



## **Chapter IX**

# **Geographic Surveillance of Crime Frequencies in Small Areas**

Peter A. Rogerson, University at Buffalo, USA

## **Abstract**

---

*In this chapter, I describe a system for monitoring crime frequencies for a set of small areas. The objective is to detect as quickly as possible any increase in any area's crime frequency, relative to a specified expected frequency. The system uses a cumulative sum approach, cumulating differences between the observed and expected frequencies of crime in each area. The approach is illustrated using 1996 burglary data from Buffalo, which is available by census tract. Computer code associated with the geosurveillance program is provided in the appendix.*

## Introduction

---

An important aspect of crime analysis is the daily, weekly and monthly monitoring of crime reports. Quick detection of significant increases in the frequency of crime and/or changes in the geographic pattern of crime can lead to efficient reallocations of enforcement effort. There may also be interest in detecting any *decreases* in crime frequencies that may, for example, result from crackdown efforts. Rogerson and Sun (2001) provide an example of such monitoring in the context of crime analysis.

In this chapter, I describe a simple system for monitoring crime frequencies in a set of small geographic areas. The purpose of the system is to signal to the crime analyst any significant changes in the frequency of crime that may occur in any of the small areas. Crime frequencies will exhibit natural fluctuations over time, and it is important to be able to distinguish significant changes in the underlying rate of crime from these natural fluctuations. The statistical detection of a significant increase in burglaries could imply, for example, that criminals had recently targeted the area; quick reaction to the statistical increase could lead to added patrols and, ultimately, to either arrests or declines in criminal activity.

The geosurveillance system is based upon methods developed in industry for the quick detection of faults in manufacturing processes (see, for example, Montgomery, 1996; Wetherill & Brown, 1991; Ryan, 1989). It makes use of the *cumulative sum* of the excess of observed frequencies over some expected, baseline frequency. If the cumulative sum of these excesses reaches some critical value, an “alarm” is sounded, and the analyst then investigates the nature of the change. In the criminological context, the alarm would imply that the frequency of criminal activity had increased by a statistically significant amount. The increase presumably would be worth investigating – it might ultimately be traced to some known cause (for example, there may have been a long spell of hot, dry weather; weather conditions are known to be correlated with criminal activity). But the cause also might be due to one or more criminals who have begun to operate in the area. Quick detection could conceivably lead to quicker arrests.

Section 2 describes the monitoring system and section 3 provides an illustration using burglary data from Buffalo, New York. The final section contains a discussion of potential extensions of the method, as well as a summary of its limitations. Computer code is included in the appendix.

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: [www.igi-global.com/chapter/geographic-surveillance-crime-frequencies-small/18822](http://www.igi-global.com/chapter/geographic-surveillance-crime-frequencies-small/18822)

## Related Content

---

### Hijacking of Clicks: Attacks and Mitigation Techniques

Hossain Shahriar and Vamshee Krishna Devendran (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (pp. 135-145).

[www.irma-international.org/chapter/hijacking-of-clicks/115753](http://www.irma-international.org/chapter/hijacking-of-clicks/115753)

### Reversible Data Hiding Based on Adaptive Block Selection Strategy

Dan Huang and Fangjun Huang (2020). *International Journal of Digital Crime and Forensics* (pp. 157-168).

[www.irma-international.org/article/reversible-data-hiding-based-on-adaptive-block-selection-strategy/240655](http://www.irma-international.org/article/reversible-data-hiding-based-on-adaptive-block-selection-strategy/240655)

### The Gatekeepers of Cyberspace: Surveillance, Control, and Internet Regulation in Brazil

Elisianne Campos de Melo Soares (2015). *Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance* (pp. 361-378).

[www.irma-international.org/chapter/the-gatekeepers-of-cyberspace/115769](http://www.irma-international.org/chapter/the-gatekeepers-of-cyberspace/115769)

### Cyber Victimization of Women and Cyber Laws in India

Debarati Halder and K. Jaishankar (2012). *Cyber Crime: Concepts, Methodologies, Tools and Applications* (pp. 742-756).

[www.irma-international.org/chapter/cyber-victimization-women-cyber-laws/60978](http://www.irma-international.org/chapter/cyber-victimization-women-cyber-laws/60978)

### Speech Content Authentication Scheme based on High-Capacity Watermark Embedding

Fang Sun, Zhenghui Liu and Chuanda Qi (2017). *International Journal of Digital Crime and Forensics* (pp. 1-14).

[www.irma-international.org/article/speech-content-authentication-scheme-based-on-high-capacity-watermark-embedding/179277](http://www.irma-international.org/article/speech-content-authentication-scheme-based-on-high-capacity-watermark-embedding/179277)