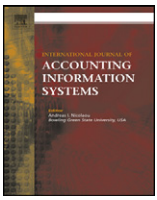
International Journal of Accounting Information Systems 16 (2015) 1–22

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems



Data visualization for fraud detection: Practice implications and a call for future research

William N. Dilla [a,*], Robyn L. Raschke [b]

[a] Department of Accounting Iowa State University, USA
[b] Department of Accounting University of Nevada, Las Vegas, USA

ARTICLE INFO

Article history:
Received 8 June 2012
Received in revised form 7 January 2015
Accepted 11 January 2015
Available online 27 January 2015

Keywords:
Fraud detection
Visual analytics
Interactive data visualization
Decision aids
Cognitive fit theory

ABSTRACT

Analysis of data to detect transaction anomalies is an important fraud detection procedure. Interactive data visualization tools that allow the investigator to change the representation of data from text to graphics and filter out subsets of transactions for further investigation have substantial potential for making the detection of fraudulent transactions more efficient and effective. However, little research to date has directly examined the efficacy of data visualization techniques for fraud detection. In this paper, we develop a theoretical framework to predict when and how investigators might use data visualization techniques to detect fraudulent transactions. We use this framework to develop testable propositions and research questions related to this topic. The paper concludes by discussing how academic research might proceed in investigating the efficacy of interactive data visualization tools for fraud detection.

1. Introduction

Fraud investigators have recently recognized the importance of data visualization for fraud detection, and are starting to implement this technique in practice (Deloitte, 2011; Clopton et al., 2014). Data visualization is especially important in the early stages of fraud investigation, where the investigator is attempting to perform an efficient and effective data analysis and desires to better understand the relationships that may be present in a complex data set. The fraud investigator may employ data visualization as a proactive detection approach, using it to search for data patterns that suggest fraudulent activity (Albrecht et al., 2012). Alternately, the investigator might be evaluating a predication of fraud, using data visualization to develop a fraud theory

* Corresponding author at: 2330 Gerdin Business Building, Iowa State University, Ames, IA 50011-1350, USA. Tel.: +1 515 294 1685.
E-mail address: wdilla@iastate.edu (W.N. Dilla)

http://dx.doi.org/10.1016/j.accinf.2015.01.001
1467-0895/

that is subsequently used to select additional investigative procedures (Wells, 2003). In either case, the investigator is following a hypothesis testing approach, developing preliminary hypotheses about fraud and analyzing relevant data to see if they appear to be true. If the data analysis phase of a fraud investigation does not support the hypothesis that fraud has occurred, then the investigation ends. On the other hand, if data analysis produces results consistent with the hypothesis that fraud has occurred, the investigator will proceed to conduct other investigative procedures, such as examination of documents and interviewing possible witnesses (Wells, 2003).

Since fraudulent actions are deliberate and non-random, traditional audit methods involving the use of statistical sampling are often ineffective for discovering fraud. Hence, fraud examination professionals recommend the use of data mining procedures for detecting fraudulent transactions (Kranacher et al., 2011; Albrecht et al., 2012). In performing data mining procedures, investigators may brainstorm about possible irregularities that could occur in the business processes or transactions they are examining. Alternately, they may have been given a predication that fraud has occurred. Regardless of whether they identify possible fraudulent activity through brainstorming or receive a predication of fraud, investigators then outline ways that the schemes might show up in data patterns. For each indicator thus identified, investigators design a data mining query or procedure intended to identify whether there are individual transactions that need to be examined more closely.

Audit software packages such as ACL and IDEA facilitate data mining for fraudulent transactions within organizations (Lanza, 2004). Additionally, custom-designed software may be used to identify items for further investigation in complex, high-risk transaction environments (e.g., Chang et al., 2008; Pryke, 2010). However, interpreting the output from these tools may require considerable skill, as anomalies in data may not be readily apparent, except to the expert investigator. Graphical analysis may facilitate identifying suspicious patterns of transactions in data (Lanza, 2005a). While spreadsheet programs can facilitate graphical analysis, such analysis can be cumbersome—if the user wants to change the variables being graphed or focus on a subset of the data, it is usually necessary to generate a new graph. Interactive data visualization programs that allow the user to more easily change the data being graphed or its format have now become readily available (e.g., Centrifuge Systems, Inc., 2015; SAP, 2010; Tableau Software, 2010; TIBCO, 2010). Given the potential for interactive data visualization to assist investigators in seeing and understanding data patterns that are consistent with fraudulent activity, forensic accounting practitioners have recently recommended the use of this technology as an investigative tool (Deloitte, 2011; Clopton et al., 2014).

Proponents of data visualization software contend that it facilitates better decisions by supporting visual thinking. For example, data visualization consultant and author Stephen Few states that

> "Visual analysis software allows us to not only represent data graphically, but to also interact with those visual representations to change the nature of the display, filter out what's not relevant, drill into lower levels of detail, and highlight subsets of data across multiple graphs simultaneously. This makes good use of our eyes and assists our brains, resulting in insights that cannot be matched by traditional approaches (Few, 2007)."

Further, the developers of Tableau Software claim that

> "Genuine data visualization supports visual thinking. The human brain can process a picture much faster than a table of numbers. The right presentation, using the best practices of information visualization, makes organizing and understanding information simple. Features, trends and outliers show up the way they never do in rows and columns (Tableau Software, 2010)."

While these statements make a plausible argument for why data visualization software might facilitate detecting fraudulent transactions, research evidence suggests that the efficacy of interactive graphical displays for decision making depends on task and user characteristics (Lurie and Mason, 2007; Baker et al., 2009; Dilla et al., 2010; Yigitbasioglu and Velcu, 2012). To date, little research has examined whether and how data visualization software might allow investigators to see patterns in data that are indicative of fraudulent activity. Conducting research on this topic is important, given that there are substantial training costs associated with adopting data visualization software, and it is important that practitioners know under what circumstances such software might facilitate more efficient and effective detection of fraudulent transactions. Therefore, the