

Automatic Classification of Behavior Patterns for High-Precision Detection of Suspicious Individuals in Video Images

LIU Jianquan, NISHIMURA Shoji

Abstract

Today surveillance cameras are becoming ubiquitous in public facilities such as shopping malls, office buildings, airports, and train stations. Until now, these cameras have typically only been used post-incident to support criminal investigations. However, the threat posed by criminal actions such as terrorist attacks is growing, which can cause serious damage or loss of life. Such an event is focusing attention on taking advantage of these tools to prevent incidents from occurring in the first place. This paper introduces new technology based on NEC's "Profiling Across Spatio-Temporal Data" technology that can classify an individual and assess their threat potential. By performing high-speed extraction of frequently appearing individuals and analyzing the results, this technology can classify the behavior patterns exhibited by these individuals — such as loitering, passing through, and standing still. The hope is that this technology will help prevent crimes by identifying suspicious individuals and alerting security personnel before an incident can occur.

Keywords



image search, image analysis, crime prevention, behavior analysis, behavior pattern, artificial intelligence (AI)

1. Introduction

Surveillance cameras are a fact of life in the modern world. They can be found everywhere from shopping malls and office buildings to airports and train stations. Until now, these cameras have typically been used after the fact; that is, to support criminal investigations by helping locate suspects or providing video of criminal incidents for subsequent analysis. Today, society is under threat from crimes with the potential to inflict enormous damage and loss of life such as terrorist attacks. Consequently, the focus of surveillance is shifting from post-crime to pre-crime. With appropriate analysis, suspicious individuals can be detected before they commit a crime.

The sheer volume of image data collected by surveillance cameras makes this a task that is difficult, if not impossible, for humans to perform. Video footage recorded with multiple cameras can be hours and hours. By watching such a long video, it is very difficult for humans to identify individuals who display suspicious behavior— for example, appearing in the same place again and again or emerging in multiple locations.

To solve this problem, NEC has developed a system

based on its NeoFace facial recognition technology. This system does the hard work of sifting through massive amounts of video images. It finds a specific individual by identifying their face with high precision¹⁾ and matching it with registered facial images. While this search technology is ideal for searching individuals already registered in the watch list, identifying people exhibiting suspicious behaviors who are not registered in the database requires a different approach. For this purpose, NEC developed its "Profiling Across Spatio-Temporal Data" technology²⁾³⁾. This technology makes possible high-speed extraction of frequently appearing persons. Those are who may be making a preliminary survey of the planned scene of crime again or who are loitering in areas where passersby are vulnerable.

However, detection of frequently appearing individuals is not enough on its own to determine suspicious behavior. To automatically identify suspicious individuals, the extracted data must be analyzed to determine how that person is behaving. Behavior that may be considered suspicious includes loitering, repeatedly passing through, or standing still. Further analysis is then required to determine whether that behavior can be con-

sidered suspicious. Proper classification assures a more reliable assessment of risk and helps prevent crime.

2. Quantification and Automatic Classification of Behavior Patterns

So how exactly is it possible to differentiate individual behavioral patterns from a massive volume of video data? NEC's answer was to focus on quantification of behavior patterns to capture the microscopic randomness in people's traffic lines.

Let's look at the differences between a person who is loitering in a camera's field of view, a person who is repeatedly recorded going back and forth, and a person who is simply standing still because he or she is waiting for someone, for example. Although these persons may appear at roughly the same frequency, the fluctuations of their movements are quite different. NEC has developed a method to quantify their behavior and distinguish their differences by capturing the microscopic randomness in their traffic lines (degree of fluctuation of movement). This is an effective tool for isolating suspicious behavior regardless of the overt actions exhibited by the individual⁽⁴⁾⁵⁾.

Moreover, by automatically classifying the behavioral patterns using this quantification method, it is possible to zoom in on people who are behaving differently from others in a large crowd and designate them as an individual who needs special attention (or a suspicious person if the definition of that term is clear).

2.1 Some issues that need to be resolved

If the system has learned these behaviors based on conventional methods, it will be able to distinguish known behaviors and differentiate the behavior of suspicious from non-suspicious individuals.

Let's assume, for example, you have collected a large amount of video of people loitering. Loitering is typically a potential indicator of suspicious behavior. You can use deep learning to teach the system the behavioral characteristics associated with loitering. Then you can create a classifier beforehand that is capable of automatically determining if someone is loitering. To actualize this capability, all you have to do is feed the system video data regarding the behavior of various individuals.

The drawback of this technique is that it cannot operate effectively if there is not enough training data to enable the system to properly comprehend a suspicious behavior or if such data is unknown in the first place. Moreover, it takes time to create the training data and for the system to learn it. The resulting gaps in the system's knowledge base mean that certain behaviors may pass unnoticed.

2.2 Entropy-based solution captures randomness

Clearly, providing the system with enough data on a wide enough range of human behaviors is a herculean task. NEC has taken a different approach, developing an analysis technology that doesn't require learning. The basic idea is this: Rather than building up a stored database of suspicious behaviors and learning to identify them, our system will start tracking a person's movements immediately upon re-identifying them. It captures the microscopic randomness in each movement and quantifies those movements by applying a mathematical model called entropy. The procedure for this proposed technology is outlined in **Fig. 1**.

This technology analyzes the movements of the individuals recorded in video in the order shown in Fig. 1. First, the images from the cameras are divided into cells, and the central points of identical individuals that have been extracted from the images are mapped in the

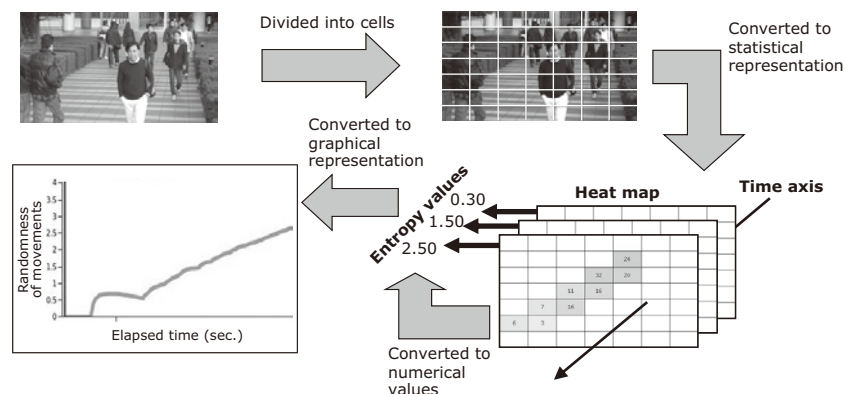


Fig. 1 Outline of the proposed technology.

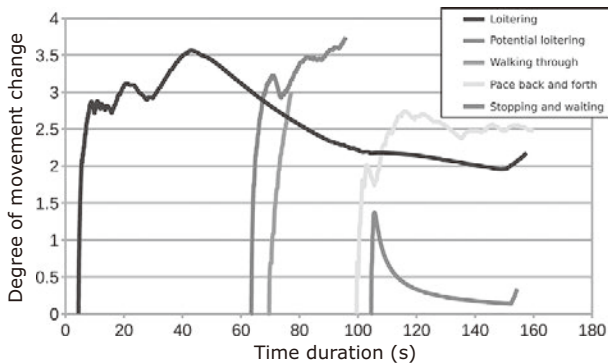


Fig. 2 Change curves that express differences in behavior patterns.

cells. Next, the number of times each individual appears in each cell is aggregated to create heat maps in accordance with the time axis. This makes it possible to follow each individual’s trajectory in a bird’s eye view fashion. Moreover, the values in the cells are summed up along with the time progress to calculate the entropy based on the appearance rate in each cell. The entropy calculation serves as a value to express the randomness of microscopic movements. Finally, this chronological change is used to express the individual’s behavior patterns quantitatively — making it possible to visualize those patterns across time.

This approach to capture is executed from a bird’s eye view, while an individual’s behavioral characteristics are based on their traffic lines. The resultant data can be converted into quantified graphs, making it possible to visualize various behavior patterns. For example, different behavior patterns can be expressed in different graphs as shown in Fig. 2, enabling us to distinguish between various behaviors. These behaviors include repeated pass through, standing still, and loitering. They can be distinguished according to the shapes of the curves in the graphs that express chronological changes in random movements.

As expressed in Fig. 2, you can classify the behavior patterns of frequently appearing individuals. Classification can be fine-tuned to indicate whether an individual is just standing still (if they make small movements) or is lost or loitering (if they make large movements). For example, movements tend to be fast when the slope of the curve is steep and slow when it is gentle. When we look at the behavior of the individual shown with a black line in Fig. 2, the curve rises suddenly and becomes gentle while fluctuating. This expresses a loitering behavior because this individual is moving back and forth over an extensive area after having arrived at the site.

Thanks to this quantification analysis technology, suspicious behavior patterns that are different from others can be extracted. The technology extracts the behavior patterns of all the individuals recorded in a massive amount of video data. It also classifies patterns that show similar changes in graphs into respective groups.

3. Narrowing down Suspicious Individuals

By using this technique to quantify behavior patterns, we have developed a video search system that highlights suspicious individuals with high precision⁵⁾ (Fig. 3).

This system puts weight on the values of conventional appearing frequencies and stay duration, in addition to the randomness of movements. By calculating the scores derived from this data, you can give a higher rank to individuals whose behavior patterns you are looking for according to the purpose of the search. For example, if you want to find a person who is passing through, you should give more weight to their movements (light gray: β). Likewise, if you want to find a person who is standing still, you would give more weight to their stay duration (dark gray: γ); if you want to find a person who is loitering, you would give added weight to both movement and stay duration. In other words, you can narrow down the type of individual you want to target according to their behaviors.

On the other hand, you can also exclude certain behavior patterns from analysis subjects when using this sys-

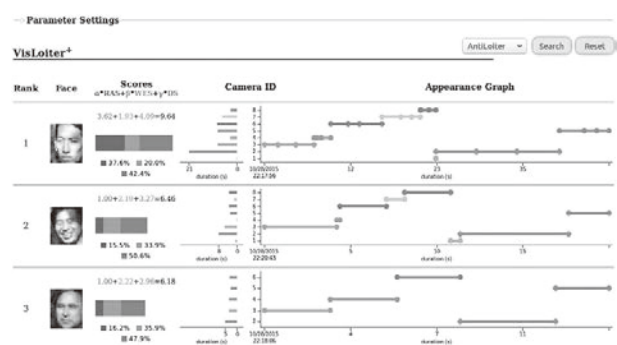


Fig. 3 Search system that highlights suspicious individuals.

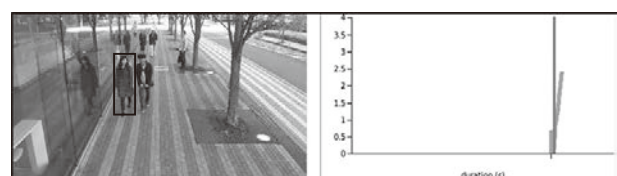


Fig. 4 Passing through behavior pattern (example 1).

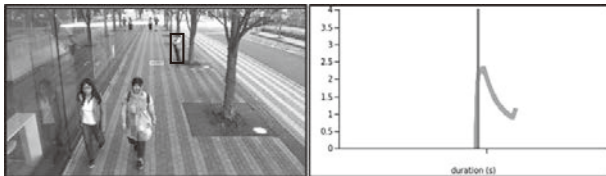


Fig. 5 Standing still behavior pattern (example 2).

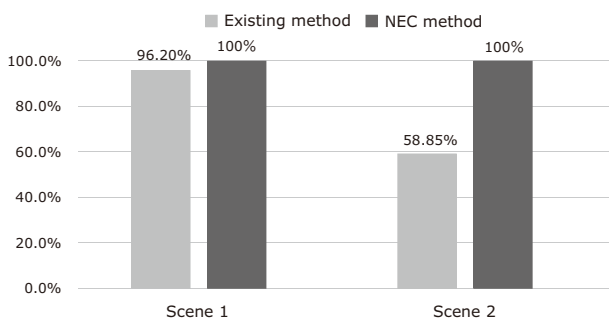


Fig. 6 Loitering detection rates (comparison experiment).

tem to eliminate most people from the search and better identify suspicious individuals. Let's look at two representative examples. In the example shown in **Fig. 4**, the curves of ordinary people rise at a certain rate until they pass through. In the example shown in **Fig. 5**, meanwhile, when people stand still, the curves of their behavior patterns fall.

To validate the effectiveness of this technology, we conducted an evaluation test using publicly available video data⁶⁾ without bias. In this test, our technology was able to correctly classify the behavior patterns such as loitering, standing still for long periods, and passing through. For loitering, we achieved a 100% detection rate. This was a 41% increase over conventional technology that detects people whose stay duration exceeds a time specified in advance (**Fig. 6**).

4. Conclusion

NEC's "Profiling Across Spatio-Temporal Data" technology provides a breakthrough method for identifying suspicious individuals that does not require the system to absorb massive amounts of learning data. Capable of responding in real-time to unknown suspicious behaviors, this system can achieve high-precision identification thanks to the quantification and automatic classification of behavior patterns. It is difficult for conventional systems to visually confirm the individual behaviors of large numbers of people. However, this technology can winnow out suspicious individuals in large crowds by

automatically classifying them using graph curves of their behavior patterns. As a result, prompt action can be taken at an early stage depending on the situation — for example, when a child has gone missing or an elderly person has wandered off. From crime prevention to tourist assistance, this technology has many potential applications in public safety and security.

We are now working to implement this technology as a viable product and plan to make it available by the end of FY 2019.

Reference

- 1) Jianquan Liu, Shoji Nishimura, Takuya Araki: Wally: A Scalable Distributed Automated Video Surveillance System with Rich Search Functionalities, ACM Multimedia 2014, pp.729-730, 2014.11
- 2) Jianquan Liu, Shoji Nishimura, Takuya Araki: Anti-Loiter: A Loitering Discovery System for Longtime Videos across Multiple Surveillance Cameras, ACM Multimedia 2016, pp.675-679, 2016.10
- 3) Jianquan Liu, Shoji Nishimura, Takuya Araki, Yuichi Nakamura: A Loitering Discovery System Using Efficient Similarity Search Based on Similarity Hierarchy, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Volume E100.A, Issue 2, pp.367-375, 2017
- 4) Maguell L. T. L. Sandifort, Jianquan Liu, Shoji Nishimura, Wolfgang Hürst: An Entropy Model for Loiterer Retrieval across Multiple Surveillance Cameras, ACM International Conference on Multimedia Retrieval 2018, pp. 309-317, 2018.6
- 5) Maguell L. T. L. Sandifort, Jianquan Liu, Shoji Nishimura, Wolfgang Hürst: VisLoiter+: An Entropy Model-Based Loiterer Retrieval System with User-Friendly Interfaces, ACM International Conference on Multimedia Retrieval 2018, pp.505-508, 2018.6
- 6) PETS 2007 Benchmark Data.
<http://www.cvg.reading.ac.uk/PETS2007/data.html>

Authors' Profiles

LIU Jianquan

Assistant Manager
Biometrics Research Laboratories

NISHIMURA Shoji

Principal Researcher
Biometrics Research Laboratories

Information about the NEC Technical Journal

Thank you for reading the paper.

If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.13 No.2 Social Value Creation Using Biometrics

Remarks for Special Issue on Social Value Creation Using Biometrics
Committed to Supporting Social Values via Biometrics

Papers for Special Issue

Commitment to Biometrics NEC Is Promoting

Bio-IDiom — NEC's Biometric Authentication Brand
The Future Evolution and Development of Biometrics Studies
Privacy Measures of Biometrics Businesses

Services and Solutions That Leverage Biometrics

The Western Identification Network: Identification as a Service in a Federated Architecture
Use of Face Authentication Systems Associated with the "My Number Card"
Face Recognition Cloud Service "NeoFace Cloud"
NEC Enhanced Video Analytics Provides Advanced Solutions for Video Analytics
New In-Store Biometric Solutions Are Shaping the Future of Retail Services
ID Service Providing Instantaneous Availability of User's Desired Financial Services
Biometrics-Based Approach to Improve Experience from Non-routine Lifestyle Fields
Construction Site Personnel Entrance/Exit Management Service Based on Face Recognition and Location Info
The Importance of Personal Identification in the Fields of Next-Generation Fabrication (Monozukuri)

Core Technologies and Advanced Technologies to Support Biometrics

How Face Recognition Technology and Person Re-identification Technology Can Help Make Our World Safer and More Secure
Advanced Iris Recognition Using Fusion Techniques
Advanced New Technology Uses New Feature Amount to Improve Accuracy of Latent Fingerprint Matching
Safety, Security, and Convenience: The Benefits of Voice Recognition Technology
Ear Acoustic Authentication Technology: Using Sound to Identify the Distinctive Shape of the Ear Canal
Automatic Classification of Behavior Patterns for High-Precision Detection of Suspicious Individuals in Video Images
Facial-Video-Based Drowsiness Estimation Technology for Operation on Low-End IoT Devices

NEC Information

NEWS

2018 C&C Prize Ceremony



Vol.13 No.2
April 2019

Special Issue TOP