ISSN 2277-3061
Volume 16 Number 1
INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

A NEW COMBINATION METHOD FOR ENCRYPTION OF MOVING OBJECTS DETECTION IN VIDEO

Nguyen Trong Nhan[1], Ye Dengpan[2]
[1, 2] School of Computer, Wuhan University, Hubei, China
trongnhanth1b@yahoo.com
[1]Dong Thap University, Vietnam

ABSTRACT

Nowadays surveillance systems have been widely deployed in various places and generate massive amount of video data every day. This raises threats of unauthorized access and potential privacy leakage as the recorded videos usually contain rich identifiable information such as facial biometrics. In order to mitigate the threats, many existing methods perform symmetric encryption on the entire frames in the videos. Unfortunately, these methods could introduce additional computation cost and storage. Moreover, as surveillance systems could be a part of distributed system, the key management is critical and challenging. In this paper, we propose a novel method which incorporates background subtraction technique and RSA encryption algorithm. Rather than encrypting the entire frames of the videos, the proposed detect the regions around moving objects in the frames of video and then perform RSA encryption on the detected regions. And RSA encryption technique has its advantages of key distribution and management. Our experimental results show that the proposed method only involve moderate computation cost and storage.

Keywords

Background subtraction, Object detection, Computer vision, RSA, Encryption.

1. INTRODUCTION

The appearance of computer vision allows us to acquire a video from camera vision and to process them. Combination of images from camera and stored images on a computer for processing has formed smart surveillance systems as well as automatic systems in public places, traffic surveillance systems, so on. Surveillance systems are widely deployed in many places and generate massive amount of video data every day. This raises threats of unauthorized access and potential privacy leakage as rich identifiable information is usually contained in the recorded videos.

Currently, there are many algorithms for encoding objects in video that prevent unauthorized access data. Recently, ROI [7] has performed encryption in the region of containing object to apply in H.264 video. In ROI, the area of moving object is detected by Gaussian Mixture Model (GMM) and then XOR operation is performed between coefficient of luminance and secret key to encrypt objects. However, ROI encryption is symmetric encryption. It use a secret key that needs to be shared among the people who needs to receive the message thus anyone who knows the secret key can decrypt the message. The key management and distribution for symmetric encryption technique could introduce additional challenges and risk of compromised secret keys.

To improve security, we propose a new combination method to encrypt the region of around moving objects in video and to prevent unauthorized access to the data application on RGB standard. Firstly, our method utilizes background subtraction method to identify moving objects in the video. Then the identified moving objects are encrypted and encoded by asymmetric encryption algorithms which have advantages of secure and convenient key distribution and key management.

Among the asymmetric encryption algorithms, RSA is typical and popular asymmetric encryption. It uses a pair of public key, and a private key to encrypt and decrypt messages when communicating. Any messages that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key. Therefore, we use RSA algorithm as encryption and encoding technique.

We further implement our proposed method and conduct experiments on real-word video data from surveillance system in order to validate the effectiveness of the method. Our experimental results show that the proposed method achieves reasonable performance in encrypting and decrypting video of surveillance at moderate computational costs.

2. SOLUTION

2.1 Background subtraction technique

Object detection is the process of finding instances of real-world objects, such as faces, bicycles, and buildings in images or videos. Object detection algorithms typically use extracted features and learning algorithms to recognize instances of an object category. It is commonly used in applications, such as image retrieval, security, surveillance, and automated vehicle parking systems

Background subtraction technique[8] is mainly used when system has static background. It means system has been fixed to camera. This technique detects moving object by subtracting the current image pixel-by-pixel from a reference background image. Reference image is created by averaging images over time from using the first few frames. The pixels with the above difference, some threshold value are declared as foreground pixel. To improve quality of detected foreground regions (to remove noise), some post processing operation such as morphological erosion and dilation can be used. The reference background image is updated over time to adjust with dynamic scene changes. There are many variation approaches existed in literature for background subtraction. A pixel at location (x, y) in the current image is marked as foreground if

$$| I_t(x,y)- B_t(x,y) | > T \qquad (1)$$

Condition is satisfied where T is a predefined threshold. The background image is updated by the use of following equation.

$$B_{t+1} = \alpha\, I_t + (1- \alpha)\, B_t \qquad (2)$$

After classifying all foreground pixels, morphological closing and opening operation are used to eliminate the small sized regions. This technique is sensitive to dynamic changes i.e. when stationary objects uncover the background or sudden illumination changes occur.

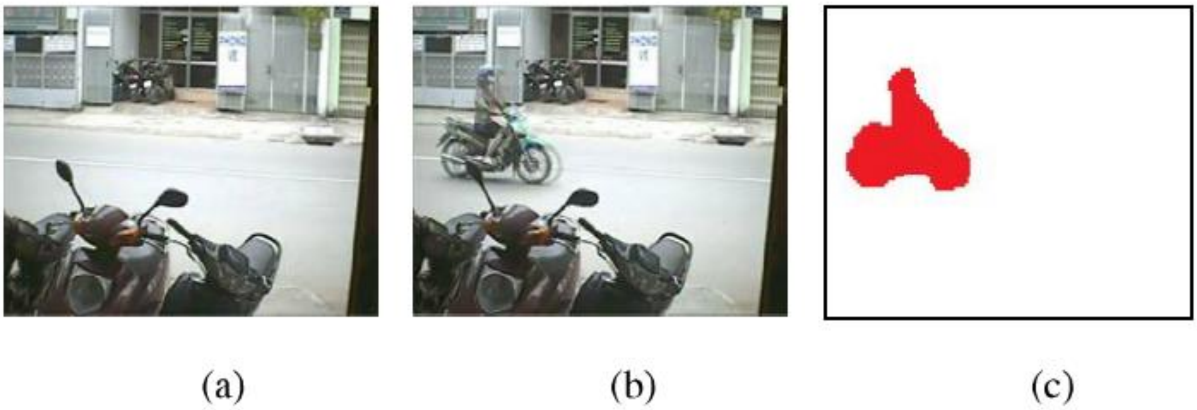

Figure 1. (a) background image, (b) get image at next step

(c) image result from background subtraction technique [9]

2.2 Asymmetric Encryption (RSA)

RSA [5] algorithm has two keys: a public key (or a communal key) and a secret key (or an private key). Each key is the use of fixed numbers during encoding and decoding. The public key is publicly accessible to everyone and is used for encryption. Any messages that are encrypted by using the public key can only be decrypted by applying the same algorithm, but by using the matching private key. Any message that is encrypted by using the private key can only be decrypted by using the matching public key

The formula for encoding and decoding according to the following algorithm

Encryption

$$c = m^e \bmod n \qquad (3)$$

Decryption

$$m = c^d \bmod n \qquad (4)$$

Including:

- m: the initial data
- e, n: the public key
- c: the encrypted data
- d: the private key

Solution to determine the public key e, n and the private key d is done as follows:

Step 1: Select two random prime numbers to distinguish between p and q (the bigger, the better)

Step 2: n = p * q

Step 3: Calculate the result of Euler function Φ (n) = (p-1) * (q-1)

Step 4: Choose e so that 1 <f <Φ (n) (e is relatively prime (or coprime) with Φ (n))

Step 5: Calculate d so that Φ d mod (n) = 1

2.3 Implementation of encryption and decryption

Encryption: After a moving object in the video is detected by background subtraction method, it will be encrypted and encoded with a public key by RSA algorithm.

Decryption: After an encrypted object is detected by background subtraction method, it will be decrypted and decoded with a private key of RSA algorithm.

The process of encryption and decryption is performed on the RGB color image frame.

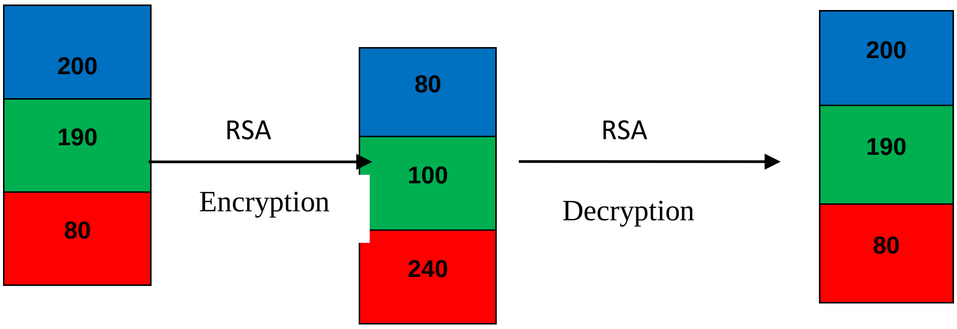

Figure 2. The process of encryption and decryption at 1 pixel of an object

3. EXPERIMENTAL RESULT

The experimental result using the language C ++, library functions processing image and video in OpenCV 2.4. Using pre-recorded AVI files.

Results of encryption

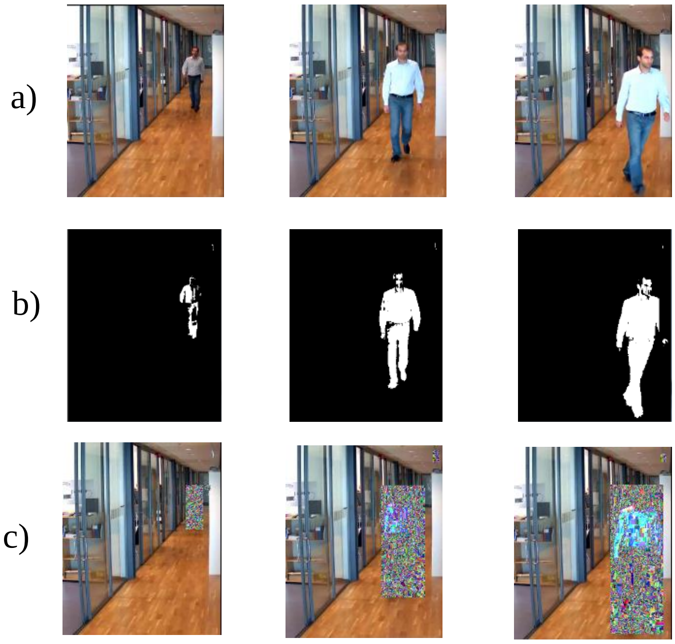

Figure 3. Results of encrytion

a) The initial frame; b) The object detection frame after applying background subtraction method; c) The encoding object frame

Results of decrytion

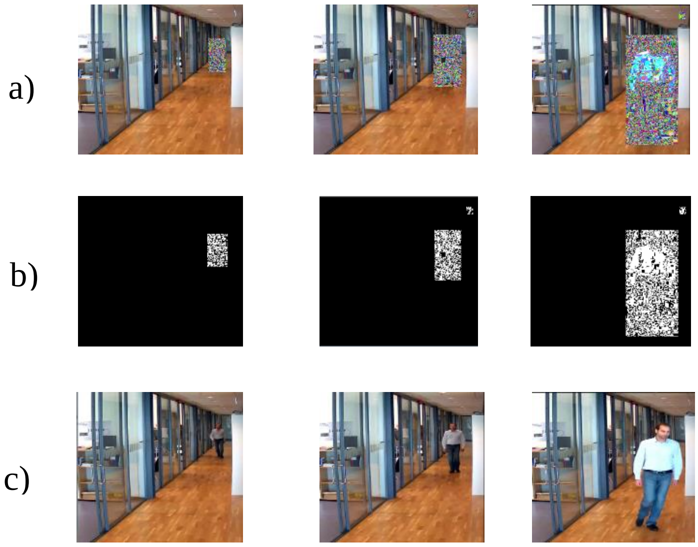

Figure 4. Results of decrytion

a) The encrypted object frame; b) The object detection frame after applying background subtraction method; c) The decoded frame returning the initial frame.

4. CONCLUSION

In this paper, we propose a novel method that combines background subtraction method and RSA encryption algorithm to protect the privacy and security of video data in surveillance systems. The proposed method automatically detect moving objects in the video and use RSA algorithm to encrypt and encode the regions of the detected moving objects rather than the entire frames in the video for efficiency. The experimental results show that our method is practical and secure and can be deployed into automatic distributed video surveillance systems.

REFERENCES

[1] Ali Arya and Farzin Farhadi-Niaki, ”*An Implementation on Object Move Detection Using OpenCV*”, Department of Systems and Computer Engineering Carleton University Ottawa, Canada, 2010.

[2] Anil K. Jain, “Biometrics: A Tool for Information Security”, IEEE transactions on information forensics and security, Vol. 1 (2), pp.125-142, 2006

[3] B. Babenko, M.-H. Yang, and S. Belongie, “Robust object tracking with online multiple instance learning”, IEEE Trans. Pattern Anal. Mach. Intell., Vol. 33(8), pp. 1619 –1632, 2011.

[4] Bradski, G., Kaehler, “Learning OpenCV: Computer Vision with the OpenCV Library”, O’Reilly Media Inc., Sebastopol, CA, 2008

[5] Evgeny Milanov, “The RSA Algorithm”, Univerity of Washington, 2009

[6] Jessica Ebert, Jennie Shipley, “Computer vision based method for fire detection in color videos”, Connecticut College, Utah State University, 2010

[7] Jiayun Xu, Jie Guo, “A ROI encryption scheme for H.264 video based on moving object detection”, 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation, 2013

[8] M. Piccardi, “Background subtraction techniques: a review” in IEEE Int. Conf. on Systems, Man and Cybernetics, 2004.

[9] Paresh M. Tank, Darshak G. Thakore, “A Fast Moving Object Detection Technique In Video Surveillance System”, International Journal of Computer Science and Information Technologies, Vol. 3(2), pp. 3787-3792, 2012

[10] Stutz, T. and Uhl, A., “A Survey of H.264 AVC/SVC Encryption”, Circuits and Systems for Video Technology, IEEE Transactions on,22(3) , pp.325-339, 2012

[11] Trần Thanh Việt, Trần Công Chiến,..”Một kỹ thuật phát hiện, bám sát đối tượng và ứng dụng”, Information Resource Center, Lac Hong University, 2012