Future Generation Computer Systems 55 (2016) 344–352

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Secure privacy vault design for distributed multimedia surveillance system

Sk. Md. Mizanur Rahman [b,*], M. Anwar Hossain [a], Mohammad Mehedi Hassan [b], Atif Alamri [b], Abdullah Alghamdi [a], Mukaddim Pathan [c]

[a] College of Computer and Information Sciences (CCIS), King Saud University, Riyadh, Saudi Arabia
[b] Research Chair of Pervasive and Mobile Computing, King Saud University (KSU), Riyadh, Saudi Arabia
[c] Telstra Corporation Limited, 10/35 Collins St, Melbourne, VIC 3000, Australia

HIGHLIGHTS

- Identification of privacy leakage channels by means of privacy leakage trees.
- A secure privacy vault design for distributed surveillance system.
- Robust against different security and privacy attacks.
- Different attack models (White-box, Gray-box, or Black-box) have been considered.

ARTICLE INFO

Article history:
Received 26 December 2013
Received in revised form
17 July 2014
Accepted 9 October 2014
Available online 20 November 2014

Keywords:
Distributed multimedia surveillance system
Video surveillance
Privacy-preserving surveillance
Data hiding
Secure privacy vault

ABSTRACT

Distributed multimedia surveillance systems utilize heterogeneous sensors such as cameras, motion sensors, sound sensors, and RFID in order to provide safety and security to people. However, due to the potential of exposing privacy by these systems, many people are reluctant to be electronically monitored and suffer from privacy loss. In order to overcome this dilemma, the current surveillance systems should adopt improved privacy preservation (i.e. hiding people's face) mechanism while they are used for typical surveillance tasks. This paper takes a holistic approach to identify the different privacy leakage channels in the distributed video surveillance context and proposes the design of a secure privacy vault to conceal privacy-sensitive data obtained from distributed visual sensors. It also shows how the proposed solution helps to mitigate the potential privacy leakage problems at different levels of the leakage channels. In order to demonstrate the viability of the proposed approach, we further provide the privacy leakage attack model as well as the security analysis of the proposed solution.

1. Introduction

Recently, we witness a significant interest in surveillance technologies due to the increased security threats around our surroundings. As a result, distributed multimedia surveillance systems are being deployed in different premises to ensure public safety and security. However, the increased presence of these systems often lead to privacy violation (i.e. exposing privacy-sensitive information) that is sensitive issue to civil liberty [1,2]. Therefore, it is important to develop improved privacy preserving technique for the surveillance systems such that these systems can be used for effective surveillance tasks while protecting people's privacy at the highest level.

Researchers have been investigating several approaches to address the privacy preservation issues. Dominant approaches are scrambling and data hiding methods [3–8], cryptographic encryption [2,9], and access control policy [10,11]. The scrambling and data hiding approaches usually first identify the regions of interest in video data that are potentially privacy-sensitive, and scramble that region to minimize the chance of privacy leakage. The cryptographic encryption approach, among other things, hides privacy information of video using watermark, while the access control strategy restricts the access of surveillance feeds to authorized users only.

Despite the above works, there is still a lack of a formal and comprehensive framework towards effective privacy preservation. At one hand, we need improved method for privacy safeguarding,

* Corresponding author. Tel.: +966 11 4676394.
E-mail addresses: mizan@scientist.com, mizan@ksu.edu.sa (Sk. Md. Mizanur Rahman).

http://dx.doi.org/10.1016/j.future.2014.10.019
0167-739X/

while on other hand we need to be aware of the different privacy leakage points. In this proposal, we updated our previous work [12] and provide a privacy leakage channel analysis for distributed surveillance system and developed a secure privacy vault to keep the secret keys of scrambled privacy sensitive regions of interest in distributed surveillance video.

This paper identifies privacy leakage channels by means of privacy leakage tree analysis and proposes the mitigation of these leakage channels by designing a secure privacy vault for distributed surveillance system. Thus, the main contribution lies in the design of a secure privacy vault, which preserves the privacy information securely. The cornerstone of this approach is that even if the privacy vault is stolen, the privacy information cannot be disclosed to the public by breaking the vault without compromising the higher level authorities of the target environments. Considering the different attack models, such as White-box, Gray-box, or Black-box, the proposed privacy vault can be implemented in different hostile environments to protect the privacy information in the surveillance video footage.

The remainder of the paper is organized as follows. Section 2 explores some related work followed by the description of background mathematics in Section 3 to clearly understand the proposed mechanism. The analysis of the privacy leakage channels is discussed in terms of privacy leakage tree (PLT) in Section 4. The overview of the proposed privacy preserving mechanism of a distributed multimedia surveillance system is given in Section 5. The privacy leakage attack model is elaborated in Section 6, while the security analysis of the proposed model is illustrated in Section 7. Finally, the conclusion is drawn in Section 8.

2. Related work

There are several related works that have a common goal of concealing privacy sensitive information to minimize privacy loss due to wide scale surveillance. These falls into the category of scrambling and data hiding, cryptographic encryption, and access control. We briefly comment on these works in the following.

Dufaux and Touradj Ebrahimi [3] proposed a code stream-domain scrambling technique that provides better scrambling result based on code-stream transformation, which pseudo randomly inverts some of the bits of AC coefficient in the target Region of Interest (ROI). Hosik Sohn et al. [13] propose a surveillance system that provides scalable video coding, ROI scrambling, and compressing. In this approach, first the images are split using Flexible Macroblock Ordering (FMO), then the FMO type 2 (rectangles over areas of ROI) are applied. The spliced sets are then forwarded to ROI scrambling and pseudo random sign inversion to AC coefficients. Shen Jie and Zheng Xiao Yu [4] describe that using the public key of the receiver the sender computes symmetric key to encrypt the seeds, the digital envelope is made by receivers public key. The receiver opens the envelope using its private key and obtains symmetric key and sends acknowledgment to sender. Sender sends scrambled seeds to the receiver and receiver uses symmetric key to decrypt the seeds and decode the scrambled coefficients.

Like the scrambling techniques, which aim to scramble the ROIs in surveillance videos, data hiding is another technique that aims the same. Isabel Martinez-ponte et al. in [6] proposed a face masking technique to hide faces in motion JPEG data. M.D. Swanson et al. [14] proposed a technique to hide high bit-rate supplementary data by pixels in the video format. Moncrieff et al. [8] suggest general techniques like data hiding, context awareness, data equity to embedded into surveillance systems to ensure that the privacy of the people is safeguarded against the increasing number of attacks on the surveillance systems. Authors in [15] proposed a compression independent approach to selectively encrypt regions that reveal identity using permutation-based encryption in the pixel domain. The work in [16] uses an obfuscation technique that uses a video console to determine the sensitive parts of the video and obscures that part in a way that the recognition software cannot identify that part. This approach is irreversible and hence is not suitable for actual surveillance needs. Another approach in [17] proposed to decrease the quality of ROI in JPEG2000, which ensures varying visual quality from poor to near invisibility. It works in bitstream domain and dependent on compression standard used. This approach is also irreversible and hence does not meet critical surveillance needs.

In our earlier work [2] we adopted cryptographic approach to also hide privacy sensitive ROIs in surveillance video. This technique takes inputs from the video surveillance data and compresses the RoI using the Chaos Encryption based on the logistic functions and mappings. J.M. Rodrigues et al. [9] proposed a method to partially encrypt the face in video sequence. This method is based on Advanced Encryption Standard (AES) stream ciphering using variable length coding of the Huffman's vector. Besides, Newton et al. [18] used a de-identification technique to hide face regions, which prevents traditional face recognition techniques to identify the original face. The actual hiding of face is done by blacking out the face. However, their approach conserves several facial properties such as eigenvectors of the original face and based on the similarity matrix of the faces they restore new faces that resemble the original face but not exactly the same as the original.

Video surveillance privacy and confidentiality are also addressed using sophisticated access control policy with which sensitive information embedded video segments will only be accessed by authorized personnel [10,19]. This approach is restricted in the sense that all the surveillance operators will require adequate access rights in order to continue monitoring the video footage and hence privacy concerns will be compromised. In a recent work [20], a different approach to privacy loss protection in surveillance is proposed, which emphasizes on identifying the location, time and activities in video footage in addition to people's faces. Unlike the above works, we identify the privacy leakage channels in video surveillance from video capture to video storage and access and propose a secure privacy vault that preserves the key information to hide the privacy sensitive regions in video.

3. Mathematical background

3.1. Discrete Cosine Transformation (DCT)

Discrete Cosine Transformation (DCT) [21] is used to compress MPEG-4 video [22] by applying on 8×8 pixel blocks. In a matter of fact, DCT is a linear and invertible function, defined as $f : \Re^N \longrightarrow \Re^N$. Equivalently, it is defined as an $N \times N$ invertible square matrix. Thus, let $F(x) \longrightarrow \alpha(\theta)$ and $G(x) \longrightarrow \beta(\theta)$, then $C_1F(x) + C_2G(x) \longrightarrow C_1\alpha(\theta) + C_2\beta(\theta)$.

3.2. Pseudo-Hadamard Transformation (PHT_r)

Consider the N-bit integers x, y, χ, and γ, i.e., $|x| = |y| = |\chi| = |\gamma| = N$. Let, transformation of x is denoted as $PT_r(x) = \chi$ and the transformation of y is denoted as $PT_r(y) = \gamma$. Therefore, the inverse transformation of χ, denoted as $PT_r^{-1}(\chi) = x$, and the inverse transformation of γ, denoted as $PT_r^{-1}(\gamma) = y$. Thus, the transformed x can be computed as $\chi = (x + y)\ mod\ 2^N$; and transformed y can be computed as $\gamma = (x + 2y)\ mod\ 2^N$. On the other hand x, and y can be computed from χ and γ as $x = (2\chi - \gamma)\ mod\ 2^N$ and $y = (\gamma - \chi)\ mod\ 2^N$, respectively. Detail description on Pseudo-Hadamard Transformation can be found in [18].