Pattern Recognition 59 (2016) 302–311

Contents lists available at ScienceDirect

Pattern Recognition

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

Video anomaly detection based on locality sensitive hashing filters

Ying Zhang [a], Huchuan Lu [a,*], Lihe Zhang [a], Xiang Ruan [b], Shun Sakai [b]

[a] School of Information and Communication Engineering, Dalian University of Technology, Dalian 116023, China
[b] OMRON Corporation, Kusatsu, Japan

ARTICLE INFO

Article history:
Received 4 July 2015
Received in revised form
8 October 2015
Accepted 20 November 2015
Available online 12 December 2015

Keywords:
Anomaly detection
Locality sensitive hashing filters
Optimal hash function
Online updating

ABSTRACT

In this paper, we propose a novel anomaly detection approach based on Locality Sensitive Hashing Filters (LSHF), which hashes normal activities into multiple feature buckets with Locality Sensitive Hashing (LSH) functions to filter out abnormal activities. An online updating procedure is also introduced into the framework of LSHF for adapting to the changes of the video scenes. Furthermore, we develop a new evaluation function to evaluate the hash map and employ the Particle Swarm Optimization (PSO) method to search for the optimal hash functions, which improves the efficiency and accuracy of the proposed anomaly detection method. Experimental results on multiple datasets demonstrate that the proposed algorithm is capable of localizing various abnormal activities in real world surveillance videos and outperforms state-of-the-art anomaly detection methods.

1. Introduction

Intelligent video surveillance plays an irreplaceable role in safe city construction due to the ability of understanding and analyzing the monitoring contents using techniques such as computer vision. As an important part of intelligent video surveillance, video anomaly detection can automatically detect the abnormal events in the monitoring scene and produce alarms to assist the security officers to deal with the unexpected events.

1.1. Related work

There have been proposed various approaches [1–11] for anomaly detection in recent years. Most methods follow the principle that abnormal events rarely occur are different from the normal training observations. Specifically, in [1,12,13], the normal training samples are employed to reconstruct the test samples, of which the samples with large reconstruction error will be considered as abnormal. It is worth mentioning that Zhao et al. [1] introduced the dictionary updating with new observations to adapt to the scene changes in testing phase.

Another kind of methods tries to build a normal activity model, and the behaviors of low compatibility with the model will be detected as anomalies. The Markov Random Field (MRF) model is utilized in [2,14] to characterize the distribution of normal motion patterns or co-occurrence patterns, and the maximum a posteriori (MAP) is computed to estimate the abnormal degree of the test sample. In [3,15–17] the Hidden Markov Model (HMM) is presented to describe the temporal and spatial relationship between and statistics of local motion patterns, and the confidence measure of the new observations is captured to reject anomalies. While Mehran et al. adopted social force model (SFM) in [4] to depict the individual motion dynamics and interaction forces in crowds for anomaly judgements. Chen et al. [11] decomposed a complex behavior using a cascade of Dynamic Bayesian Networks (CasDBNs) for the detection of subtle anomalies in surveillance videos. Hiroyuki et al. [18] proposed the Normality Sensitive Hashing (NSH) where a set of hash functions are selected that instances within the normal region are allocated into the same bucket while instances across the region boundary are assigned to different buckets.

Similarities of the test samples to the training data are computed in [19–21,9], where the samples with low similarities will be given high abnormal scores in the test videos. Clustering [21] and sub-class discovering [20] were proposed to reduce the computation cost in training phase. Some other algorithms were also designed for anomaly detection such as scan statistics [7], chaotic invariants [6], multiple fixed-location monitors [22], and energy model based methods [10,23,24].

In this paper, we propose a novel framework based on Locality Sensitive Hashing Filters (LSHF) for anomaly detection in video scenes. To build the normal activity model, training videos are hashed by LSH functions into a list of buckets with each bucket represented as a miniature filter, and the abnormal degree of a test sample is estimated by its nearest filter. Consider that the scene context tends to change over time, we introduce an online

* Corresponding author. Tel./fax: +86 411 84708971.
E-mail address: lhchuan@dlut.edu.cn (H. Lu).

http://dx.doi.org/10.1016/j.patcog.2015.11.018
0031-3203/

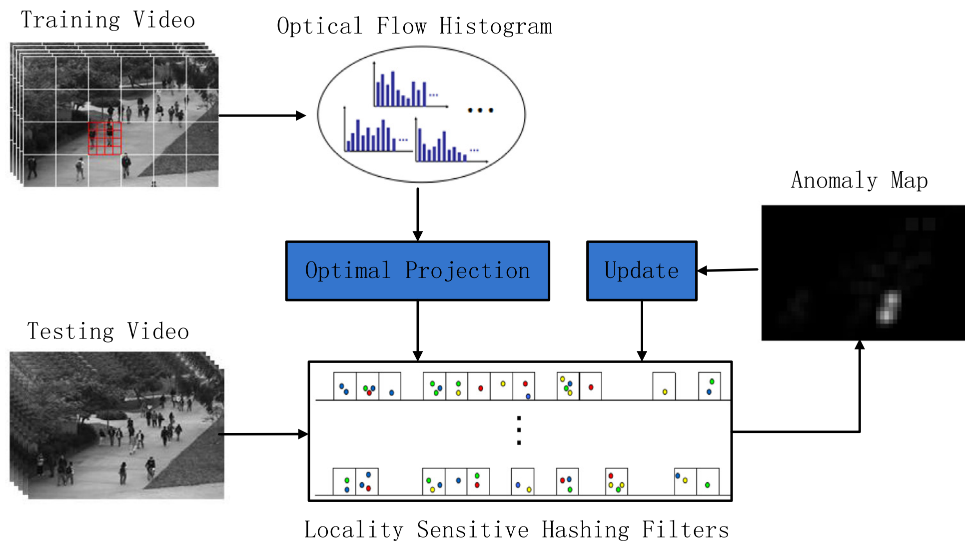

Fig. 1. Overview of anomaly detection algorithm.

updating mechanism, where the new normal behaviors will be added into the LSHF model and the outmoded miniature filters will be removed. Moreover, we develop a new evaluation function to evaluate the LSH functions and adopt the Particle Swarm Optimization (PSO) algorithm to search for the optimal hashing functions. The LSHF built by the optimal functions shows remarkable advantages by increasing the accuracy of anomaly detection. The overview of our approach is shown in Fig. 1.

It should be noted that the Normality Sensitive Hashing (NSH) [18] has also made improvements on LSH for anomaly detection, which selects a set of hash functions to define a normal region and instances across the region boundary are regarded as abnormal. However, the feature data usually scatter in the high-dimensional space, and the normal region surrounded by a number of hyper-planes may be so large that the abnormal points are easily incorporated, which may greatly reduce the detection rate. On the other hand, by selecting the hash functions minimizing the objective function from random candidates, the NSH may be unstable to get the optimal solution. In contrast, we build a list of buckets as a fine partition of the data, which can filter out abnormal events with higher detection rate. We estimate the anomalies by both considering the location and the distance from the point to the bucket, leading to higher accuracy and lower false alarm rate. In addition, we seek the optimal LSH functions with the PSO algorithm, which enhances the stability of the proposed method.

1.2. Paper contribution and organization

We summarize the contributions of this paper as follows:

- We propose a novel anomaly detection algorithm based on Locality Sensitive Hashing Filters (LSHF), where the abnormal events are filtered out by the nearest hash buckets.
- We present an online updating mechanism in LSHF to handle the scene variation, which is simple but effective in video streams.
- We develop an evaluation function for LSH functions and employ the Particle Swarm Optimization (PSO) algorithm to search for the optimal hash functions, which helps improve the detection accuracy.

The remainder of this paper is organized as follows. In Section 2, we briefly introduce the related algorithms of Locality Sensitive Hashing (LSH) and bloom filter. Section 3 provides detailed demonstration of the proposed LSHF model for anomaly detection, followed by the PSO algorithm searching for optimal hash functions presented in Section 4. The experimental results on three public datasets illustrating the superiority of our approach are shown in Section 5. Finally we conclude our work in Section 6.

2. Background

2.1. Locality Sensitive Hashing (LSH)

As an important technique for fast approximate similarity search, hashing has gained much popularity in recent years. For instance, the Minimal Loss Hashing (MLH) [25], Kernel-based Supervised Hashing (KSH) [26], Supervised Discrete Hashing (SDH) [27], and Bit-Scalable Deep Hashing (BSDH) [28], etc. Among various hashing methods, Locality Sensitive Hashing (LSH) is widely used for approximate nearest neighbor searching in large high-dimensional databases [29]. The key idea of LSH is to hash the data into a low-dimensional binary (Hamming) space, and similar data points are mapped into the same bucket with a high probability while dissimilar data points are hashed into the same bucket with a low probability. To implement LSH on dataset S with distance measure D, we introduce the LSH family [30] defined as:

Definition 2.1. A family $\mathcal{H}=\{h:S\to U\}$ is called (r_1,r_2,p_1,p_2)-sensitive for D if for any $\boldsymbol{x}_1,\boldsymbol{x}_2\in S$

- if $D(\boldsymbol{x}_1,\boldsymbol{x}_2)\le r_1$, then $\Pr_{\mathcal{H}}[h(\boldsymbol{x}_1)=h(\boldsymbol{x}_2)]\ge p_1$,
- if $D(\boldsymbol{x}_1,\boldsymbol{x}_2)\ge r_2$, then $\Pr_{\mathcal{H}}[h(\boldsymbol{x}_1)=h(\boldsymbol{x}_2)]\le p_2$,

where U is the dataset distributed in the Hamming space. In order to make the LSH family practical, we have probabilities $p_1>p_2$ and distances $r_1<r_2$.

Given a family $\mathcal{H}$ of hash functions characterized by Definition 2.1, the gap between the high probability p_1 and low probability p_2 is amplified by concatenating several functions. Specifically, a function family $\mathcal{G}$ is defined as $\mathcal{G}=\{g:S\to U^K\}$, where $g(\boldsymbol{x})=(h_1(\boldsymbol{x}),h_2(\boldsymbol{x}),\dots,h_K(\boldsymbol{x}))$ is the concatenation of K LSH functions and $h_i\in\mathcal{H}$. To ensure accuracy for nearest neighbor searching, a set of hash concatenations $T=\{g_1,g_2,\dots,g_L\}$ are usually built by selecting L independent functions from $\mathcal{G}$.

LSH family proposed in [31] is defined for the case where the distances are measured according to the ℓ_p norm, for any $p\in[0,2]$.