A Video-Selection-Encryption Privacy Protection Scheme Based on Machine Learning in Smart Home Environment

Qingshui Xue[1(✉)], Haozhi Zhu[1], Xingzhong Ju[1], Haojin Zhu[2], Fengying Li[2], Xiangwei Zheng[3], and Baochuan Zuo[1]

[1] School of Computer Science and Information Engineering, Shanghai Institute of Technology, Shanghai 201418, China
xue-qsh@sit.edu.cn
[2] Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[3] School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China

Abstract. The Internet of things is a new technological revolution following the computer and Internet. It aims to connect all physical objects existing in the world and forms a network with everything. In recent years, smart home gradually enters into our life. Smart home uses the Internet of things technology to connect all kinds of devices in the home, to achieve a smart home environment. Although the development of smart home has brought a qualitative leap to people's life, there are many problems in security. Privacy security is one of the challenges to the smart home environment. Attackers can intrude various smart devices in the smart home environment, to achieve the purpose of stealing users' personal information and privacy. Among these devices, smart cameras are the most intruded frequently. Since many cameras are installed in users' homes to achieve real-time monitoring of the environment, but the existence of these cameras provides a channel to get information for attackers. In recent years, the leak of video privacy is emerging in an endless stream. According to the researches about privacy protection, this paper proposes a new scheme to selectively encrypt the video captured by the cameras through machine learning technology, so as to protect the personal privacy of users and improve the security of the smart home environment.

Keywords: Internet of things · Smart home · Privacy protection · Machine learning · Video selective encryption

1 Introduction

The Internet of things (IoT) has gradually entered into our lives due to the continuous development of wireless communication technology and brings great changes to our lives [1]. The Internet of things is a new stage in the development of ubiquitous networks based on the Internet. It can be integrated with the Internet over a variety of wired and wireless networks. It integrates the application of a large number of sensors

S. Han et al. (Eds.): AICON 2019, LNICST 287, pp. 65–76, 2019.
https://doi.org/10.1007/978-3-030-22971-9_6

and intelligent processing terminals to achieve the anytime and anywhere connection of objects with objects and objects with people. The Internet of things has led the third wave of the information industry revolution and will become the most important infrastructure for social and economic development, social progress and scientific and technological innovation in the future. By 2020, experts believe that the Internet of things network will contain about 50 billion object entities [2]. By using the Internet of things, everything around us, including computers, mobile phones, cars, etc., will be connected through the wireless network to achieve self-organized communication.

Security is an important factor restricting the rapid development of the Internet of things, which has been mentioned in literature [3–5]. The smart home is one of the best applications of the Internet of things. With the continuous development of the Internet of things technology, the smart home industry is also developing. The smart home is a residential platform, which integrates the facilities related to home life with technologies such as integrated wiring technology, network communication technology, and security prevention technology [6]. A self-organized home network can be formed to share resources and communicate [7], which can build an effective management system of residential facilities and family schedule, improve the safety, convenience, comfort, and artistry of the home, and realize the energy-saving living environment.

The smart camera is an important part of the smart home, which installed in the home to achieve monitoring the home real-time. The video captured by the camera can be transmitted to the storage device via a wireless or wired network, such as a computer or cloud server. The users can view the video when they go home, and can also check the environment of home in real time through the APP terminal on their mobile phone when they are out, so as to ensure that have a grasp of the situation at home. With the continuous development of technology, the smart camera can not only be used for monitor, but also for communication, video, information collection, and other multimedia functions. However, due to the use of these smart cameras, there are also many security issues. Most of the smart cameras on the market are not very secure, and they are easily attacked and exploited by attackers. In recent years, malicious attackers have posted a lot of incidents on the user's video privacy by attacking the cameras, which has brought a lot of troubles and injuries for users. Now, many companies and researchers concerned about the privacy of the home environment and are working hard to improve the security of smart cameras.

In the smart home environment, many places involve the privacy of the user, such as the daily activities of the user at home, the time of the user at home, and the personal preferences of the user [8]. If the attacker obtains information by attacking the cameras, then the users' privacy may be leaked, which will affect the users. It is the most intuitive benefit and the most common attack method for an attacker to obtain the user's personal privacy information by attacking cameras installed at home. Therefore, when users purchase these smart cameras, security is the first consideration for them. Only when the cameras are highly secure, users will be assured to purchase and use them. At the same time, the security of the camera is also the selling point of major companies. Only high-security cameras can survive in the market and bring benefits to the company.

In recent years, researchers have also proposed a lot of video encryption schemes for camera shooting. From these schemes, they can be roughly divided into two categories,

one is full encryption and the other is selective encryption [13]. For full encryption, all data in the video stream is directly encrypted by the encryption algorithm. However, this approach leads to high computational complexity and does not meet real-time requirements. Another type of video encryption is selective encryption. This method encrypts part of the video content, or selectively encrypts, encrypts important or sensitive information. On the premise of ensuring security, selective encryption can not only protect users' privacy but also reduce computational complexity and overhead [13]. So, selective encryption has been widely used in recent years.

As the amount of information in the video data is large, the video should be compressed before being transmitted [14]. Therefore, the relationship between encryption and compression should be considered clearly. It can neither make encryption affect the quality and efficiency of video compression nor can video compression increase the complexity of encryption. Therefore, the best way is to combine encryption and compression. The first to consider this combination is the order of encryption and compression, whether it is compressed before encrypted, or compressed after encrypted, or at the same time, and the order used different, the results obtained are different [13].

In recent years, many researchers have conducted in-depth research on the combination of encryption and compression based on H.264 video coding technology. According to this method of combining encryption and compression, we can filter the information in the process of compression, select important information or sensitive information for encryption [15]. In general, the focus of this encryption method is how to choose the location of the encryption during the compression process [13].

Many scholars have conducted in-depth research on video encryption. Radha et al. [14] proposed a security mechanism based on the measurement matrix to generate secret keys to encrypt video information, but the scheme still encrypts the video completely, although it can guarantee the security of video information, the computational complexity is too large and inefficient. Xu et al. [13] proposed an efficient chaotic pseudo-random number generator to encrypt video data. This scheme can also selectively encrypt video, but it is too complicated to select sensitive information. Based on the above-mentioned selective encryption of video and encrypt some important or sensitive information, our team proposed a new video selective encryption scheme, which utilizes machine learning technology and principle to encrypt video selectively.

Due to the development of video technology at present, the new video coding technology HEVC is becoming more and more mature. Our team chooses the HEVC standard to be applied in the camera to obtain high-quality video information. By combining machine learning, video compression technology, and video encryption, we can selectively encrypt video in an efficient, high-quality and comprehensive way, which can greatly reduce the computational complexity and improve efficiency, as well as improve the security and protect the privacy of users.

We will introduce the process of selective encryption of video through machine learning technology. The rest of the paper is organized as follows. Section 2 introduces the related works and knowledge involved in the scheme. Section 3 introduces the whole process of implementation. In Sect. 4, we do performance and security analysis. Finally, the paper is concluded and look forward to in Sect. 5.

2 Related Works and Knowledge

This section introduces some of the related works about video selective encryption, and relevant knowledge used in our program, including machine learning technology and HEVC coding standard.

2.1 Related Works

Selective video encryption has emerged in recent years, considers the coding structure of the video bitstream and encrypts only the most sensitive information in the video bitstream. There are some research discussed:

Authors in [14] proposed an efficient compressed sensing-based security approach for video surveillance. The solution is applied in wireless multimedia sensor networks. The security keys are generated from the measurement matrix elements for protecting the user's identity. The scheme can achieve selective encryption.

Hamidouche et al. [15] proposed a real-time selective video encryption scheme based on the chaos system. And the solution blends High Efficiency Video Coding (HEVC) standard which named SHVC. The SHVC parameters including TCs, TCsign, MV difference sign.

Authors in [16] have investigated the encryption of Region of Interest based on tiles repartition in HEVC through both selective and naive encryption of the tiles within the Region of Interest.

These schemes can achieve selective encryption. However, they cannot achieve encrypt different people with different secret keys. Our scheme can do this.

2.2 Machine Learning

With the continuous development of technology, many popular emerging technologies, such as artificial intelligence, machine learning, and deep learning have emerged in recent years. Machine Learning is a multi-disciplinary subject, which includes probability theory, statistics, approximation theory and algorithm complexity theory [16]. As the technical basis of artificial intelligence, machine learning not only has the ability to process computer data quickly through algorithms, but also has the ability to predict and classify problems in statistical models, and under the current trend of increasing data volume, there is a huge development potential for it [16]. The goal of machine learning is to study how computers simulate or implement human learning behaviors to acquire new knowledge or skills and reorganize existing knowledge structures to continuously improve their performance [17].

Machine learning is a general term for a class of algorithms that attempt to mine the implicit rules from a large amount of historical data and use them for prediction or classification. More specifically, machine learning can be seen as looking for a function, and input is sample data, the output is the desired result, but this function is too complicated to be formally expressed. It is important to note that the goal of machine learning is to make the learned functions work well for "new samples," not just for training samples. The ability of the learned function to apply to new samples is called generalization ability [18].

2.3 HEVC

Our scheme using the coding technology standard is the High-Efficiency Video Coding (HEVC) standard, a new video compression standard used to replace the H.264/AVC coding standard. HEVC has become an international standard officially, and it has many advantages over H.264, as follows:

(1) Better compression
Compared to the H.264 codec, HEVC offers significant improvements in compression. In fact, HEVC compresses video twice as efficiently as H.264. With HEVC, video of the same visual quality takes up half the space. Or, videos with the same file size and bit rate can exhibit better quality [19].

(2) Improved inter-frame motion prediction
A major factor in video compression is the prediction of motion between frames. When the pixel remains stationary (solid-state background image), the intelligent video codec can save space by referencing it instead of reproducing it. With improved motion prediction, HEVC can provide smaller file sizes and higher compression quality [19].

(3) Improved inter-frame prediction
Video compression also benefits from analyzing the "movement" within a single frame, which allows for more efficient compression of a single frame of video. This can be achieved by using a mathematical function instead of the actual pixel value to describe the pixel layout [20]. This feature takes up less space than pixel data, reducing file size. However, the codec must support sufficiently advanced mathematical functions to make the technology really work. HEVC's interframe prediction function is more detailed than H.264, which supports motion prediction in 33 directions, while the latter only supports 9 directions [21].

HEVC coding technology has many advantages, and it is now more and more widely used. Although the mature of HEVC coding technology may take some time, it is inevitable that it will become the future video coding standard. Therefore, combined with the Internet of things technology in the smart home environment, the use of HEVC coding standard for smart cameras will become popular.

3 The Video-Selection-Encryption Privacy Protection Scheme Based on Machine Learning in a Smart Home Environment

In this section, we will introduce the implementation process of our scheme in detail, which will elaborate on the definition of privacy in the home environment, image classification and character recognition, and privacy protection.

3.1 Definition of Privacy in the Home Environment

Privacy of individual refers to the secrets of citizens who are unwilling to disclose or known for others in their personal lives. In modern society, the quality of citizens is constantly improving, and the requirements for quality of life are constantly improving, the awareness of the protection of personal privacy is also constantly strengthening, and the security of personal privacy is also valued. Personal privacy includes many aspects, including personal data privacy, location privacy, identity privacy, behavioral privacy and environmental privacy [6]. They are inviolable and indispensable for building a happy and harmonious society. Therefore, the protection of personal privacy is very important.

In the smart home environment, the entire home environment belongs privacy category for the user, including all activities of the family's characters, schedules, and personal preferences. These personal privacy screens are captured during the entire surveillance of the camera, so it is necessary to encrypt these video images that involve the user's personal privacy. However, there is more than one person in the home, and everyone has privacy. Hence, the people at home, do not want privacy to be accessed by attackers, also not want privacy to be accessed by the others who at home. So, it is necessary to encrypt each person's video image individually to achieve protect everyone privacy. Besides, an image will include both the character and the background, we just need to encrypt the character in the image to protect the privacy of the person. The problems are how to classify these video images taken by the smart camera and how to recognize the person and select the character area for encryption. The scheme we proposed will achieve this function. This issue is being discussed in detail in succeeding paras.

3.2 Image Classification and Character Recognition

Before the smart cameras are put into use, the first thing what should we do is make the smart cameras to be smarter. We need to design a machine learning algorithm, the function of this algorithm is to distinguish different images. And then, the algorithm will be implanted into the smart cameras when it is mature so that the smart cameras can distinguish different character images. Therefore, the key to achieve this function is how to choose an appropriate algorithm, and how to set different labels, and how to train the algorithm. These issues are being discussed in detail in succeeding paras.

Choose an Appropriate Algorithm. Machine learning has many algorithms, different algorithms achieve different functions. As deep learning is a branch of machine learning, and the convolutional neural network algorithm of deep learning is very suitable for image classification [23]. Therefore, we choose a convolutional neural network (CNN) as an appropriate algorithm. The convolutional neural network is a multi-layer neural network, each layer is composed of multiple two-dimensional planes, and each plane is composed of multiple independent neurons (as shown in Fig. 1). The input image is convolved with three trainable filters and a bias. After the convolution, three feature maps are generated in the C1 layer, and then the four pixels

of each group in the feature map are summed, weighted, and offset [23]. The feature maps of the three S2 layers are obtained through a sigmoid function. These maps are then filtered to the C3 layer. This hierarchy then generates S4, just like S2. Finally, these pixel values are rasterized and connected into a vector input to the traditional neural network to obtain the output [24].

Set Different Labels. We assume that there are three people at home, such as user1, user2, user3. The cameras will take abundant images, and these images involve the three people's privacy. It is necessary to distinguish them. Hence, we set the images which involve the user1 as label-1, the images which involve the user2 as label-2, and the images which involve the user3 as label-3. And consider the outsiders, we set outsiders as OS. Then, collect thousands of images of user1, user2 and user3, and use them to train algorithm.

Training Algorithm. For an algorithm to become mature, it must undergo extensive samples training. The training steps of convolutional neural network algorithm are divided into four steps, and the four steps between two stages [24]. The first stage, forward propagation stage: ① take a sample (X, Yp) from the sample set and input X into the network; ② calculate the corresponding actual output Op. The second stage is the backward propagation stage: ① calculate the difference between the actual output Op and the corresponding ideal output Yp; ② the weight matrix is adjusted by back propagation according to the method of minimizing error [25]. So, we according to the steps to train the algorithm that we design. First, give about thousands of images with label-1 to the algorithm, and make the algorithm can tell which image belongs to the label-1 image and recognize the person in the image is user1 and mark the character area. Second, through the same process, make the algorithm can tell which image belongs to the label-2 image, label-3 image, and recognize the person in the image is user2 or user3 and mark the character area. After the algorithm becomes mature, embed it into the smart camera. Hence, the smart camera can classify the three kinds of label images automatically.

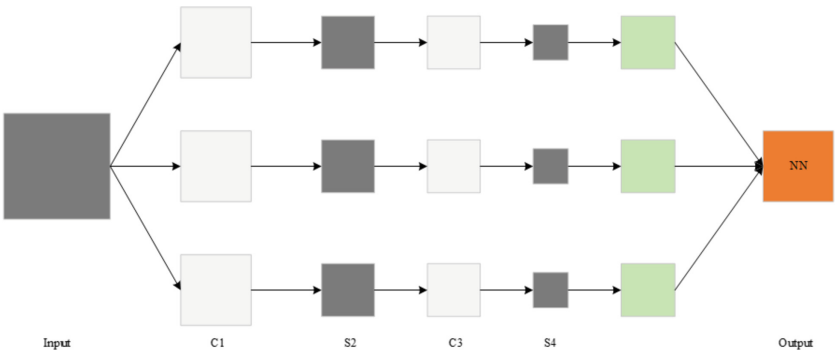

Fig. 1. Structure of the convolutional neural network

3.3 Privacy Protection

After the above introduction, the cameras installed at home have the ability to intelligently recognize and can classify different images that involve different people. Therefore, smart cameras can selectively encrypt images according to classification. So, the key is how to encrypt these images. The issue is being discussed in detail in succeeding paras.

Because video data is huge and it's a real-time stream of data, fast encryption is required, we choose AES (128bits) as the encryption algorithm of our scheme. As mentioned above, we supposed there are three users at home, user1, user2 and user3. And after the camera classification, the camera can identify the users in the image and mark them. In order to be able to encrypt them separately, it is necessary to generate three different secret keys, such as K_1, K_2 and K_3. Besides, the K_1 belongs to user1, and only encrypts the area of images which involve user1. The K_2 belongs to user2, and only encrypts the area of images which involve user2. The K_3 belongs to user3, and only encrypts the area of images which involve user3. And we also need to generate a separate key, such as K. The K used to encrypt the area of images which the camera can't identify, for example, outsiders (OS). When the camera is in the process of shooting, there will be countless frame images. We study on the basis of one frame of the images. Before the camera encrypts the images, it numbers every frame image which it takes. The specific encryption process is as follows.

Step 1: The camera selects a frame image.
Step 2: The camera determines if there are any characters in the image. If there is no one in the image, the camera does nothing to this image and continues to select the next frame image. If there is somebody in the image, go to step 3.
Step 3: The camera determines which the user in the image is, and recognizes the user. After that, confirms the position of the character in the image, and uses the four corners of the rectangle to determine the coordinates of the character in the image. The coordinates are defined as (A_i, B_i, C_i, D_i) (i represents the user of the image). For example, the user is user1.
Step 4: The camera uses the K_1 to encrypt the identified character rectangle area information data. The others are the same as user1.
Step 5: Make the number of the frame, the user number, the user's position and time in the frame image are stored in a table in the local database(as shown in Table 1).

After the above steps, each frame of the image is selectively encrypted (as shown in Fig. 2). When the users want to view the encrypted video, they need to decrypt it. The decryption process is as follows.

Step 1: When the user wants to view the video for a certain period of time, use the ID of each frame in the video during this time to look up the record of that frame in the table.
Step 2: Determines the location to be decrypted and the decryption key to use.

Step 3: Determines the identity of the decryptor and decrypt the encrypted region in the frame image with the decryptor's secret key. For example, the user1 wants to decrypt the video, then uses K_1 to decrypt the video. Besides, the user1 only can view the video about himself. The others are the same as user1.

The above is the whole process of encryption and decryption. The process of encryption can selective encryption exactly and do the record so that the process of decryption can be done quickly.

Table 1. The information recorded in each frame

Frame ID	User ID	Coordinates	Frame Time
1	User1	(A_1, B_1, C_1, D_1)	Time 1
	User2	(A_2, B_2, C_2, D_2)	
	User3	(A_3, B_3, C_3, D_3)	
	OS1	(A, B, C, D)	
	…	…	
2	User1	(A_1, B_1, C_1, D_1)	Time 2
	User2	(A_2, B_2, C_2, D_2)	
	User3	(A_3, B_3, C_3, D_3)	
	OS1	(A, B, C, D)	
	…	…	
…	User1	(A_1, B_1, C_1, D_1)	…
	User2	(A_2, B_2, C_2, D_2)	
	User3	(A_3, B_3, C_3, D_3)	
	OS1	(A, B, C, D)	
	…	….	
n	User1	(A_1, B_1, C_1, D_1)	Time n
	User2	(A_2, B_2, C_2, D_2)	
	User3	(A_3, B_3, C_3, D_3)	
	OS1	(A, B, C, D)	
	…	…	

Fig. 2. The result of selective encryption

4 Performance and Security Analysis

In this section, we analyze the performance and security of our scheme. Our scheme aims at implementing selective encryption for video, so that reduces computational complexity and reduces overhead. Compared with other schemes, our scheme incorporates machine learning and HEVC standard to achieve encryption for video. Privacy information in the video can be classified and encrypted quickly, efficiently and with high quality by our scheme. Besides, our scheme also achieves real-time encryption. And our scheme encrypts everyone in the home separately.

Considering security, our scheme is resistant to various passive and active attacks.

① **The cameras' gateway by breached**

In order to make the cameras secure, the first step is authentication security, so that the attacker cannot easily break through the cameras. We assume that the attacker has already broken into the cameras and can check the situation at home. Our scheme is to encrypt the video shot by the camera in real time. Every frame shot by the camera is encrypted for the privacy involved, so the scheme is relatively safe.

② **The attacker obtains the stored video file**

When attacker stole the video file, it's hard to decrypt it, because the video images that involve privacy are encrypted by AES algorithm, which security is very high, and it is hard for attackers to get the key.

③ **The attacker obtains one of the keys of users**

When the attacker obtains one of the keys of users, for example, the user's K_1 is stolen, the attacker just can decrypt the video images which involve user1, the others video images are still secure. So, our scheme can protect privacy well.

5 Conclusions

In this paper, an efficient video-selective encryption scheme is proposed based on machine learning and HEVC. In our scheme, we just propose a new method to achieve selective encryption for video. After theoretical analysis, it indicates that our scheme can encrypt video quickly and efficiently. Due to our goal is not to design a new encryption algorithm, so we choose the traditional encryption algorithm AES as our scheme algorithm.

Although our scheme can improve encryption efficiency and reduce computational complexity, there are still some problems that require follow-up work. The proposed scheme of applying machine learning technology to smart cameras to protect privacy is still in the feasibility stage of theoretical research and requires follow-up work for feasibility experiments. And there are still not many related articles found to study machine learning applications to protect user privacy in the smart home environment.

Besides, there is a problem exist in our scheme, when the people in the image overlap, the camera doesn't mark the area very well, so, need further study. Considering the development of technology and the maturity of IoT technology, these smart cameras will become more and more intelligent, their size will be smaller and smaller, and most of them are in the wireless environment, they are used to collect multimedia information. So, resource limitation is an important issue. Their computing power and

storage capacity are not very high. It is necessary to study a more suitable lightweight cryptography to encrypt the video.

At present, our team only applies the research environment of the scheme to the smart home. Considering the superiority of machine learning for selective video encryption, this scheme can continue to be applied in more fields, such as smart cities. Covered with a large number of smart cameras throughout the city, these cameras can monitor well. But due to the presence of these large number of smart cameras, and they are distributed in every corner of the city, most of them are in an unsafe channel and are vulnerable to be attacked, many of the people and environments captured by these cameras are in the privacy category. Once they are used by attackers, it will cause great harm. However, most cameras are in a public environment, most of the information is not in the privacy category. At this time, the video can be selectively encrypted by machine learning technology, and only the video information related to the privacy category can be encrypted, which can improve the privacy security of urban people and reduce the overhead and computational complexity. We will then conduct in-depth research on its application in smart cities to explore better privacy protection options.

Acknowledgments. This paper is supported by NSFC under Grant No. 61672350 and 61373149, NSSFC under Grant No.16BGL003, Ministry of Education Fund under Grant No. 39120K178038 and 14YJA880033, SIT Collaborative innovation platform under Grant No. 3921NH166033, and SIT Foundation for Distinguished Scholars under Grant No. 39120K176049. We are also grateful for the support of the National Natural Science Foundation of China (61170227).

References

1. Xiaolei, D.: Advances of privacy preservation in internet of things. J. Comput. Res. Dev. **52**(10), 2341–2352 (2015)
2. Ping, Q., Meng, W.: Survey on privacy preservation in IoT. Appl. Res. Comput. **30**(01), 1001–1008 (2013)
3. Zhihao, Y., Li, M., Chunping, H.: Internet of Things Security Technology. Tsinghua University Press, Beijing (2016)
4. Masum Sadique, K., Rahmani, R.: Towards security on internet of things: applications and challenges in technology. Procedia Comput. Sci. **141**, 199–206 (2018)
5. Miorandim, D., Sicari, S., De Pellegrini, F.: Internet of things: vision, applications and research challenges. Ad Hoc Netw. **10**(7), 1497–1516 (2012)
6. Yinghui, Z., Robert, H.: Secure smart health with privacy-aware aggregate authentication and access control in internet of things. J. Netw. Comput. Appl. **123**, 89–100 (2018)
7. Lu, Z., Jiguo, Y., Chuanqing, H., Honglu, J.: Fine-grained access control with privacy support and network service optimization in ad hoc networks. Procedia Comput. Sci. **129**, 372–374 (2018)
8. Kevin, A., Katia, O., Leland, M.: Solar-powered, wireless smart camera network: an IoT solution for outdoor video monitoring. Comput. Commun. **118**, 217–233 (2018)
9. Charlie, W., Tom, H., et al.: Benefits and risks of smart home technologies. Energy Policy **103**, 72–83 (2017)
10. Frédéric, B., Kevin, B., Gaboury, S.: Tracking objects within a smart home. Expert Syst. Appl. **113**, 428–442 (2018)

11. Burrows, A., Coyle, D., GoobermanHill, R.: Privacy, boundaries and smart homes for health: an ethnographic study. Health Place **50**, 112–118 (2018)
12. Min, L., Wenbin, G., Wei, C.: Smart home: architecture, technologies and systems. Procedia Comput. Sci. **131**, 393–400 (2018)
13. Hui, X., Xiaojun, T., Xianwen, M.: An efficient chaos pseudo-random number generator applied to video encryption. Optic **127**, 9305–9319 (2016)
14. Aasha Nandhini, S., Radha, S.: Efficient compressed sensing-based security approach for video surveillance application in wireless multimedia sensor network. Comput. Electr. Eng. **60**, 175–192 (2017)
15. Hamidouche, W., Farajallah, M., Sidaty, N.: Real-time selective video encryption based on the chaos system in scalable HEVC extension. Signal Process. Image Commun. **58**, 73–86 (2017)
16. Mousa, F., Wassim, H., Olivier, D.: ROI encryption for the HEVC coded video centents. In: IEEE International Conference on Image Processing, ICIP, Spain, Barchalona, pp. 3096–3100 (2015)
17. Santiago, L., Rafael, M.: Using machine learning to detect and localize concealed objects in passive millimeter-wave image. Eng. Appl. Artif. Intell. **67**, 81–90 (2018)
18. Assem Mahmoud, A., Mai, A.: A time-efficient optimization for robust image watermarking using machine learning. Expert Syst. Appl. **100**, 197–210 (2018)
19. Sheng, H., Lambert, S.: Deep adaptive learning for writer identification based on single handwritten word images. Pattern Recogn. **88**, 64–74 (2019)
20. Shengtao, Y., Cheolkon, J., Qiaozhou, L.: HEVC encoder optimization for HDR video coding based on irregularity concealment effect. Sig. Process. Image Commun. **64**, 68–77 (2018)
21. Sami, J., Mohamed-Chaker, L., Jamel Belhadj, T.: Low complexity intra prediction mode decision for 3D-HEVC depth coding. Signal Process. Image Commun. **67**, 34–47 (2018)
22. Xiaojie, L., Wenpeng, D., Yunhui, S.: Content adaptive interpolation filters based on HEVC framework. J. Vis. Commun. Image R. **56**, 131–138 (2018)
23. Xing, X., Xiaopeng, S., Chunhui, D.: Captcha recognition based on deep learning. J. Test Measur. Technol. **33**(02), 138–142 (2019)
24. Hong, H., Liang, P., Zhongzhi, S.: Image matting in the perception granular deep learning. Knowl.-Based Syst. **102**, 51–63 (2016)
25. Yuan, J., Xingxing, H., Yaoqiang, X., Da, C.: Multi-criteria active deep learning for image classification. Knowl.-Based Syst. **172**, 86–94 (2019)