Local Chaotic Encryption Based on Privacy Protection on Video Surveillance

Suolan Liu and Lizhi Kong

Changzhou University, Jiangsu, China, 213164

lan-liu@163.com

Keywords: Pedestrian detection; Face localization; Encryption; Chaotic map

Abstract. Privacy protection has been a hot research topic in recent years with the widely application of surveillance systems. Most developed mechanisms focused on modifying the monitored targets partly or wholly in the surveillance scenes. These methods are usually irreversible of privacy protection and have negative influences on the subsequent action recognition in intelligent monitoring system. In this paper, a novel privacy preserving scheme is produced by only encrypting human face region. To properly localize human face, we firstly do pedestrian detection and then extract face region by using skin color information in YCbCr color space, which is the predominant difference between face and other parts of a person. Furthermore, an improved spatial chaotic map is developed to encrypt face region. The performance evaluation on a video clip with complex background shows that the proposed scheme can effectively and robustly track pedestrian and obscure the face region in real time.

Introduction

Recently, privacy protection has been a sensitive and hot topic with the increasingly deploying of video surveillance systems [1-3]. On one hand, with the rapid improvements of network performance and multimedia applications, private videos in the network space have been frequently exposed. On the other hand, whether you like it or not, video surveillance has provided great help to public security and been widely applied in airports, supermarkets, roads, banks and communities. Therefore, how to balance the requirements between application and privacy preserving has been an urgent problem [4]. In general, there are two kinds of methods can be used to address these issues. Firstly, related laws should be made to regulate videos acquisition, storage, usage and transmission. The purpose of video collection is mainly used by law enforcement agencies; therefore, any unauthorized person should not be allowed to watch and use it. Both law enforcement agency and the individual should provide secure storage to avoid malicious infringement and disclosure of private information [6,7]. And then for the users who maliciously use and spread of videos should have corresponding laws and regulations to punish them. Secondly, some technical measures such as data encrytion and video hiding techinique can be employed to protect the applications [8]. For an example, multiple digital chaotic systems based on chaotic video encryption scheme (CVES) can provide high security for fast and real-time encryption and be independent of any video compression algorithms. However, this method is mainly used to scramble the whole image, which results in the interference of the watching and recognition of human activities but is good for storage and transmission. Actually, most of the conventional encryption algorithms such as Data encryption standard (DES), International data encryption algorithm (IDEA), Diffe-Hellman and Elliptic curve cryptography (ECC), etc. work as protect the whole content of digital images/ videos instead of partial sensitive information, and can not be directly utilized to protecting privacy on monitoring application [9-11].

In this paper, we address this issue by proposing a novel privacy preserving method based on local encryption. Instead of encrypting a whole image frame, we only select and detect the face from human body to scramble. Furthermore, an improved spatial chaotic map is developed to encrypt face region, which can provide both high efficiency and rather good security by expanding its key space.

The rest of this paper is organized as follows. In Section 2, we review previous work related to privacy protection on video surveillance. Section 3 gives the proposed framework. Face is localized based on human detection and image local encryption based on chaotic map is described. In section 4, simulation results are reported. Finally, concluding our work in section 5.

Related Work

Recently, privacy protection has been a sensitive and hot topic with the increasingly deploying of video surveillance systems [1-3]. On one hand, with the rapid improvements of network performance and multimedia applications, private videos in the network space have been frequently exposed. On the other hand, whether you like it or not, video surveillance has provided great help to public security and been widely applied in airports, supermarkets, roads, banks and communities. Therefore, how to balance the requirements between application and privacy preserving has been an urgent problem [4]. In general, there are two kinds of methods can be used to address these issues. Firstly, related laws should be made to regulate videos acquisition, storage, usage and transmission. The purpose of video collection is mainly used by law enforcement agencies; therefore, any unauthorized person should not be allowed to watch and use it. Both law enforcement agency and the individual should provide secure storage to avoid malicious infringement and disclosure of private information [6,7]. And then for the users who maliciously use and spread of videos shoud have corresponding laws and regulations to punish them. Secondly, some technical measures such as data encrytion and video hiding techinique can be employed to protect the applications [8]. For an example, multiple digital chaotic systems based on chaotic video encryption scheme (CVES) can provide high security for fast and real-time encryption and be independent of any video compression algorithms. However, this method is mainly used to scramble the whole image, which results in the interference of the watching and recognition of human activities but is good for storage and transmission. Actually, most of the conventional encryption algorithms such as Data encryption standard (DES), International data encryption algorithm (IDEA), Diffe-Hellman and Elliptic curve cryptography (ECC), etc. work as protect the whole content of digital images/ videos instead of partial sensitive information, and can not be directly utilized to protecting privacy on monitoring application [9-11].

The Proposed Method

Pedestrian Detection and Face Localization

Automatic face detection is viewed as the first step in many applications such as face recognition, face tracking and intelligent video surveillance. However, face changes with these factors like variations in illumination, position, orientation and accessories, which will result in great difficulties for directly extracting facail region from an image. Motived by the success in pedestrian detection, our work begins with full-body detection and then localizes face region based on the first step. For doing this, the sliding window classifiers based on three-frame difference and optical flow proposed in [9] is used to detect pedestrian. The following task is to localize face region of each pedestrian in the adaptive bounding boxes. Since skin color is the predominant difference between face and other parts of a person, color information can be used as an efficient clue for identifying facial region. As reported in [10-11], skin color based method works effectively only on the chrominance subspaces of Cb-Cr and H-S. Therefore, in YCbCr color space, the next two rules are formulated to search face candidates [12,14].

$$|f_{Cb}(x,y) - \mu_{Cb}| < \gamma\sigma_{Cb} \tag{1}$$

$$|f_{Cr}(x,y) - \mu_{Cr}| < \gamma\sigma_{Cr} \tag{2}$$

where (μ_{Cb}, σ_{Cb}) and (μ_{Cr}, σ_{Cr}) are the parameters of Gaussian distriution. $f(x,y)$ denotes the value of a pixle with coordinates (x,y) in chrominance component Cb or Cr. γ is a adjusting parameter, $\gamma > 0$.

Rules (1) and (2) are combined by the logical operator “AND” to obtain candidates. By this processing many isolated pixels may be present, a morphological closing operation with a 5×5 mask [13] as experimentally applied to converge them into a relative region. Therefore, the interference from these regions such as eyes and mouth will be effectively supressed. Besides this, in candidates there may be some regions with small areas. To eliminate false candidates, in every detection pedestrian region only the candidate with area more than 625 pixels is preserved as used in [14].

Chaotic Encryption for Face Concealing

Researchers have proposed a large number of encryption methods based on discrete systems, which can be roughly divided into the following categories: value transformation, position scrambling, multiple chaotic systems, the high dimensional chaotic system, multiple iterativeof the chaotic system and other technologies. However, most of these methods are fragile to the deciphers who have exposed the inherent defects of these encryption systems. To improve security, spatiotemporal chaotic system is widely applied to chaotic cryptography because of its superior chaotic dynamic performance. Motived by its success, in this paper an improved encryption method based on spatial chaotic map is developed to conceal face region.

The two dimensional spatial difference of the chaotic map can be expressed as follows:

$$x_{s+1,t} + wx_{s,t+1} = M(\mu, (1+w)x_{s,t}) \tag{3}$$

where $M(\mu, (1+w)x_{s,t})$ is a nonlinear function. s, t, $x_{s,}$ are geometric coordinates in the three dimensional space. μ and w are parameters.

To logistic map, formula (3) can be rewritten as:

$$x_{s+1,t} + wx_{s,t+1} = 1 - (\mu, (1+w)x_{s,t})^2 \tag{4}$$

Especially, when $1.55 \leq \mu < 2$ and $w \in (-1,1)$, the system shows chaotic state.

To facilitate encyption process, we resize the detected facial region in a square by valuing its center with mean value and width is two times of the maximum distance out-of-the mean value.

After scrambling, every pixel value of the image is decimal. Then we convert the decimal number into binary number and obtain a new matrix $B(i,j)$. The final image can be produced by the following formula:

$$R(i,j) = \big(B(i,j) + O(i,j)\big) mod\ 2\ )\otimes C(i,j) \tag{5}$$

Where $0 \leq i \leq M-1, 0 \leq j \leq N-1$, $O(i,)\ and\ C(i,j)$ are scrambling matrixes produced by formula (4).

Implementation and Results

In this section, we test the performance of our proposed method by choosing a video clip with life scenarios. The backgrounds are cluttered and changing with views. Especially, the colors of clothes are similar with human skin, which will increase the difficulty of face extraction. The operations including human detection, face localization, encryption and decryption will be conducted in Matlab running on a laptop. The experimental results are shown in Figure.1 and Figure.2.

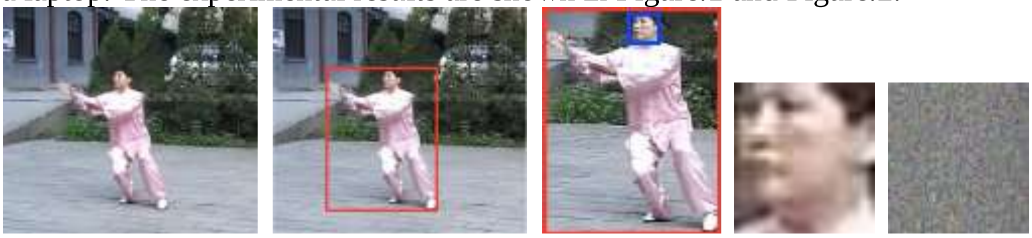

Figure.1 Examle A of face detection and encryption

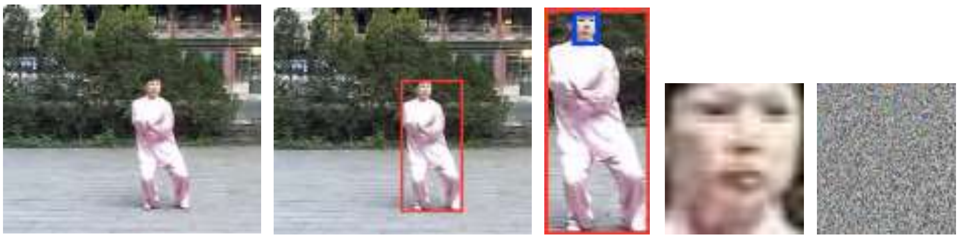

Figure.2 Example B of face detection and encryption

As displayed in the above two figures, from left to right there are orignal frame, human detection result, face localization, closeup of face region and encrypted result. Obviously, by using our proposed method human face can be effectively detected even though great interference from clothes are appeared. The performances verify that the proposed approach can be performed in real time for the need of privacy perserving with challenging and complex surveillance scenes.

Conclusion

To protect privacy on video surveillance, in this paper a novel scheme is proposed, which includes these processing steps: human body detection and tracking, face region localization and spatial chaotic encryption. By tracking the whole human body, we can effectively detect and localize the face. Test results demonstrate our method can suppress the interference from background and enviroment and encrypt human face properly.

Acknowledgements

This work is supported by National Natural Science Foundations of China (61572085, 61502058), Jiangsu Joint Research Project of Industry, Education and Research (BY2016029-15) and Changzhou Science and Technology Support Program (Social Development) Project (CE20155044).

References

[1] Shujun Lia, Xuan Zhengb, Xuanqin Moua. Chaotic Encryption Scheme for Real-Time Digital Video, Proceedings of SPIE 2002

[2] P Zhang, T Thomas, M Kankanhalli. Privacy Preserving Video Surveillance Using Pedestrian Tracking Mechanism, Acm Workshop on Multimedia in Forensics, 2010

[3] P Carrillo, H Kalva. Compression Independent Reversible Encryption for Privacy in Video Surveillance. Journal on Information Security. 2009, 1-13

[4] Y Ban, S Kim, S Kim, K Toh. Face detection based on skin color likelihood.Pattern Recognition, 2014 , 47 (4) :1573-1585

[5] J Meyneta, V Popovicib, J Thiran. Face detection with boosted Gaussian features. Pattern Recognition, 2007, 40 : 2283–2291.

[6] J Chen, Z Zhu b, C Fu, H Yu. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Commun Nonlinear Sci Numer Simulat , 2015,20: 846–860

[7] A Kadir, M Aili, M Sattar. Color image encryption scheme using coupled hyper chaotic system with multiple impulse .injections. Optics & Lasers in Engineering, 2017, 129 :231-238

[8] G Chen, Y Mao, C Charles. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos,solitons and fractals, 2004, 20:749-761

[9] A Halidou, X You,. Fast pedestrian detection based on region of interest and multi-block local binary pattern descriptors. Computers and Electrical Engineering, 2014, 40: 375–389

[10] S Gundimada, L Tao and V Asari. Face Detection Technique based on Intensity and Skin Color Distribution. ICIP2004: 1413-1416

[11] S Phung, A Bouzerdoum and D Chai. A Novel Skin Color Model in YCbCr Color Space and its Application to Human Face Detection. ICIP2002: 289-292

[12] N Anwar, A Rahman. RGB-H-CbCr Skin Colour Model for Human Face. http://pdfs.semanticscholar.org/b1c6/f513e347ed9fbf508bd67f763407fa6d5ec6.pdf

[13] S Liu, C Chen. A Computationally Efficient Denoising and Hole-filling Method for Depth Image Enhancement. SPIE Conference on Real-Time Image and Video Processing 2016（9897）: 1-8

[14] C Czirjek, N Connor, Smarlow. Face detection and clustering for video indexing applications. 2003, http://schema.iti.gr/SCHEMA/files/document/10-06-2004/ACIVS2003.pdf