^{15})$. Modify the secret keys in α (a), x_0 (b), y_0 (c), and the decrypted frame using the correct secret key (d).

with the compressed size. Accordingly, we define the compression ratio (CR) using the following equation:

$$\mathrm{CR} = \frac{\mathrm{UnCompressed\ Frame}}{\mathrm{Compressed\ Frame}}. \tag{10}$$

The CR values should be higher than 1. This means that the size of the original data has been reduced. Otherwise, the size of the uncompressed image would be more than the original image (amplified data). The high CR values refer to good performances of compressing the data; however, it can also mean that the image compressed quality is too low. Therefore, any compression technique should pay attention to the balance between size reduction and image compressed quality.

The compression rate can be computed depending on the quality factor and DCT performances. Note that the maximum compression ratio should be around 30% from the original image so that the quality of the decrypted image will be visually acceptable. Accordingly, we listed the results of compressed images from the SIPI database. This is an explication of results based on our previous work [25]. Table 2 shows the results of the compression ratio of the selected images from this database. The proposed cryptosystem archives good performances and reduces the size of data representation, allowing to reduce the data storage and bandwidth requirements in processing and communication.

3.3. Randomness Analysis. The entropy analysis of the encrypted data is a very important test that allows us to examine the encrypted data randomness. Shannon's entropy [39] is presented as follows:

$$E(C) = -\sum_{i=1}^{n} P(c_i)\log_2 P(c_i). \tag{11}$$

Herein, $P(c_i)$ presents the probability of $c_i \in C$, C is an ensemble of symbol. The ideal score in this test is eight

Table 2: Compression ratio results.

Image name	Compression ratio
Airplane	3.29
Moon surface	3.79
Airplane	3.32
Aerial	3.21
Clock	3.06
Resolution chart	3.24
Chemical plant	3.19
Couple	3.11

Table 3: The local Shannon entropy tests.

Component	Plaintext	Encrypted
R	7.2576	7.91
G	7.0141	7.92
B	6.9113	7.98

according to Shannon, where the encrypted data should exhibit a uniform distribution. Table 3 shows the results of local Shannon entropy for plaintext data and its corresponding encrypted data. Additionally, the comparison with other state-of-art techniques [40, 41] is shown in Table 4. The results present that all the Shannon scores of the encrypted data are very close to 8, confirming the performance of the proposed cryptosystem. Our proposed cryptosystem managed to change the original data to random data with a uniform distribution.

3.4. Correlation Coefficient Analysis. The correlation coefficient analysis measures the correlation between adjacent pixels of an image. This means that this test determines the strength and direction of a linear relationship between two sources. Accordingly, we explore this test between two adjacent pixels of the encrypted and the original data.

Table 4: The local Shannon entropy comparison tests.

Algorithm	Entropy		
	Horizontal	Vertical	Diagonal
Lenna image	0.9849	0.9345	0.9226
Our cryptosystem	0.0019	0.025	0.0028
Gong et al. [12]	0.4968	0.4938	0.0480
Zhou et al. [40]	0.0119	0.0925	0.0325
Chen et al. [41]	−0.0016	−0.001	−0.0014

Table 5: The correlation coefficient analysis.

Component	Plaintext			Encrypted		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
R	0.9937	0.9901	0.9541	0.002	−0.027	0.002
G	0.9909	0.9834	0.9987	−0.07	0.0021	−0.0010
B	0.9931	0.9824	0.9801	0.003	−0.010	0.007

We randomly select 1024 adjacent pixel pairs to examine the two adjacent pixels' correlation from vertical, horizontal, and diagonal directions, respectively. The following equation (12) shows how the correlation of two adjacent pixels can be computed:

$$\mathrm{CC}_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)} \times D(y)}, \tag{12}$$

$$\mathrm{cov}(x, y) = \frac{1}{n} \sum_{i=1}^{n} \left(x_i - E(x)\right)\left(y_i - E(y)\right), \tag{13}$$

$$D(x) = \frac{1}{n} \sum_{i=1}^{n} \left(x_i - E(x)\right)^2, \tag{14}$$

$$E(x) = \frac{1}{n} \sum_{i=1}^{n} x_i. \tag{15}$$

Table 5 lists the numerical results of this test with a selected keyframe and the encrypted one for each red, blue, and green channel. The typical value of this test should be found CC = 0 [33] for a random source. Generally, the original data have a higher correlation between adjacent pixels with a score CC $\sim = 1$. The encrypted data should have noncorrelation coefficients with a score CC $\sim = 0$. This indicates that the pixels (of the plaintext) have been distributed uniformly. Hence, these results confirm the conclusion that the proposed cryptosystem reduces efficiently the correlation between adjacent pixels of the plaintext data.

3.5. Differential Attacks. Any cryptosystem should be able to withstand against the differential attacks. Accordingly, we employed the NPCR and UACI tests [42] to measure the resistant against the differential attacks. The typical score of these tests should be around NPCR = 99.61% and UACI = 33.44%, respectively, for the encrypted data [42]. NPCR and UACI tests employ the following equations:

Table 6: Results of NPCR and UACI test.

	0.05 level
Expected value NPCR	>99.5693%
Expected value UACI	33.2824–33.6447%
Our NPCR	99.5826
Our UACI	33.4213

$$\begin{aligned} \mathrm{NPCR}(C_1, C_2) &= \sum_{i,,j} \frac{S(i, j)}{D} \times 100\%, \\ \mathrm{UACI}(C_1, C_2) &= \sum_{i,,j} \frac{C_1(i, j) - C_2(i, j)}{255 \times D} \times 100\%. \end{aligned} \tag{16}$$

"D" denotes the number of pixels, whereas "S" is expressed by equation (14) as follows:

$$S(i, j) = \begin{cases} 0, & \mathrm{IF} C_1(i, j) = C_2(i, j), \\ 1, & \mathrm{Elsewise}. \end{cases} \tag{17}$$

Here, we compute NPCR and UACI scores between two encrypted data C_1 and C_2. First, we encrypt using the proposed cryptosystem framework two images J and I vary in one pixel. Then, we get the encrypted images C_1 and C_2. Finally, we apply NPCR and UACI tests using both C_1 and C_2. Table 6 presents some results for different sample images. The proposed cryptosystem demonstrates that each encryption generates completely different encrypted data. In other words, the proposed cryptosystem produces randomized encrypted images.

Based on the same approach above, we apply NPCR and UACI for the pair encrypted data. Table 6 presents the ideal score for these tests from Wu et al. [43]. To get accurate results, Table 6 presents the average result of 100 times. Figures 6 and 7 show the NPCR and UACI results for two encrypted images with theoretically critical values of NPCR and UACI. Most of NPCR and UACI values satisfy the theoretically critical values, and only some outliers are detected outside the expected range. It is clear that the obtained

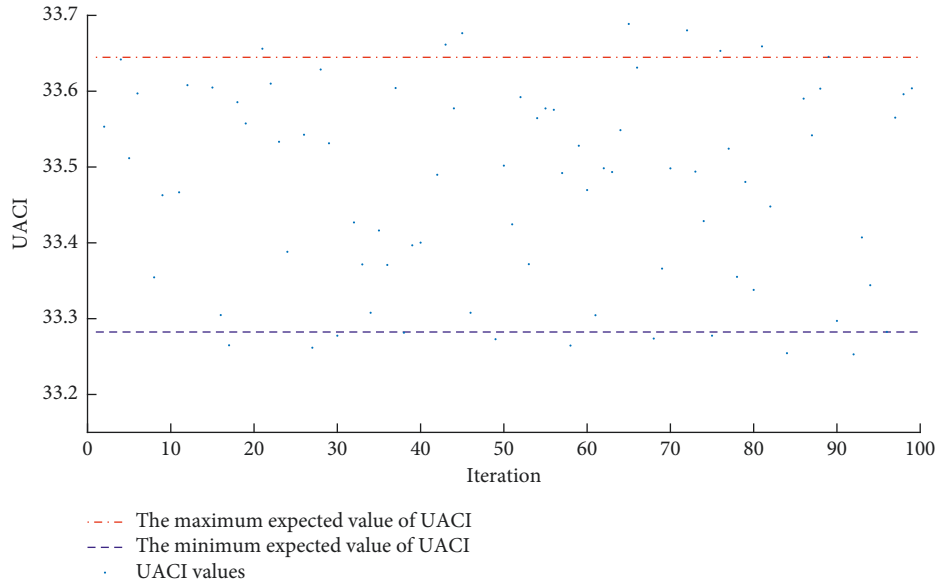


Figure 6: UACI results with 100 iterations.

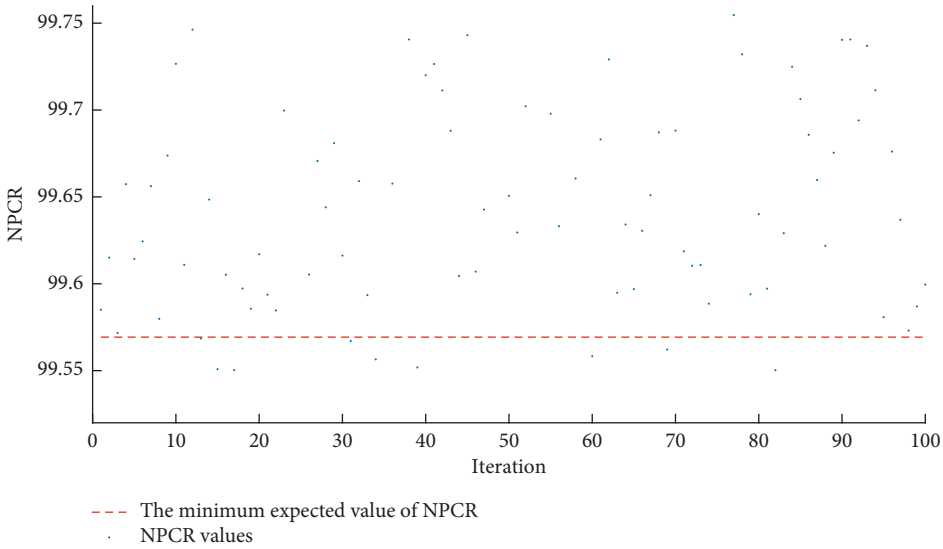


Figure 7: NPCR results with 100 iterations.

results are satisfactory and passed NPCR and UACI tests which match all theoretical expectations.

3.6. Robustness Analysis. In this section, we test the ability of the proposed cryptosystem against noise and cropping attacks. A strong cryptosystem should be able to reconstruct the plain image from not complete encrypted images or corrupted images. This test is simulated as follows. First, true random bits (noises) are embedded with the encrypted image:

$$C_0 = C + \beta W, \tag{18}$$

where C_0 is the encrypted images with noises, C is the encrypted images, β is the coefficient related to noise intensities, and W is the white Gaussian random (with zero mean and unit standard deviation).

Figures 8–10 show the results of attacks with $\beta = 5$, $\beta = 10$, and $\beta = 15$ noise intensities, respectively, while Figures 11 and 12 show results of attacks with different cropping sizes related to noise intensities, and W is the white Gaussian random data. As shown in Figures 8–10, the decrypted image can be distinguished in general although the noises are embedded in the encrypted image. It is clear that increasing cropping and noises make the decrypted images unclear as shown in Figures 11 and 12. However, the major content of the images can be retrieved. Therefore, the proposed cryptosystem has high robustness toward noise and cropping attacks.

4. Conclusion and Future Work

An efficient cryptosystem for secure IoT surveillance systems is proposed in this paper. First, we extract the informative

(a) (b)

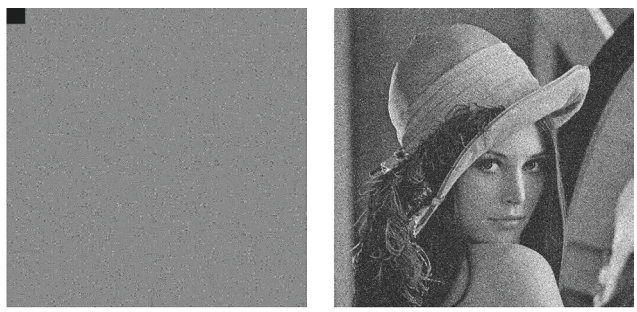
Figure 8: Effect of noise attacks with $\beta = 5$. (a) Encrypted image with noises. (b) Decrypted image.

(a) (b)

Figure 9: Effect of noise attacks with $\beta = 10$. (a) Encrypted image with noises. (b) Decrypted image.

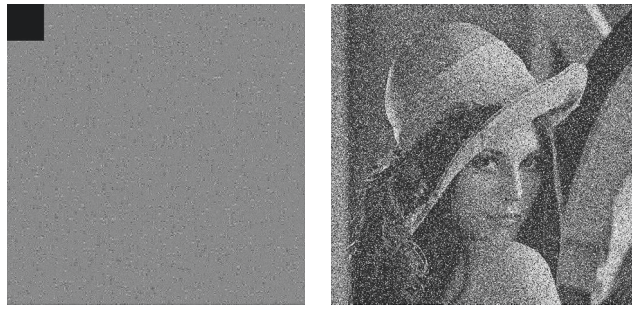
(a) (b)

Figure 10: Effect of noise attacks with $\beta = 15$. (a) Encrypted image with noises. (b) Decrypted image.



(a) (b)

Figure 11: Results of attacks with cropping attack. (a) Encrypted image with (32×32) cropping size. (b) Decrypted image.



(a) (b)

Figure 12: Results of attacks with cropping attack. (a) Encrypted image with (64×64) cropping size. (b) Decrypted image.

data from video surveillance using K-means clustering with HSV histograms. Then, we compress the extracted keyframes using fractional cosine transform and the spectrum is compressed by spectrum cutting. The encryption process is performed using a discrete fractional random transform and nonlinear system. Here, Chen's chaotic map is used to produce two keys. First is the permutation key to confuse the pixels and the second key is the randomized matrix in discrete fractional random transform. The proposed cryptosystem can encrypt multiple frames once instead of one-to-one traditional encryption techniques and maintains the visual representation of the decrypted data. This reveals an important advantage of this work since compress-encrypt several images in one operation will minimize the network overhead and reduce the cost of implementation. The proposed cryptosystem shows good performances and results compared to the state-of-art cryptosystems. The disadvantage of the proposed work related mainly to the compression by the method of spectrum cutting. In the case of increasing the compression rate, the decrypted data would have bad quality. Therefore, future work will investigate deep learning-based compression techniques to improve the performances of this work. We also aim to develop an access control mechanism [44] with aggregate-signcryption to secure multiple surveillance IoT applications.

Data Availability

The data used to support the findings of this study are included in the article. Some or all data used during the study are available from the corresponding author by request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (nos. 61902081, 61702125, and 61702126).

References

[1] F. Wortmann and K. Flüchter, "Internet of things," *Business & Information Systems Engineering*, vol. 57, no. 3, pp. 221–224, 2015.

[2] X. Liu, J. Liu, S. Zhu, W. Wang, and X. Zhang, "Privacy risk analysis and mitigation of analytics libraries in the android ecosystem," *IEEE Transactions on Mobile Computing*, p. 1, 2019.

[3] A. Hassan, N. Eltayieb, R. Elhabob, and F. Li, "An efficient certificateless user authentication and key exchange protocol for client-server environment," *Journal of Ambient Intelligence and Humanized Computing*, vol. 9, no. 6, pp. 1713–1727, 2018.

[4] L. Qi, X. Zhang, W. Dou, C. Hu, C. Yang, and J. Chen, "A two-stage locality-sensitive hashing based approach for privacy-preserving mobile service recommendation in cross-platform edge environment," *Future Generation Computer Systems*, vol. 88, pp. 636–643, 2018.

[5] A. Hassan, R. Hamza, V. G. Mawutor, A. S. Patil, and F. Li, "A lightweight certificateless user authentication scheme for mobile environment," in *Proceedings of the International Conference on Machine Learning for Cyber Security*, pp. 112–122, Springer, Xi'an, China, September 2019.

[6] W. Wang, Y. Li, X. Wang, J. Liu, and X. Zhang, "Detecting android malicious apps and categorizing benign apps with ensemble of classifiers," *Future Generation Computer Systems*, vol. 78, pp. 987–994, 2018.

[7] L. Li, J. Liu, L. Cheng et al., "Creditcoin: a privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 7, pp. 2204–2220, 2018.

[8] X. Zhang, W. Dou, Q. He et al., "LSHiForest: a generic framework for fast tree isolation based ensemble anomaly analysis," in *2017 IEEE 33rd International Conference on Data Engineering (ICDE)*, pp. 983–994, IEEE, San Diego, CA, USA, April 2017.

[9] T. Sato, M.-S. Dao, K. Kuribayashi, and K. Zettsu, "SEPHLA: challenges and opportunities within environment-personal health archives," in *Proceedings of the International Conference on Multimedia Modeling*, pp. 325–337, Springer, Thessaloniki, Greece, January 2019.

[10] M.-S. Dao and K. Zettsu, "Automatic labeling streaming data for event detection from heterogeneous sensors," in *Proceedings of the 2015 Seventh International Conference on Knowledge and Systems Engineering (KSE)*, pp. 365–370, IEEE, Ho Chi Minh City, Vietnam, October 2015.

[11] J. Wu, S.-H. Zhong, J. Jiang, and Y. Yang, "A novel clustering method for static video summarization," *Multimedia Tools and Applications*, vol. 76, no. 7, pp. 9625–9641, 2017.

[12] L. Gong, C. Deng, S. Pan, and N. Zhou, "Image compression-encryption algorithms by combining hyper-chaotic system with discrete fractional random transform," *Optics & Laser Technology*, vol. 103, pp. 48–58, 2018.

[13] M. Rochan, L. Ye, and Y. Wang, "Video summarization using fully convolutional sequence networks," in *Proceedings of the European Conference on Computer Vision*, pp. 347–363, ECCV, Munich, Germany, September 2018.

[14] R. Hamza, Z. Yan., K. Muhammad, P. Bellavista, and F. Titouna, "A privacy-preserving cryptosystem for IoT E-healthcare," *Information Sciences*, 2019.

[15] Z. Wei, J. Li, X. Wang, and C.-Z. Gao, "A lightweight privacy-preserving protocol for vanets based on secure outsourcing computing," *IEEE Access*, vol. 7, pp. 62785–62793, 2019.

[16] Y. Zhang, D. Zheng, X. Chen, J. Li, and H. Li, "Efficient attribute-based data sharing in mobile clouds," *Pervasive and Mobile Computing*, vol. 28, pp. 135–149, 2016.

[17] L. Qi, X. Zhang, W. Dou, and Q. Ni, "A distributed locality-sensitive hashing-based approach for cloud service recommendation from multi-source data," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 11, pp. 2616–2624, 2017.

[18] J. Li, Z. Liu, X. Chen, F. Xhafa, X. Tan, and D. S. Wong, "L-EncDB: a lightweight framework for privacy-preserving data queries in cloud computing," *Knowledge-Based Systems*, vol. 79, pp. 18–26, 2015.

[19] L. Jiang, L. Tong, X. Li, M. Atiquzzaman, H. Ahmad, and X. Wang, "Anonymous communication via anonymous identity-based encryption and its application in IoT," *Wireless Communications and Mobile Computing*, vol. 2018, Article ID 6809796, 8 pages, 2018.

[20] H. Yan, X. Li, Y. Wang, and C. Jia, "Centralized duplicate removal video storage system with privacy preservation in IoT," *Sensors*, vol. 18, no. 6, p. 1814, 2018.

[21] L. Jin, X. Chen, M. Li, J. Li, P. P. C. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 6, pp. 1615–1625, 2014.

[22] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using probabilistic image encryption," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3679–3689, 2018.

[23] N. Zhou, T. Dong, and J. Wu, "Novel image encryption algorithm based on multiple-parameter discrete fractional random transform," *Optics Communications*, vol. 283, no. 15, pp. 3037–3042, 2010.

[24] L. Sui, H. Lu, Z. Wang, and Q. Sun, "Double-image encryption using discrete fractional random transform and logistic maps," *Optics and Lasers in Engineering*, vol. 56, pp. 1–12, 2014.

[25] R. Hamza, A. Hassan, and A. S. Patil, "A lightweight secure IoT surveillance framework based on DCT-DFRT algorithms," in *Proceedings of the International Conference on Machine Learning for Cyber Security*, pp. 271–278, Springer, Xi'an, China, September 2019.

[26] H. Wu, X. Sun, J. Yang, W. Zeng, and F. Wu, "Lossless compression of JPEG coded photo collections," *IEEE Transactions on Image Processing*, vol. 25, no. 6, pp. 2684–2696, 2016.

[27] X. Wang, J. Li, J. Li, and H. Yan, "Multilevel similarity model for high-resolution remote sensing image registration," *Information Sciences*, vol. 505, pp. 294–305, 2019.

[28] Q. M. Rajpoot and C. D. Jensen, "Security and privacy in video surveillance: requirements and challenges," in *Proceedings of the IFIP International Information Security Conference*, pp. 169–184, Springer, Marrakech, Morocco, 2014.

[29] H. Keval and M. A. Sasse, "To catch a thief–you need at least 8 frames per second: the impact of frame rates on user performance in a cctv detection task," in *Proceedings of the 16th ACM International Conference on Multimedia*, pp. 941–944, ACM, Vancouver, Canada, October 2008.

[30] E. Bertino and E. Ferrari, "Big data security and privacy," in *A Comprehensive Guide through the Italian Database Research over the Last 25 Years*, pp. 425–439, Springer, Berlin, Germany, 2018.

[31] J. Huang, T. Nandha Kumar, H. A. F. Almurib, and F. Lombardi, "A deterministic low-complexity approximate (multiplier-less) technique for DCT computation," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 8, pp. 3001–3014, 2019.

[32] A. Madanayake, R. J. Cintra, V. Dimitrov et al., "Low-power VLSI architectures for DCTDWT: precision vs approximation for HD video, biomedical, and smart antenna applications," *IEEE Circuits and Systems Magazine*, vol. 15, no. 1, pp. 25–47, 2015.

[33] R. Hamza, "A novel pseudo random sequence generator for image-cryptographic applications," *Journal of Information Security and Applications*, vol. 35, pp. 119–127, 2017.

[34] Z. Liu, H. Zhao, and S. Liu, "A discrete fractional random transform," *Optics Communications*, vol. 255, no. 4–6, pp. 357–365, 2005.

[35] I. A. T. F. Taj-Eddin, M. Afifi, M. Korashy, D. Hamdy, M. Nasser, and S. Derbaz, "A new compression technique for surveillance videos: evaluation using new dataset," in *Proceedings of the 2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*, pp. 159–164, IEEE, Konya, Turkey, July 2016.

[36] A. G. Weber, "The USC-SIPI image database version 5," *USC-SIPI Report*, vol. 315, pp. 1–24, 1997.

[37] M. Zhang and X. Tong, "A new algorithm of image compression and encryption based on spatiotemporal cross chaotic system," *Multimedia Tools and Applications*, vol. 74, no. 24, pp. 11255–11279, 2015.

[38] S. Zhu and C. Zhu, "A new image compression-encryption scheme based on compressive sensing and cyclic shift," *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 1–21, 2019.

[39] C. E. Shannon, "A mathematical theory of communication," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 5, no. 1, pp. 3–55, 2001.

[40] N. Zhou, J. Yang, C. Tan, S. Pan, and Z. Zhou, "Double-image encryption scheme combining dwt-based compressive sensing with discrete fractional random transform," *Optics Communications*, vol. 354, pp. 112–121, 2015.

[41] X.-D. Chen, Y. Wang, J. Wang, and Q.-H. Wang, "Asymmetric color cryptosystem based on compressed sensing and equal modulus decomposition in discrete fractional random transform domain," *Optics and Lasers in Engineering*, vol. 121, pp. 143–149, 2019.

[42] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[43] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT)*, vol. 1, no. 2, pp. 31–38, 2011.

[44] K. Riad, R. Hamza, and H. Yan, "Sensitive and energetic IoT access control for managing cloud electronic health records," *IEEE Access*, vol. 7, pp. 86384–86393, 2019.