IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 12, 2018, accepted March 19, 2018, date of publication April 2, 2018, date of current version April 23, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2820724

A Lightweight Encryption Method for Privacy Protection in Surveillance Videos

XING ZHANG[1], SEUNG-HYUN SEO[2], (Member, IEEE), AND CHANGDA WANG[1], (Member, IEEE)

[1]School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China
[2]Division of Electronic Engineering, Hanyang University, Ansan 15588, South Korea

Corresponding author: Changda Wang (changda@ujs.edu.cn)

This work was supported in part by the National Science Foundation of China under Grant 61172269 and in part by the Jiangsu Provincial Science and Technology Project under Grant BA2015161.

ABSTRACT Privacy protection of surveillance videos is an important issue because of the pervasiveness of surveillance cameras. Region of interest (RoI) privacy protection prefers encrypting limited privacy-sensitive areas to encrypting the entire video because of the resource-tightened Internet of Things devices. However, many cryptographic technologies now applied in privacy protection, e.g., AES and RSA, are not efficient to meet the real-time requirement for surveillance videos. A lightweight encryption approach is then devised based on layered cellular automata (LCA). Using our approach, the extracted RoIs are fed into the initial state of an 8-layer cellular automata, which is driven by the randomly selected rules for the LCA's state transitions. As a result, all RoIs are encrypted independently and synchronously. The encrypted RoIs are stored at the camera side and can be used by authenticated users through an on-demand manner. The surveillance video without RoIs can be watched in real-time by any user online. Theoretical analyses and experimental results show that our approach is both efficient and effective.

INDEX TERMS Surveillance video, RoI encryption, layered cellular automata, reversible rule, shift transformation.

I. INTRODUCTION

With the rapid development of network and communication technology, the application of surveillance systems have significantly increased in the last two decades. Surveillance cameras are deployed not only in public places such as airport, bus station, but also in private places such as home, office, to name a few. By surveillance videos, the authenticated users can identify most of objects they want to observe or track with. For example, the users can see the live or stored surveillance videos on hand-held devices to know what is happening or has happened in their house. However, as it's possible to obtain the photos of humans' faces, the plate numbers of the cars among the monitoring area, the privacy information is then jeopardized through the surveillance cameras in public areas. The private places like homes are vulnerable to the surveillance videos too. Generally, encryption is an effective method to protect privacy as well as security. Surveillance video encryption algorithms can be categorized as two kinds: 1) encrypt the entire video [1]–[3], and 2) encrypt the region of interest (RoI) which contains sensitive information [4]–[12]. Note that encrypt each frame of a video is not only computationally expensive but also hard to meet real-time requirement for the video's transmission. Only encrypt the RoIs and then keep the non-privacy region visually intact not only protect the privacy of the objects, but also increase the efficiency of the encryption.

To hide privacy from sensitive areas, different cryptographic and RoI extraction techniques are presented. Chaos cryptographic techniques are applied to encrypt RoIs in [6] and [7]. Scrambling techniques in transform-domain and codestream-domain are proposed in [10], [13], and [14]. Pseudo-random permutation-based RoI encryption approaches for H.264 videos are proposed in [4] and [14]. Traditional encryption algorithms, e.g., AES and DES, are also used in [9] and [15] for the same purpose. However, most of the known cryptographic techniques are not suitable to encrypt video because of their large computational costs [16]. In addition, chaotic system is not well suited for hardware implementation due to high numerical precision requirements [17]. As a result, hardly is it integrated with an IoT device at the surveillance cameras' side. Therefore, the lightweight and hardware friendly encryption approach is preferred.

Although video are made from frames, where each frame is an image with a compressed format, some inherent features such as redundancy, bulk data capacity and high correlation between pixels make the typical image cryptosystems unsuitable for videos. In recent years, various image encryption methods which utilizes the chaos theory [18], [19], the quantum technique [20], the DNA sequence [21]–[23] and the wavelet transform have been proposed. Nevertheless, applying CA to encrypt image is preferred because of its intrinsic features such as parallelism, locality and homogeneity.

Some researchers applied one dimensional (1D) CA to devise image encryption schemes [24]–[28], because the evolution of 1D CA is both efficient and easy to be implemented. Since a two dimensional (2D) pixel matrix can represent an image more efficiently, a 2D CA is more suitable for image encryption [29]–[31]. Nevertheless, each value in a pixel matrix has to convert into a binary sequence. Note that the binary representation of an image is a composition of some binary matrices, which implicates an image can be viewed as a combination of some independent 2D CAs. Therefore, that layered CA (LCA) consists of a series of 2D CAs is suitable for image encryption.

A LCA is a highly parallel system, not only has the inherent advantages of traditional CA but also has more complex and flexible neighborhood structures. LCA is firstly introduced in [32] and [33] by which to generate pseudo random sequence. Then LCA has been applied to design block cipher along with reversible CA in [34]. It has been found that the proposed block cipher is better than AES with respect to the requirements of confusion and diffusion. Recently, a new public key encryption algorithm and a digital signature scheme based on LCA have been proposed in [35] and the experiments show that such a public key encryption algorithm is more efficient than that of RSA-1024. A LCA-based reverse iterative image encryption scheme has been proposed in [36], where the plain image is set as the state of a LCA and then the LCA is backwardly shifted to generate the cipher image. As a result, to decrypt the cipher image need to forwardly shift the LCA with a preceding state. Hence, a block of the same size as the plain image should be kept as well as the corresponding cipher image. If such a scheme is used to encrypt the privacy sensitive RoIs, the transmitted surveillance data are doubled. Therefore, such a scheme is not suitable for the privacy protection in surveillance videos because of resource tightened IoT devices at the surveillance video side.

In this paper, we propose a lightweight LCA-based method to encrypt the privacy sensitive RoIs for surveillance videos with H.264 format, which is a popular video format currently. The proposed method is devised for the compressed videos and thus allows extending the existing surveillance systems without modifying the camera's hardware. Since the paper focuses on the RoI privacy protection with lightweight cryptographic techniques, how to extract the RoIs from video frames is not highlighted. In the paper, the RoIs are extracted by the method in [8].

The surveillance video is composed of a sequence of group of pictures (GOP) which consists of **I** frame, **P** frames and **B** frames, where **I** frame has spatial redundancy in still images. Generally, the other frames are all incremental information between the adjacent frames. In our method, each RoI derived from **I** frames will be organized as binary blocks and then set as the initial states for a LCA proposed in the paper. Thereafter, the LCA uses its reversible rules and simple transformations model for state transitions. The final state data of the LCA is extracted and saved as the encrypted RoI. All RoIs are encrypted independently. Specifically, the main contributions of this paper are as follows.

- The RoIs are encrypted and stored at the camera side for an on-demand service required by the authenticated users, which makes the proposed method both effective and efficient.
- A LCA-based approach is devised to encrypt RoIs for privacy protection in surveillance videos. The simple rule evolution and shift transformation make the RoI encryption efficiently, and therefore it satisfies the lightweight requirements of surveillance videos.
- A randomized key is generated to ensure that the same RoI blocks from different video frames will show different encryption results, and thus the algorithm is able to resist the known plaintext attacks. Experimental results show that our approach has desirable security effects, which ensure that the attackers cannot the derive private information from the encrypted RoIs without the key.

The remainder of this paper is organized as follows. In Section II, we introduce the preliminaries of our approach, including the concepts of cellular automata, elementary cellular automata and layered cellular automata. In Section III, the framework of the proposed RoI privacy protection method is specified. In Section IV, we present the lightweight LCA-based RoI encryption, followed by the experimental results in Section V. We give a detailed security analysis in Section VI. The related works are reviewed in Section VII. Finally, we concluded our work in Section VIII.

II. PRELIMINARIES

A CA is a dynamic information processing system whose space, time and state are all discrete. The CA consists of several cells arranged in a regular grid. Each cell has its own state and all cells update their states synchronously according to a presetting local rule. The new state of a cell depends not only on its own state in history, but also the states of its neighbors'. For a finite CA, the periodic boundary conditions are usually applied, where the boundary cells are concatenated as a cascading system and thus the CA can be treated as a finite state machine.

For an 1D CA, its local transition rule f is defined as follows:

$$s_i^{t+1} = f(s_{i-r}^t, \cdots, s_{i-1}^t, s_i^t, s_{i+1}^t, \cdots, s_{i+r}^t)$$

where s_i^t denotes the state of i^{th} cell at time t and r is neighborhood radius with the center as s_i^t. If there are two

cell states only, totally f has 2^{2r+1} different inputs followed by $2^{2^{2r+1}}$ different local transition rules.

Elementary CA (ECA) is the simplest CA that each cell only has two possible states and three neighbors. There are $2^8 = 256$ elementary rules in total and each of them is indexed by an integer lies in [0, 255]. All possible input states of f are arranged in the order as $111, 110, \cdots, 001, 000$, where the resulting output states formed a binary sequence and the corresponding rule number is represented by the chosen decimal numbers. The example elementary rules are showed in Table 1.

TABLE 1. Elementary rule 15, 30 and 90.

Rule	111	110	101	100	011	010	001	000
15	0	0	0	0	1	1	1	1
30	0	0	0	1	1	1	1	0
90	0	1	0	1	1	0	1	0

Reversible cellular automata (RCA) is a special case of CA whose transition rule is reversible and each state has only one successor and one predecessor. RCA is especially suitable for cryptosystem because the reversibility property of CA ensures that any encrypted message can be decrypted by the same algorithm performed in the reverse direction. It has been proved that whether a rule of an 1D CA is reversible is determined, whereas for a two or more dimension CA the same reversibility is undecidable.

A layered cellular automata (LCA) is a cascading system of 2D CAs with the same size, where each layer is a composition of 1D CAs. The structure of LCAs makes a more complex but flexible expression ability. In this paper, an 8-layer CA is devised by us to encrypt the RoIs of the gray surveillance video frames because the 8-layer CA can match up with the binary pixel matrix of a video frame completely. The relationship between the pixel matrix and a layered CA is shown in Fig. 1.

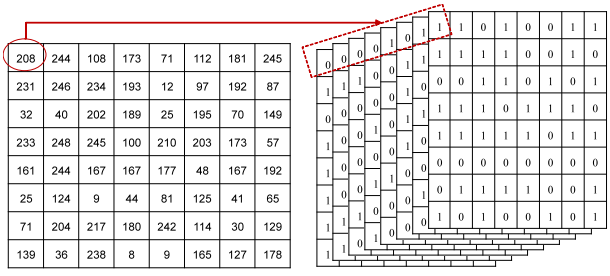


FIGURE 1. Relationship between pixel matrix and 8-layer CA.

III. THE FRAMEWORK OF OUR APPROACH

Our approach is a hierarchical privacy protection method for surveillance videos now can apply to the video format H.264. By our approach, the non-authenticated users can only see the real-time surveillance video without RoIs, while the authenticated users can watch the complete surveillance video through an on-demand manner.

The framework of the proposed RoI encryption approach is shown in Fig. 2 (a). The RoIs containing privacy sensitive information such as faces and license plates are extracted from the **I** frames (JPEG format) through the RoI detection and segmentation methods in [8]. It's possible that there are more than one RoI in a video frame. The length and width of each RoI is the multiples of 16, so that each RoI can be divided into the sub-blocks of the size 16×16.

LCA-based lightweight encryption algorithm is performed on every RoI to make the privacy sensitive information unrecognizable, and then all RoIs from a frame are encrypted independently. Hence, if there are some bits spoiled during the encoding and/or transmission, it will only affect the decryption within their blocks, which limits the errors propagation. All RoI blocks in a video frame are encrypted by the same random keys, which can reduce the consumption of the key's exchange and storage. Note that the RoIs from different video frames are required to use different encryption keys.

After the RoIs are extracted, the pixel values with all 0 (or 1) are filled back to replace the extracted RoI regions in the **I** frames. In what follow, the new surveillance video based on the new **I** frames is then re-encoded and transmitted, which can be watched real-time on a computer or a handheld device with network service. Whereas the encrypted RoIs are stored at the camera side without compression and be used for the on-demand service later, i.e., the stored RoI will be transmitted, decrypted and then integrated with the new **I** frames to recover the original surveillance video *if and only if* the authenticated users require to do so. Note that the encrypted RoI data lost almost all spatial correlations, compression cannot decrease the data size remarkably.

The RoIs encryption and the new video's encoding are carried out independently, which make the proposed method can not only protect privacy information, but also meet the real-time requirement. In addition, since the RoIs in the original **I** frames are replaced with regions that pixel values are all 0 or 1, the surveillance video data compression ratio is increased because the correlations of these data are increased. The cost of our approach is the affordable delay for the authenticated users to retrieve the complete surveillance video.

As shown in Fig. 2 (b), the non-authenticated users still can see the non-privacy region that remains intact and the privacy region is replaced with a white region, whereas the authenticated users can see the entire surveillance video.

IV. LIGHTWEIGHT ROI ENCRYPTION ALGORITHM

The encryption algorithm uses the binary sequences from each RoI block as the initialization of an 8-layer CA. Since each layer of the LCA can be treated as a composition of a series of 1D CAs, we then randomly select the reversible ECA rules to train the LCA and then obtain the LCA's final state, which can be mapped into a pixel matrix of the encrypted image. In order to obtain better confusion and diffusion effects, we also apply half shift transformation in

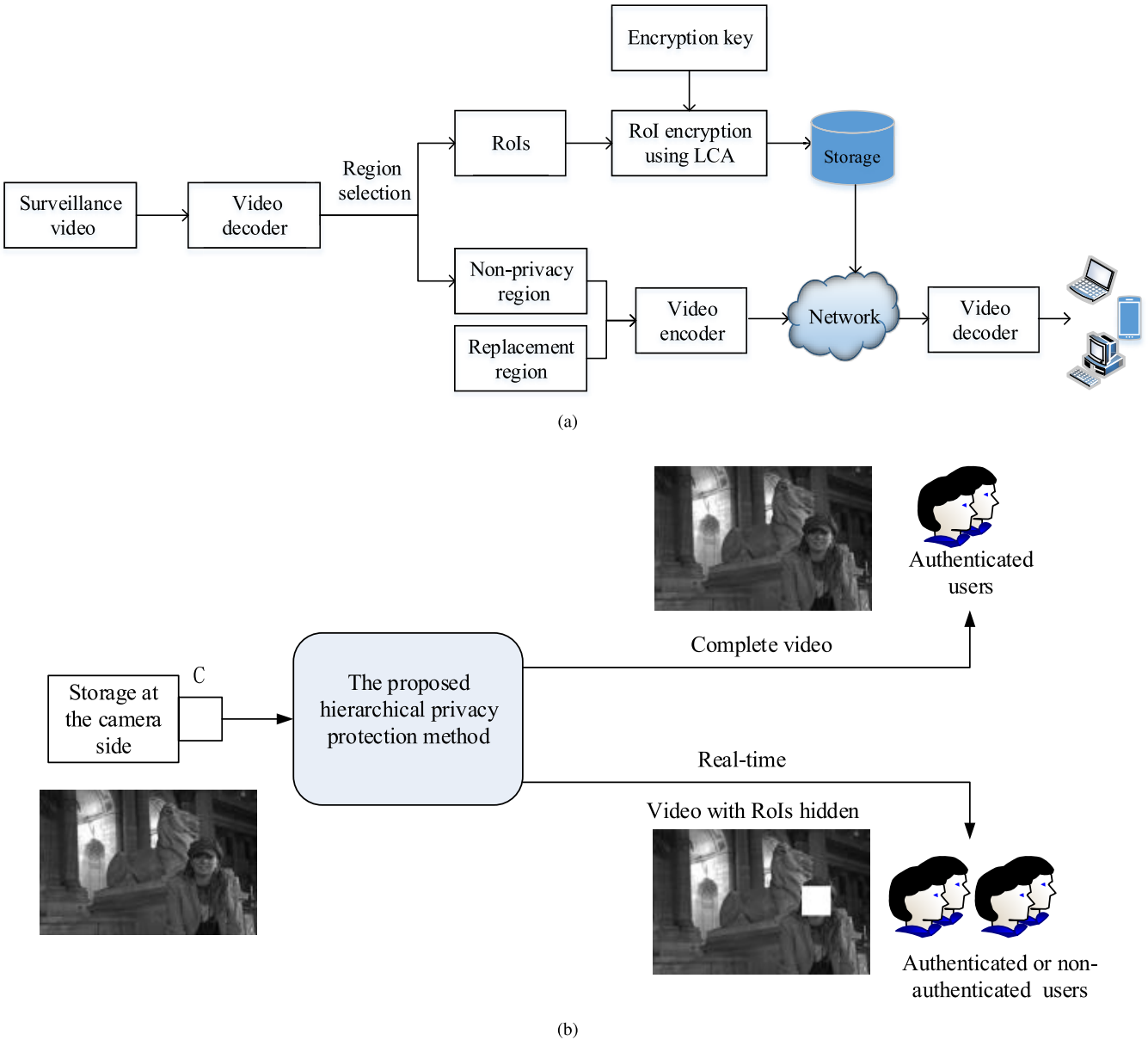


FIGURE 2. The framework of the proposed LCA-based RoI encryption approach.

each layer as well as in adjacent layers. Besides, a random shift transformation on each 1D CA is applied, too.

A. KEY GENERATION

We first choose four pairs of reversible ECA rules, {15, 85}, {51, 51}, {170, 240}, and {204, 204}, as the transition rules, and then such rules are indexed by a mapping function as following:

$$\mathcal{F} : \{00, 01, 10, 11\} \rightarrow \{15/85, 51/51, 170/240, 204/204\}$$

where $\mathcal{F}$ is an injective function. Furthermore, in each pair of rules, the one is used for encryption and the other is used for decryption.

A pseudo random binary sequence *PR* is generated from a seed number, which is secretly shared between the encryption and the decryption sides. The *PR* is divided into blocks of two bits, where each block represents a particular rule for a 1D CA in the LCA. Therefore, the length of the sequence *PR* is determined by the number of 1D CA in the LCA, where the number is decided by the height of its RoI block. Specifically, the size of a RoI block is 16×16, each layer of the layered CA has 16 rows and then the length of the sequence *PR* is $8 \times 2 \times 16 = 256$.

The binary sequence *PR* with the iteration number N will be used as the encryption and decryption key.

B. ENCRYPTION

The RoI blocks are encrypted as follows.

Step 1: Initialization. Arrange the binary sequence from the original RoI block into an 8-layer CA, and then let each layer contain 16×16 bits.

Step 2: Rule evolution. Each layer is treated as a composition of the rows of the 1D CAs with the same size. Thereafter, cells from different 1D CAs change their states independently according to different ECA rules which selected by the blocks in the sequence PR.

Step 3: Intra-layer shift. A half shift transformation is performed in each layer. For every row in a layer, only half cells change their states to the states of the cells at their adjacent row. Specifically, the cells at posterior columns will change their states and the other cells will keep static.

If there are $k(k \in \mathbb{N}^+)$ columns in each layer, the state of i^{th} row in the l^{th} layer at time t is $(s^t_{l,i,1}, \cdots, s^t_{l,i,j}, \cdots, s^t_{l,i,k})$. It will be shifted to the new state $(s^{t+1}_{l,i,1}, \cdots, s^{t+1}_{l,i,j}, \cdots, s^{t+1}_{l,i,k})$ after an intra-layer half shift transformation, where

$$s^{t+1}_{l,i,j} = \begin{cases} s^t_{l,i,j}, & 1 \le j \le \lceil \frac{k}{2} \rceil; \\ s^t_{l,i+1,j}, & \lceil \frac{k}{2} \rceil + 1 \le j \le k. \end{cases}$$

Note that such a transformation makes the half cells in each layer change their states, and it indirectly influences the cells not shifted because such transformation can change their neighbors' states. Therefore, if a cell in a row changes its state, it will affect the cells not only in the same row but also in the other rows.

Step 4: Inter-layer shift. It is a half shift transformation between adjacent layers. In addition, this is a periodic transformation, where half cells in one layer will shift to its upper layer and the cells in the first layer will shift to the last layer.

Specifically, when the inter-layer half shift transformation has happened, the new states of the i^{th} row in the l^{th} layer is $(s^{t+1}_{l,i,1}, \cdots, s^{t+1}_{l,i,j}, \cdots, s^{t+1}_{l,i,k})$ at time $t+1$, where

$$s^{t+1}_{l,i,j} = \begin{cases} s^t_{l+1,i,j}, & 1 \le j \le \lceil \frac{k}{2} \rceil; \\ s^t_{l,i,j}, & \lceil \frac{k}{2} \rceil + 1 \le j \le k. \end{cases}$$

Step 5: Intra-row random shift. Each 1D CA in a layer performs a periodic intra-row shift transformation. All cells in a 1D CA shift to their left according to a random shift number.

Let ab denote the transition rule of an 1D CA appointed by the binary sequence in the key, where $a, b \in \{0, 1\}$, then the shift number of the CA is defined as $a \times 2^1 + b \times 2^0 = 2a + b$. Therefore, each 1D CA in the layered CA has four possible shift numbers.

Repeat **Step 2** to **Step 5** until the predefined iteration number reached.

Finally, the encrypted RoI block is built by converting the final state of the 8-layer CA into a pixel matrix. Fig. 3 shows the aforementioned encryption process. Algorithm 1 is used for RoIs encryption.

Table 2 lists the *rule indexes* and the *resulting shift numbers*. Fig. 4 shows a shift transformation on a layer according to the shift numbers shown in Table 2.

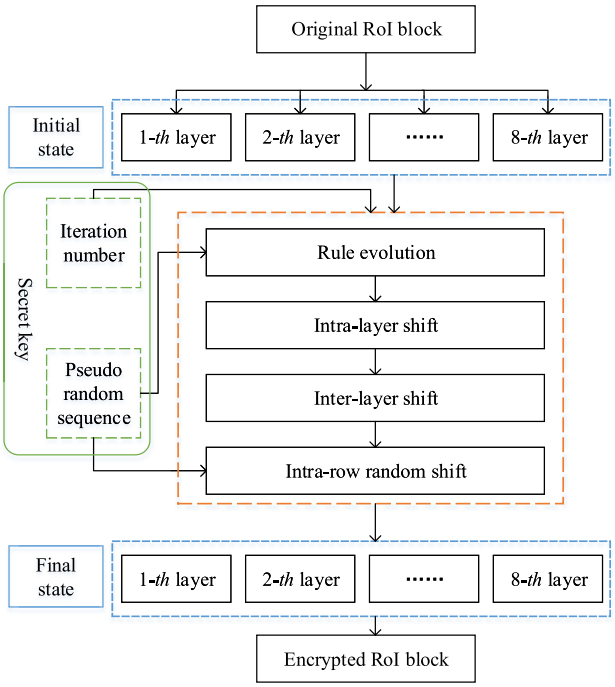


FIGURE 3. The LCA-based surveillance video encryption algorithm.

Algorithm 1 Encryption Algorithm

Input: RoI block RB, random sequence PR, iteration number N;

Output: Cipher block CB

```
RB ← Cell(RB);
for k = 1 to N do
    RB ← Rule(RB, PR); // Rule evolution
    RB ← IntralayerST(RB); // The intra-layer shift
    RB ← InterlayerST(RB); // The inter-layer shift
    RB ← IntrarowST(RB, PR);
    // The intra-row random shift
end for
CB ← Mat(RB);
return CB
```

TABLE 2. Shift numbers with its corresponding rule indices.

Rule index	11	10	00	01	00	10	11	10
Shift number	3	2	0	1	0	2	3	2

C. DECRYPTION

The decryption key is the same as the encryption key. The evolution rules represented by the sequence are the reverse rules of the ones used in the encryption.

The binary sequence of an encrypted RoI block is set as the initial state of an 8-layer CA. Forward shifting uses the rules selected by the decryption key. Thereafter, the inverse transformations of the three different transformations mentioned above are performed, too.

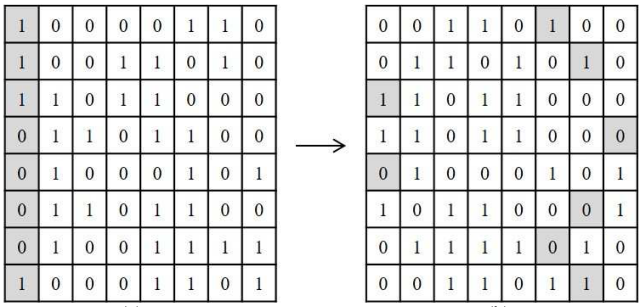


FIGURE 4. An example of random shift.

The difference between the intra-layer half shift transformation and its inverse procedure is the LCA's shift direction. For example, after the inverse transformation, the new state of the cell at i^{th} row j^{th} column in l^{th} layer on time $t+1$ is:

$$s_{l,i,j}^{t+1} = \begin{cases} s_{l,i,j}^{t}, & 1 \le j \le \lceil \frac{k}{2} \rceil; \\ s_{l,i-1,j}^{t}, & \lceil \frac{k}{2} \rceil + 1 \le j \le k. \end{cases}$$

Similarly, when the inverse inter-layer half shift transformation happens, the cell's new state on time $t+1$ is:

$$s_{l,i,j}^{t+1} = \begin{cases} s_{l-1,i,j}^{t}, & 1 \le j \le \lceil \frac{k}{2} \rceil; \\ s_{l,i,j}^{t}, & \lceil \frac{k}{2} \rceil + 1 \le j \le k. \end{cases}$$

The inverse procedure of intra-row shift transformation is that each cell shifts to its right according to a shift number, where the number is the same as the one used in the encryption.

The final state of the LCA is converted into the pixel matrix by which to recover the RoI blocks. Algorithm 2 is used for decryption.

Algorithm 2 Decryption Algorithm

Input: Cipher block CB, random sequence PR, iteration number N;
Output: RoI block RB

$CB \leftarrow Cell(CB)$;
for $k = 1$ to N **do**
  $CB \leftarrow InIntrarowST(CB, PR)$;
  // The inverse procedure of intra-row random shift
  $CB \leftarrow InInterlayerST(CB)$;
  // The inverse procedure of inter-layer shift
  $CB \leftarrow InIntralayerST(CB)$;
  // The inverse procedure of intra-layer shift
  $CB \leftarrow Rule(CB, PR)$; // Rule evolution
end for
$RB \leftarrow Mat(CB)$;
return RB

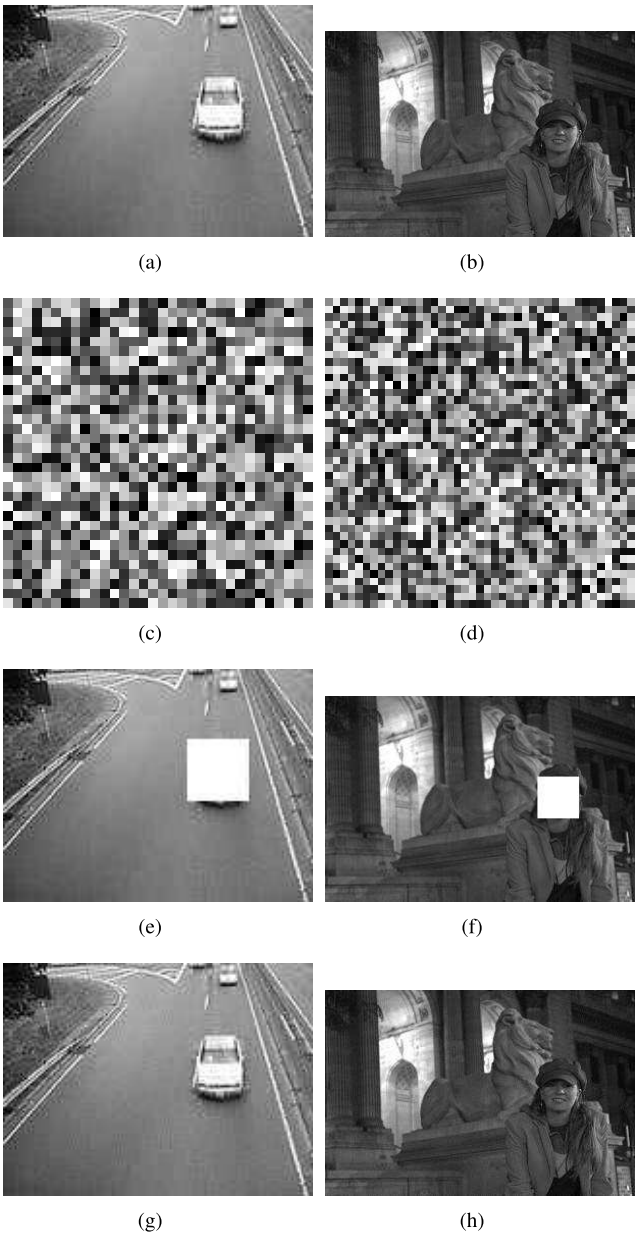


FIGURE 5. Experimental results.

V. EXPERIMENTAL RESULTS

The experiments based on the surveillance videos of H.264, as showed in Fig. 5 (a) and (b), where the RoIs contain privacy sensitive information, such as human face and vehicle plate number. In our experiments, the RoIs are extracted by the method in [8].

The proposed approach is applied on these extracted RoIs, the encrypted RoIs are showed in Fig. 5(c) and (d), the non-privacy regions are then integrated with the replacement regions (white region) for privacy protection are showed in Fig. 5 (e) and (f) and the recovered complete video frames for the authenticated users are showed in Fig. 5 (g) and (h).

TABLE 3. Entropy comparisons of our approach and some of the known schemes.

Entropy / Image	Plain image	Cipher image				
		Proposed	1D CA		2D CA	
			Ref [24]	Ref [37]	Ref [30]	Ref [31]
rice	7.0115	7.9957	7.9706	7.9357	7.9811	7.9886
cameraman	7.0097	7.9888	7.9811	7.9733	7.9893	7.9885
lift	6.4916	7.9976	7.9795	7.9781	7.9886	7.9889

In addition, the blocks of any two RoIs in a frame are encrypted by the same key, whereas the RoI blocks from different frames are encrypted by different keys. Even if the encryption key of the RoI blocks in a frame is leaked, the encrypted RoI blocks in others frames cannot be decrypted. Therefore, it can not only protect the privacy in a surveillance video, but also reduce the costs of the key's distribution.

VI. SECURITY AND PERFORMANCE ANALYSIS

Encryption algorithm used for privacy protection in surveillance video should be secure enough to prevent attackers deriving the privacy information from the encrypted videos. In our work, regions contain private information in frames are encrypted by our LCA-based approach and the non-privacy regions are going to remain intact.

Several statistical tests and measurements are used to analyze the security of our approach.

A. INFORMATION ENTROPY

Information entropy is an important measurement for the gray levels distribution in an image. The entropy of an image I is defined as follows:

$$H(I) = -\sum_{i}^{L} p(x_i) log_2 p(x_i),$$

where L is the number of gray levels, x_i is the i^{th} gray value in the image I, $p(x_i)$ is the occurrence probability of x_i, and $\sum_i p(x_i) = 1$.

The higher the entropy is, the more the gray levels close to uniform distribution are. For an image satisfies uniform distribution, there are 256 gray levels with the same occurrence possibility, therefore the optimal entropy value is 8 and the entropy of an encrypted image should be approach to such a value. Table 3 shows a comparison of the entropies of three gray images and their corresponding cipher images encrypted by our LCA-based method and some other methods in [24], [30], [31], and [37]. In Table 3, the entropies of the images encrypted by our method are very close to the optimal value 8, which demonstrates that our method is better than that of the other methods.

B. HISTOGRAM

An image histogram directly presents the statistical characteristics of the image pixel values. Generally, the pixel values of the encrypted images have to satisfy a uniform random distribution.

Fig. 6 shows the histograms of three plain images and their corresponding cipher images encrypted by our approach. Furthermore, Fig. 7 shows the encrypted images whose plain images pixel values are all binary numbers 1 or 0, and the histograms of the two encrypted images. Entropies of the cipher images shown in Fig. 7 (b) and (c) are 7.988 and 7.987, respectively. It's obvious that all histograms of the cipher images are close to strict uniform distribution, which far away from the plain images with irregular distributions. Therefore, it is computationally infeasible to derive any information about the plain images from its corresponding cipher images without the key.

C. CORRELATION OF ADJACENT PIXELS

Correlation test of the adjacent pixels is an important statistical method to evaluate the diffusion and confusion of an encryption algorithm. Encrypted images should have an almost zero correlation between the adjacent pixels, whereas the plain images should present a strong correlation.

To perform a correlation test on an image, we randomly choose 1,000 pairs of adjacent pixels in vertical, diagonal and horizontal directions from a plain image and its cipher image, respectively. We then calculate the correlation coefficient, where the correlation coefficient is defined as follows:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x) \cdot \sqrt{D(y)}}},$$

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

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

$$cov(x, y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))(y_i - E(y)).$$

Table 4 shows the correlation coefficients of the three plain images and their corresponding cipher images. We can see that all the coefficients of the plain images are close to 1, and coefficients the values of the cipher images are close to 0. It shows that our approach reduces the correlation between the adjacent pixels effectively. Fig. 8 shows the correlation distribution of the pixels selected from the three directions of image 'rice' where the adjacent pixels in the plain images are distributed diagonally because of their similar gray levels. Nevertheless, in the cipher image it satisfies random distribution, which shows that our approach satisfies the requirements of confusion and diffusion, too.

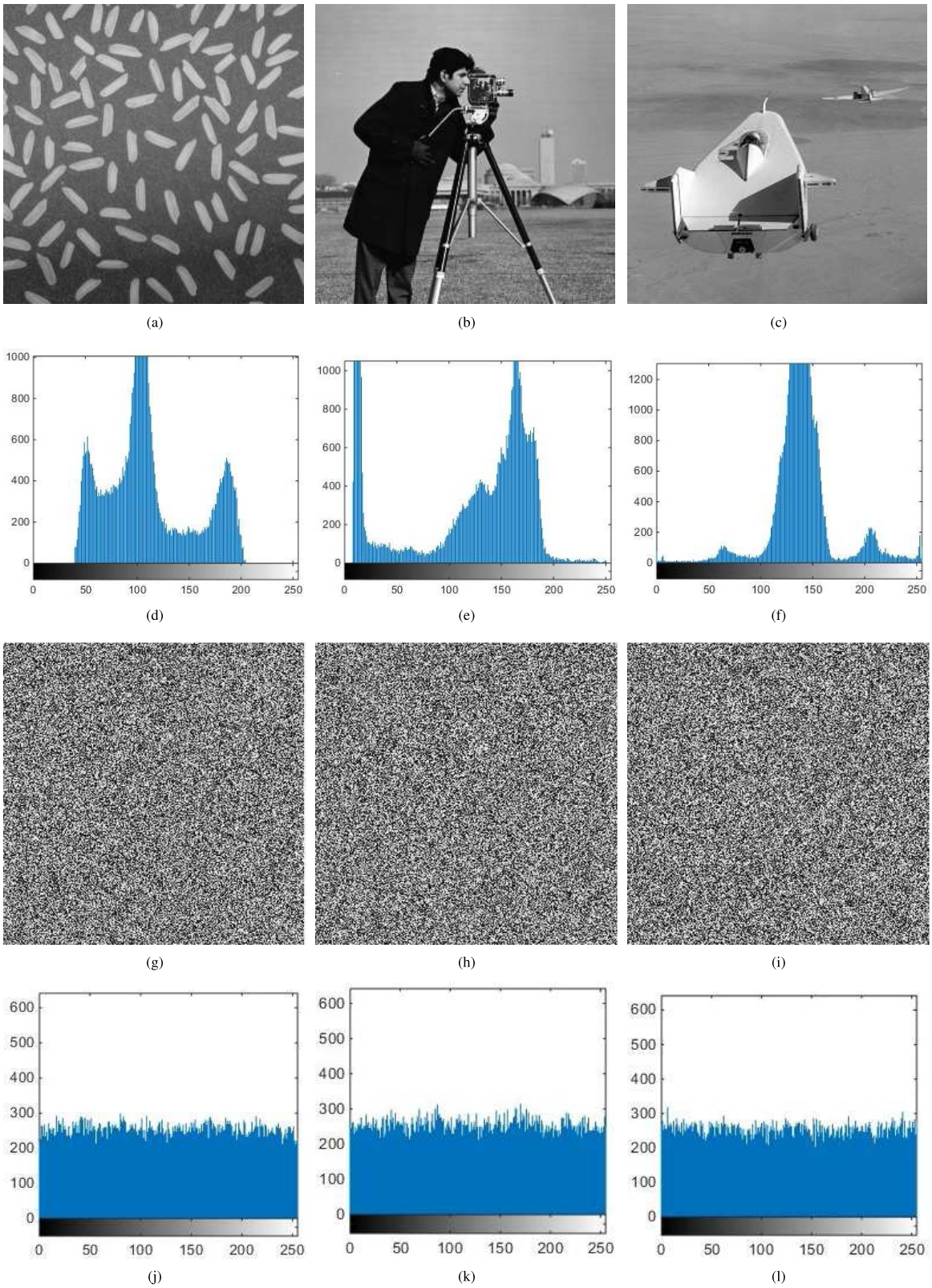


FIGURE 6. Histograms of images of the rice, the cameraman and the lift. (a) rice. (b) cameraman. (c) lift. (d) The histogram of the rice. (e) The histogram of the cameraman. (f) The histogram of the lift. (g) The rice's cipher. (h) The cameraman's cipher. (i) The lift's cipher. (j) The histogram of the rice's cipher. (k) The histogram of the cameraman's cipher. (l) The histogram of the lift's cipher.

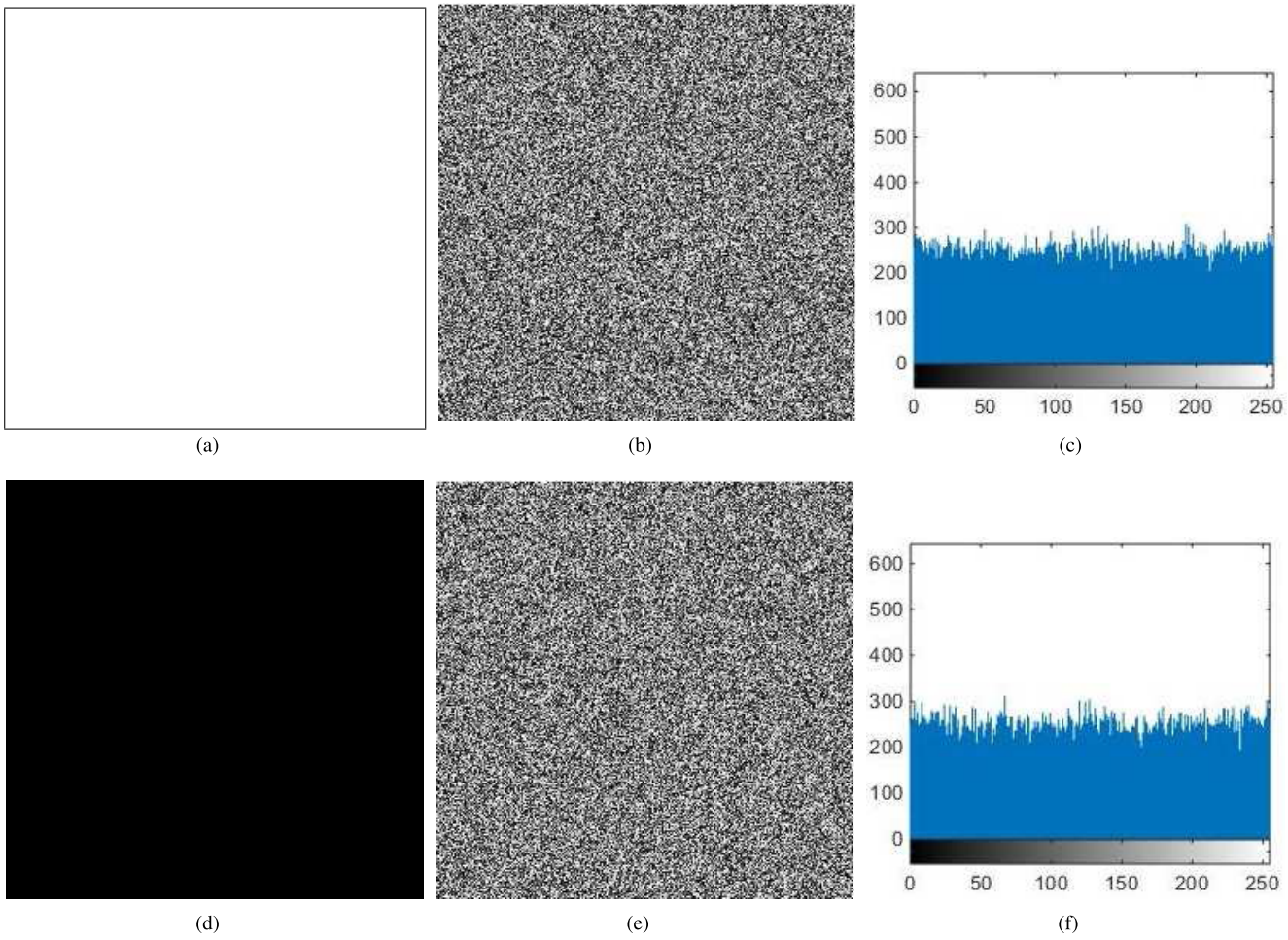


FIGURE 7. Histograms of images with all ones or zeros pixel value, where (a) and (d) are plain images, (b) and (e) are cipher images of (a) and (d), and (c) and (f) are histograms of (b) and (e).

TABLE 4. Correlation coefficients of the horizontal, the vertical and the diagonal directions.

coefficients / Image	Plain image			Cipher image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
rice	0.9430	0.9313	0.9108	0.0105	-0.0451	0.0375
cameraman	0.9639	0.9264	0.9114	0.0287	0.0168	0.0233
lift	0.9511	0.9340	0.9272	0.0022	0.0344	0.0084

D. DIFFERENTIAL ANALYSIS

A differential analysis refers to the influence of slight change in plain image with respect to the cipher image. If a single pixel's change can have a significant influence in the cipher image, that the encryption algorithm is secure against the differential attack is concluded.

Two indexes are used to measure such a influence in the paper, viz., the number of pixels change rate (NPCR) and the unified average changing intensity (UACI), where:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\%,$$

$$UACI = \frac{1}{M \times N} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%,$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j); \\ 1, & otherwise. \end{cases}$$

According to [30], the optimal values of NPCR and UACI are 99.61% and 33.46% respectively. Fig. 9 shows the results of NPCR and UACI with different iterations where quite a few iterations can make NPCR and UACI approach close to their optimal values. Fig. 9 shows that a pixel change in plain image can promptly cause a significant changes in the cipher image, too.

E. KEY SENSITIVITY

According to Shannon's theory, encryption result should be sensitive to any changes in a key. In our algorithm, the key is made up of a pseudo random binary sequence and an iteration number.

To test the key's sensitivity, the following experiments are performed on a 64×64 bits gray image 'rice', viz., Fig. 10(a). We first encrypted the image with $K_0(PR, N = 5)$ to get

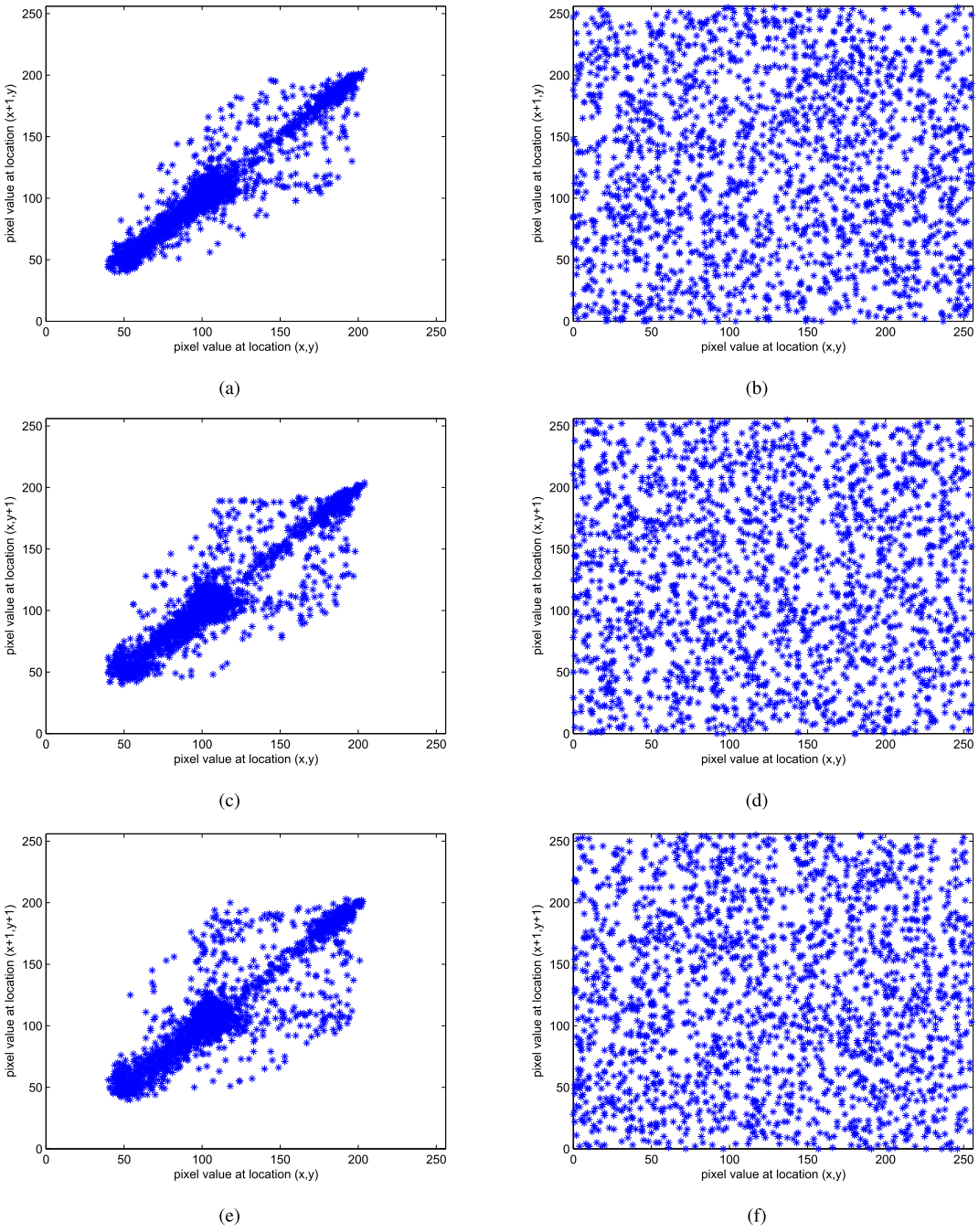


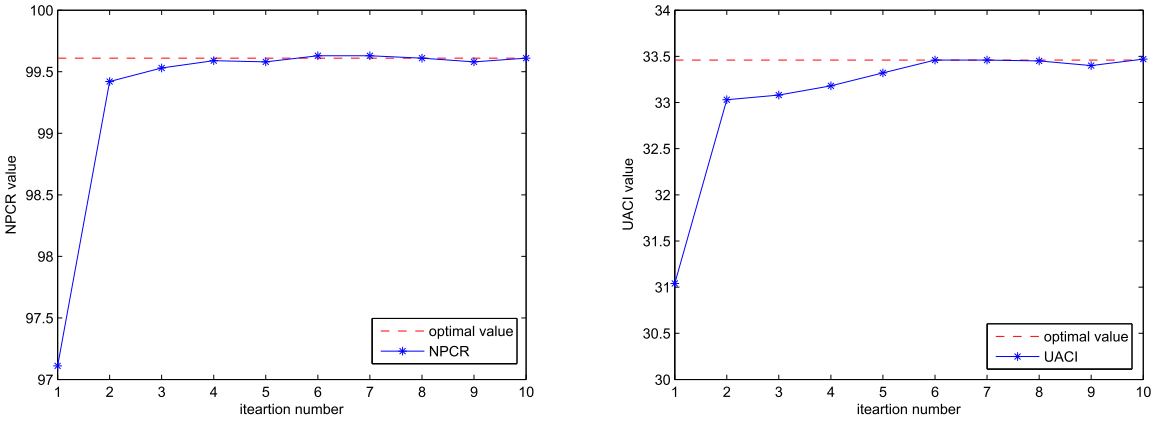
FIGURE 8. Correlation between horizontally, vertically and diagonally adjacent pixels: (a), (c) and (e) are in the plain image; (b), (d) and (f) are in the cipher image.

a reference cipher image C_0, where PR is a 16×64 bits binary sequence, and then we encrypt the plain image with two modified keys $K_1(PR_1, N = 5)$ and $K_2(PR, N = 7)$, where the difference between PR and PR_1 is only one bit. The corresponding cipher images are denoted by C_1 and C_2 respectively, as shown in Fig. 10. In order to present a quantitative illustration, correlation coefficients between C_0 and C_1, C_0 and C_2 are calculated. The values are -0.0196 and 0.0021, respectively, which show that our LCA-based approach is key sensitive.

Fig. 11 shows the decryptions of cipher image C_0 with three different keys K_0, K_1 and K_2, the data show that our approach is key sensitive.

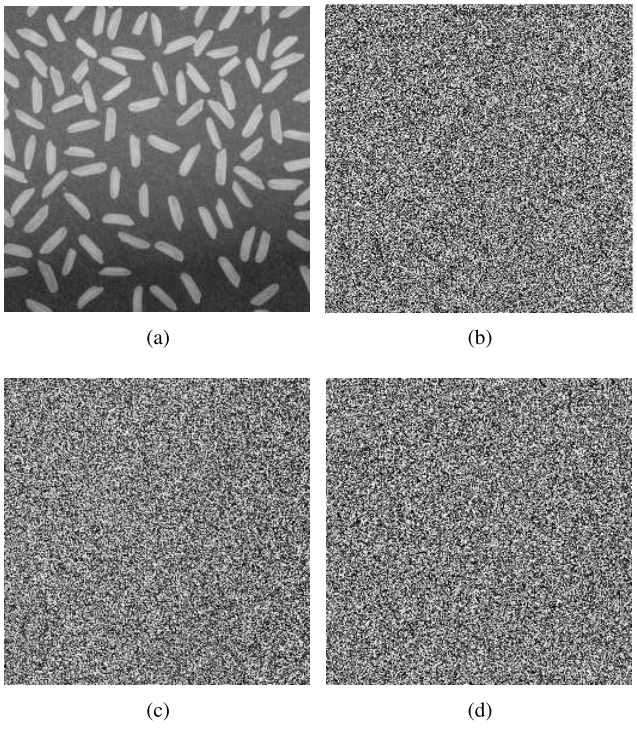
F. BRUTE-FORCE ATTACK

Brute-force attack or exhaustive attack is a basic technique of trying every possible key in turn until the correct key is identified. Theoretically, the size of the key space determines the practical feasibility of performing a brute-force attack [34].



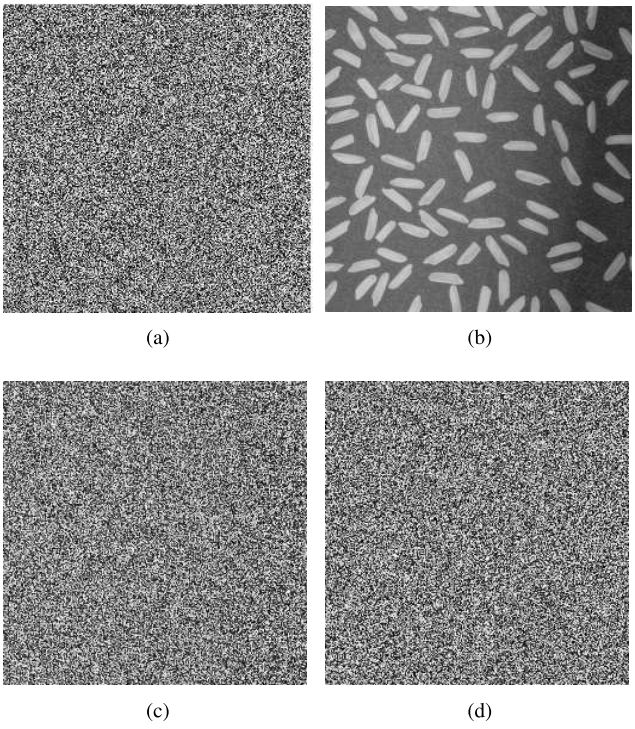
(a) (b)

FIGURE 9. NPCR and UACI values at different encryption iterations.



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

FIGURE 10. Key sensitivity with respect to encryption. (a) Plain image rice. (b) Cipher image C_0. (c) Cipher image C_1. (d) Cipher image C_2.



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

FIGURE 11. Key sensitivity with respect to decryption. (a) Cipher image C_0. (b) Decrypted by K_0. (c) Decrypted by K_1. (d) Decrypted by K_2.

In our method, the key used to encrypt the RoIs in a frame is composed of a pseudo random binary sequence PR and an iteration number N. Let S denote the set of all possible keys, $|S|$ is the cardinality of S. The length of the binary sequence is decided by the size of the encrypted RoI block, which is set as 16×16. Since each bit pair in the binary sequence specifies a transition rule for a 1D CA in the LCA, the same sequence denotes different rule sequences when different mapping function $\mathcal{F}$ is applied. Therefore, the cardinality of S satisfies $|S| > 2^2 \times 4! \times 2^{16\times16} > 2^{262}$, which is larger than that of AES and DES, where the same $|S|$ of AES and DES are 2^{128} (or 2^{192}, 2^{256}) and 2^{56}, respectively.

Note that a frame may has more than one RoIs. In order to reduce the cost of the key's distribution, all RoI blocks in a frame will be encrypted with the same key. Because our approach satisfies the requirements of confusion and diffusion, even if two blocks which have minor differences are encrypted by the same key, the results are far different. Furthermore, a RoI extracted from a frame may be the same as the one from the other frames, those frames will be encrypted

by different keys and hence even the same RoI will show different encryption results. As a result, it's computationally infeasible to launch a key brute-force attack to our approach.

G. PERFORMANCE ANALYSIS

Since CA are natively parallel, CA-based encryption scheme is very efficient in both hardware and software implementations. In the lightweight LCA-based iterative image encryption method proposed in [36], each cell performs rule evolution, transposition and XOR operations for N iterations, the computational complexity is $O(N)$. The results of the performance analysis showed that it is more efficient when compared with some 1D and 2D based encryption methods.

In our LCA-based method, fewer operations are performed for each cell in all RoI blocks than the one in [36]. Only one rule evolution and three shift transformations are involved in each iteration. For N iterations, the computational complexity of our method is $O(N)$, too. Since the RoIs in each frame are organized into blocks and be encrypted independently and synchronously, which contribute to the efficiency of our approach. Furthermore, the results of the above analysis show that even less iteration rounds enable the encrypted blocks to have a good statistical characteristic.

VII. RELATED WORK

Encrypting the RoIs are more practical than to encrypt the entire surveillance video. By far, several types of techniques to encrypt the RoIs in surveillance videos have been proposed.

A permutation-based privacy protection method for surveillance videos was proposed in [4]. It applies permutation in pixel domain to hide private information and tolerates lossy compression and transcoding. The encrypted bitstream is format-compliant with H.264 standard, so it's convenient for transmission and implementation. However, it increases the transport bit rate dependent on the size of the encrypted regions.

Two efficient scrambling techniques applied in transform-domain and codestream-domain for MPEG-4 surveillance videos was proposed in [10], which can be adapted for H.264 videos. In the transform-domain scrambling technique, the sign of selected transform coefficients is pseudo randomly flipped during encoding, which influence the coding efficiency because the length of the coefficients codewords remains identical whenever the coefficient sign is flipped. In the second technique, some bits of the codestream are inverted. Similarly, several scrambling-based privacy protection methods are proposed [13], [14], [38], [39], too. The main advantage of scrambling-based privacy protection techniques is that they are reversible. However, the scrambling-based methods requires high processing power and heavy modification of a compression encoder [40].

An object-based unequal encryption method for H.264 compressed surveillance videos was proposed in [9]. Based on the H.264 bit sensitivity analysis, the bits with the highest sensitivity are encrypted by AES. Note that AES is not suitable for surveillance videos encryption due to its high computational cost.

A chaos-based approach to encrypt privacy sensitive RoIs in video frames has proposed in [6]. This approach supports various levels of abstraction of data hiding according to the authority of the observer. Similarly, a chaos-based encryption method are also proposed in [7]. Some pseudo-random numbers are generated by a chaotic system with an initial seed, and then these numbers are used to encrypt the RoIs to hide the sensitive information. However, chaotic system is not well suited for hardware implementation due to high numerical precision requirements. Hence, it cannot be integrated with a resource-tightened surveillance camera in IoTs.

Since most of the existing RoI encryption methods are focused on the confidentiality of the surveillance videos, the integrity of the RoIs are ignored. To fill such a gap, a lossless RoI privacy protection for surveillance video was proposed in [8]. With this method, the sign of the residual coefficient and intra-frame prediction modes are encrypted by the pseudo-random sequences, which is similar to the method in [13] that can be integrated into the existing surveillance systems.

A moving object detection based RoI encryption method for H.264 videos has been proposed in [12]. The encryption is performed by XOR operation between the luminance coefficients and their key sequence, which does not satisfy the secure requirement though it is easy to be implemented.

VIII. CONCLUSION

Traditional cryptosystems are not suitable for surveillance video encryption due to the high computational costs. A RoI encryption approach based on LCA is proposed. The RoIs are extracted from **I** frames and then being encrypted by our approach and then stored in an IoT device at the camera's side, the new frames without RoIs are re-encoded and then can be viewed on line by any user. The authenticated users can retrieve the original surveillance video with an on-demand manner. Since LCA is a highly parallel system, LCA-based encryption with the simple rules and transformations is inherently efficient and easy to be implemented. Additionally, each RoI is divided into a series of binary blocks and all the blocks are encrypted synchronously, the proposed method satisfies the real-time requirements of surveillance videos. The experimental results show that our approach satisfies both confusion and diffusion encryption requirements and is able to resist brute-force attacks as well as statistical attacks.

ACKNOWLEDGMENT

Many thanks to anonymous reviewers and Prof. Hua Jin for their valuable comments on an earlier version of the paper.

REFERENCES

[1] S. G. Choi, J.-W. Han, and H. Cho, "Privacy-preserving H.264 video encryption scheme," *ETRI J.*, vol. 33, no. 6, pp. 935–944, 2011.

[2] M. I. Khan, V. Jeoti, and M. A. Khan, "Perceptual encryption of jpeg compressed images using dct coefficients and splitting of dc coefficients into bitplanes," in *Proc. Int. Conf. Intell. Adv. Syst.*, 2010, pp. 1–6.
[3] S. Auer, A. Bliem, D. Engel, A. Uhl, and A. Unterweger, "Bitstream-based jpeg encryption in real-time," *Int. J. Digit. Crime Forensics*, vol. 5, no. 3, pp. 1–14, 2013.
[4] P. Carrillo, H. Kalva, and S. Magliveras, "Compression independent reversible encryption for privacy in video surveillance," *Eurasip J. Inf. Secur.*, vol. 2009, no. 1, pp. 1–13, 2010.
[5] A. Unterweger, K. V. Ryckegem, D. Engel, and A. Uhl, "Building a post-compression region-of-interest encryption framework for existing video surveillance systems: Challenges, obstacles and practical concerns," *Multimedia Syst.*, vol. 22, no. 5, pp. 617–639, 2016.
[6] S. M. M. Rahman, M. A. Hossain, H. Mouftah, A. E. Saddik, and E. Okamoto, "A real-time privacy-sensitive data hiding approach based on chaos cryptography," in *Proc. IEEE Int. Conf. Multimedia Expo*, Jul. 2010, pp. 72–77.
[7] S. M. M. Rahman, M. A. Hossain, H. Mouftah, A. El Saddik, and E. Okamoto, "Chaos-cryptography based privacy preservation technique for video surveillance," *Multimedia Syst.*, vol. 18, no. 2, pp. 145–155, 2012.
[8] X. Ma, W. K. Zeng, L. T. Yang, D. Zou, and H. Jin, "Lossless ROI privacy protection of H.264/AVC compressed surveillance videos," *IEEE Trans. Emerg. Topics Comput.*, vol. 4, no. 3, pp. 349–362, Jul./Sep. 2016.
[9] Y. Zhao, L. Zhuo, N. Mao, J. Zhang, and X. Li, "An object-based unequal encryption method for H. 264 compressed surveillance videos," in *Proc. IEEE Int. Conf. Signal Process., Commun. Comput.*, Aug. 2012, pp. 419–424.
[10] F. Dufaux and T. Ebrahimi, "Scrambling for privacy protection in video surveillance systems," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 18, no. 8, pp. 1168–1174, Aug. 2008.
[11] Q. M. Rajpoot and C. D. Jensen, *Security and Privacy in Video Surveillance: Requirements and Challenges*. Berlin, Germany: Springer, 2014.
[12] J. Xu, J. Guo, and J. Bao, "A roi encryption scheme for H.264 video based on moving object detection," in *Proc. Int. Symp. Instrum. Meas., Sensor Netw. Autom.*, 2014, pp. 494–497.
[13] F. Dufaux and T. Ebrahimi, "H. 264/AVC video scrambling for privacy protection," in *Proc. IEEE Int. Conf. Image Process.*, Oct. 2008, pp. 1688–1691.
[14] F. Dufaux, "Video scrambling for privacy protection in video surveillance: Recent results and validation framework," *Proc. SPIE*, vol. 8063, pp. 307–314, May 2011.
[15] Z. Shahid, M. Chaumont, and W. Puech, "Fast protection of H.264/AVC by selective encryption of CAVLC and CABAC for I and P frames," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 21, no. 5, pp. 565–576, May 2011.
[16] A. Pande, P. Mohapatra, and J. Zambreno, "Securing multimedia content using joint compression and encryption," *IEEE MultimediaMag.*, vol. 20, no. 4, pp. 50–61, Oct. 2013.
[17] C. Torres-Huitzil, "Hardware realization of a lightweight 2D cellular automata-based cipher for image encryption," in *Proc. Conf. IEEE 4th Latin Amer. Symp. Circuits Syst. (LASCAS)*, Feb. 2013, pp. 1–4.
[18] A. Kumar and M. K. Ghose, "Substitution-diffusion based image cipher using chaotic standard map and 3D cat map," in *Proc. Inf. Process. Manage.-Int. Conf. Recent Trends Bus. Admin. Inf. Process. (BAIP)*, Trivandrum, Kerala, India, Mar. 2010, pp. 34–38.
[19] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 7, pp. 2943–2959, 2012.
[20] N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, "Quantum image encryption based on generalized Arnold transform and double random-phase encoding," *Quantum Inf. Process.*, vol. 14, no. 4, pp. 1193–1213, 2015.
[21] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system," *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, 2012.
[22] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.
[23] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.
[24] A. A. Abdo, S. Lian, I. A. Ismail, M. Amin, and H. Diab, "A cryptosystem based on elementary cellular automata," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 1, pp. 136–147, 2013.
[25] J. Jin, "An image encryption based on elementary cellular automata," *Opt. Lasers Eng.*, vol. 50, no. 12, pp. 1836–1843, 2012.
[26] S. Nandi, S. Roy, S. Nath, S. Chakraborty, W. Ben A. Karaa, and N. Dey, "1-D group cellular automata based image encryption technique," in *Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol. (ICCICCT)*, 2014, pp. 521–526.
[27] S. A. Hosseini, I. Mohammadi, and S. R. Kamel, "A parallel image encryption based on elementary cellular automata using two processors," in *Proc. Int. Congr. Technol., Commun. Knowl. (ICTCK)*, 2015, pp. 26–27.
[28] P. Ping, F. Xu, and Z. J. Wang, "Image encryption based on non-affine and balanced cellular automata," *Signal Process.*, vol. 105, pp. 419–429, Dec. 2014.
[29] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 11, pp. 3075–3085, 2013.
[30] X. Zhang, C. Wang, S. Zhong, and Q. Yao, "Image encryption scheme based on balanced two-dimensional cellular automata," *Math. Problems Eng.*, vol. 2013, no. 9, pp. 1–10, 2013.
[31] W. Zhi-Jian, "A two-dimensional cellular automata based method for multiple image encryption," in *Proc. CSSS*, 2014, pp. 525–528.
[32] R. Ayanzadeh, K. Hassani, Y. Moghaddas, H. Gheiby, and S. Setayeshi, "Multi-layer cellular automata for generating normal random numbers," in *Proc. 18th Iranian Conf. Elect. Eng. (ICEE)*, 2010, pp. 495–500.
[33] A. Moosavi, "Two-layer cellular automata based cryptography," *Trends Appl. Sci. Res.*, vol. 7, pp. 68–77, Jan. 2012.
[34] C. S. Rao, "Implementation of object oriented encryption system using layered cellular automata," *Int. J. Eng. Sci. Technol.*, vol. 3, no. 7, pp. 5786–5795, 2011.
[35] X. Zhang, R. Lu, H. Zhang, and C. Xu, "A new public key encryption scheme based on layered cellular automata," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 10, pp. 3572–3590, 2014.
[36] X. Zhang, H. Zhang, and C. Xu, "Reverse iterative image encryption scheme using 8-layer cellular automata," *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 7, pp. 3397–3413, 2016.
[37] A. Bakhshandeh and Z. Eslami, "An authenticated image encryption scheme based on chaotic maps and memory cellular automata," *Opt. Lasers Eng.*, vol. 51, no. 6, pp. 665–673, 2013.
[38] L. Tong, F. Dai, Y. Zhang, and J. Li, "Restricted H.264/AVC video coding for privacy region scrambling," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2010, pp. 2089–2092.
[39] J. Jiang, Y. Liu, Z. Su, and G. Zhang, "An improved selective encryption for H.264 video based on intra prediction mode scrambling," *J. Multimedia*, vol. 5, no. 5, pp. 464–472, 2010.
[40] P. Korshunov and T. Ebrahimi, "Using warping for privacy protection in video surveillance," in *Proc. Int. Conf. Digit. Signal Process.*, 2013, pp. 1–6.

XING ZHANG received the B.S. degree from Xuchang University, China, in 2010, and the Ph.D. degree from the Nanjing University of Science and Technology, Jiangsu, China, in 2016. She is currently a Lecturer with the School of Computer Science and Communication Engineering, Jiangsu University. Her research interests include applied cryptography and network security.

SEUNG-HYUN SEO received the B.S., M.S., and Ph.D. degrees from Ewha Womans University, South Korea, in 2000, 2002, and 2006, respectively. Before joining the faculty with Hanyang University in 2017, she was an Assistant Professor with Korea University Sejong Campus for two years. Before that, she was a Post-Doctoral Researcher of computer science with Purdue University for two and half years, a Senior Researcher of the Korea Internet and Security Agency for two years, and a Researcher for three years with the Financial Security Agency, South Korea. She is currently an Associate Professor with the Division of Electronic Engineering, Hanyang University. Her main research interests include cryptography, IoT security, mobile security, secure cloud computing, and malicious code analysis.

CHANGDA WANG was a Visiting Researcher with Carleton University and Purdue University. He is currently a Professor with the School of Computer Science and Communication Engineering, Jiangsu University. His recent research focuses on IoT security, network communication, and cloud computing. He is a member of CCF and serves in the Network and Data Communication Committee. He was a recipient of the Qinglan and Liuda Gaofeng Awards of Jiangsu Province.