International Symposium on Visual Analytics Science and Technology (2010)
J. Kohlhammer and D. Keim (Editors)

Sensemaking in Visual Analytics: Processes and Challenges

S.J. Attfield, S.K. Hara, and B.L.William Wong

School of Engineering and Information Sciences
Middlesex University United Kingdom

Abstract

Since Visual Analytic systems support human sensemaking it is essential that such systems are designed with characteristics of this process in mind. Drawing on our previous work with lawyers and reports from experienced fraud investigators we describe the nature of the cognitive work to be supported. We describe the cognitive work domain in terms of its data characteristics, and develop a model of the sensemaking as basis for discussing a distinction between 'naturalistic' and 'normative' sensemaking with a particular emphasis on inference types and the potential for bias. We also report results from a questionnaire-based case study designed to elicit memorable incidents from fraud investigators' experiences. Given the legal context the case study exemplifies skills and strategies that are necessary in order to achieve normative and defensible sensemaking under pressure of high-volume datasets.

Categories and Subject Descriptors (according to ACM CCS): H.1.2 [Information Systems] User/Machine Systems—Human factors Human—Human information processing.

1. Introduction

In this paper we briefly discuss the need for Visual Analytics technologists to be familiar with the human sensemaking process: Since VA, by definition, is the science and technology that uses interactive visualisation and other smart technology to support the analytic and reasoning processes. In doing so, we hope to draw attention to likely pitfalls such as human biases, that can lead to errors in data assessment, judgement and the drawing of conclusions. In being aware, we can then take steps to mitigate these pitfalls in the way we design the information handling [WB07] processes as well as the way we perceive and understand the meaning being represented by the interactive visualisations. Although the analytical process of intelligence tradecraft has been described (e.g. [Heu99]) more work is needed to understand whether the way in which information is presented in VA systems helps or hinders the sensemaking process. Drawing on our work with lawyers (e.g. [AB in press] and reports from recently retired fraud investigators, and practitioners (e.g. Hara), we present an early attempt at describing the nature of the cognitive work that VA science and technology needs to support.

In the next section, we briefly describe the characteristics of the data environment that potential users of VA systems (e.g. lawyers, intel. analysts, fraud investigators) typically encounter. We will then discuss characteristics of sensemaking drawing a distinction between naturalistic and normative sensemaking. We then report findings from a case study of the processes and challenges presented in fraud investigations in order to demonstrate aspects of the skills and support tools necessary for defensible, normative sensemaking.

DOI: 10.2312/PE/EuroVAST/EuroVAST10/001-006

2. Data Characteristics of the Sensemaking Environment

In this section, we attempt to characterise the cognitive work domain of typical workers and users of VA systems. This characterisation is in terms of the kinds of data that they have to analyse and make sense of:

- Very large amounts of data, about many different topics—some possibly related, but many un-related, and each topic area may have fragmentary information relating to several threads;
- Supplied by many different sources, residing on possibly un-connected or loosely coupled data sets;
- Many different formats such a numerical, video, photos, un-structured text
- Varying quality, reliability, and ambiguity
- Incomplete and missing data, and data out of sequence
- Entities with unknown and unexpected relationships
- A lack of context (the big picture)

These problems are illustrated in Figure 1.

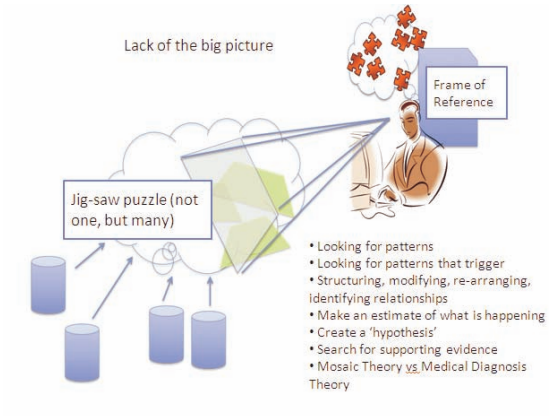

Figure 1. *Typical nature of the cognitive work domain in visual analytics.*

3. Sensemaking

Users often interact with an information system in order to develop some 'picture' or 'model' of a domain [Der93, Spe99]. However, what this means and how it is achieved is not well understood. The process through which people develop interpretations of the world is known as sensemaking [c.f. Wei95, PC05], and interactive visualisations can potentially play a significant role in enabling the sensemaking process. Nevertheless, how this is achieved remains unclear. We explore this question with the motivation that visualisations need to be considered in terms of wider sensemaking processes that they support.

We develop our ideas in terms of a distinction we draw between two complementary kinds of sensemaking. This is made by analogy to a distinction that Klein [Kle99] makes between normative and naturalistic decision making. Klein observed that decision-makers seldom evoke and comparatively evaluate multiple options to a problem (the normative or 'rational' approach). Instead, the situations they encounter evoke singular solutions in a process of 'satisficing' [Sim57]; if the solution criteria are not met then another solution is sought and so on.

Likewise, we distinguish between naturalistic and normative forms of sensemaking. Sensemaking is a very human process in which tacit knowledge and 'gut' instinct play an important role. This is what we refer to as 'naturalistic' sensemaking. However, the potential fallibility of a naturalistic approach and demands for 'due diligence' (to use a legal term) in many domains (e.g. intelligence analysis, legal investigations, medicine etc.) suggest the need to combine naturalistic sensemaking with complimentary normative approaches. We consider what these are and suggest ways in which they might be related to the use of interactive visualisations.

4. A Model of Sensemaking

We represent the sensemaking process in Figure 2 which shows interactions between its significant elements; this representation is based on accounts by Weick [Wei95] and Klein et al [KPR*07]. In the figure, *model* (Klein refers to this as a 'frame') refers to the user's interpretation of some situation. It may be more or less loosely formed or it may not exist at all. The model is triggered and changed through the combination of exposure to new *information* (Klein uses the term 'data') interpreted in the light of *semantic knowledge*. Semantic knowledge is generalised knowledge about how the world works, such as causal knowledge. For example, observing a visualisation showing warmer air rising over colder air can enable a meteorologist to predict snow, but this is only possible given knowledge of that connection.

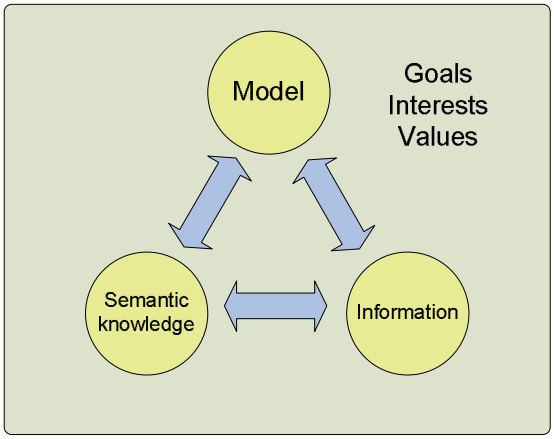

Figure 2. *Interactions between significant elements in the sensemaking process*

Figure 2 also shows the sensemaking process as situated within a context of *goals*, *interest* and *values*. The significance of these is, (a) to determine the kind of model that the user is interested in generating i.e. one that can provides a basis for appropriate action in some domain or activity, (b) that they may bias the kind of conclusion that is reached.

5. Naturalistic Sensemaking

A significant aspect of sensemaking is that it can operate with very little information, with semantic knowledge filling in additional gaps to form an interpretation. One common way in which gaps are filled is through the process of *abduction*. This operates by reversing the direction of a causal connection. Instead of moving from antecedent to a consequent (a->b, a therefore b), the sensemaker perceives one or more consequents and infers an antecedent (a >b, b therefore a). An example is to infer that a knife was a murder weapon from blood found on the blade. *Abductive* reasoning is a process of forming hunches or *reasoning to the best possible explanation.*

Abduction provides a powerful way of moving from a set of seemingly unrelated facts to a possible cause. It is a natural reasoning strategy which also plays an important role in many domains (including intelligence analysis, legal reasoning, medical diagnosis). The significance of abduction lies in its ability to help us draw inferences from limited information; we then fill in the gaps. Significantly, it relies as much upon knowledge as it does upon observation. This suggests that one role for visualisation systems can be to provide indicators from which users can derive useful hypotheses given a set of background knowledge and interests; for example, providing a web designer with a website's 'bounce rate' can lead to inferences about how customers feel about the site.

6. Normative Sensemaking

Whilst abductive reasoning is powerful it is also fallible and its conclusions can be subject to a number of biases. To begin with, the use partial information can easily lead to false interpretations. One way that this can be corrected is by further exposure to incongruent data [KPR*07]. This argues the case for multiple visualisations presenting complementary indicators of a domain. However, confirmation bias can lead people to prefer data that is congruent with an interpretation. Hence, such systems should be embedded within a social practice of hypothesis testing. This complements abductive reasoning (a->b, b therefore a) with deduction used to falsify existential hypotheses (a->c, ¬c therefore ¬a).

Interpretations can be very stubborn, and another challenge faced is assimilation bias in which disconfirming evidence is explained away. Klein [Kle99] observes a number of examples with catastrophic consequences. This and the dependence that abduction has on knowledge, means that two people seeing the same data can form very different interpretations. Attfield and Blandford [AB in press] note work practices during legal investigations used to overcome this kind of problem such as review meetings in which lawyers challenge each others' interpretations with credible alternatives. Here again, biases are mitigated through social processes. However, these also make demands on design, such as allowing multiple data points and trends leading to an interpretation to be recorded and open to scrutiny in some social forum.

7. Case Study: Analytical Challenges in Fraud Investigation

Whilst naturalistic sensemaking reflects powerful human faculties the need for normative approaches to the generation of defensible interpretations gives rise to a need for meticulous enquiry and high technical ability. In this section we illustrate both of these through a case study exploring the experiences of forensic fraud investigators.

7.1 Method

We sent out an open-ended questionnaire via email. The questions were based on the probes used in a Cognitive Task Analysis method called the "Critical Decision Method" [KCM89]. This method seeks to understand why some things are done and how people think through the issues. It is retrospective in nature in that the interviewee is asked to reflect upon a particularly memorable incident they had experienced in the past. This is usually done on a face-to-face basis. The face-to-face approach would enable follow-up questioning when interesting issues arise. As we adapted the method to be administered by a questionnaire, this would be more difficult. The questions were designed to elicit the

respondents' expertise in the analytical and investigative reasoning process. They probed for occasions that were memorable (because of the difficulty of the problem, errors made or novelty of the solution) and asked participants to elaborate:

- the setting (physical and social surroundings, formal and informal tools etc.) ;
- what they did, what an observer of the situation would see, how they used tools;
- what someone less experienced would find difficult and why;
- mistakes or omissions a less experienced person might have made;
- advice they would give to a novice;
- how they would group and characterise the difficulties that they highlighted and the source of the difficulty (e.g. tool design, inherent complexity);

7.2 Results: Retrospections of a Fraud Investigator

In this section, we present the retrospections of an experienced fraud investigator, guided by the CDM inspired questions described above.

In a fraud investigation, large volumes of digital media may be gathered from multiple business sites or residential addresses and other jurisdictions. Fraud investigations require pre-search intelligence to seize material from key players and organisations that are suspected of being involved in the first instance.

Due to the transactional nature of most fraud-based crimes, large amounts of digital media need to be processed and analysed before a suspicion can be substantiated or disproved.

The first task Digital Investigators undertake is to acquire valid forensic images from digital media devices. This can be a time intensive exercise due to increasing hard disk sizes. This prolongs the time it takes to image one computer and verify its image. Once these images are acquired investigators then proceed to investigate the image. The primary task is to sort out relevant evidential data from irrelevant data.

Irrelevant data is data that is not user-generated. This may include the operating system and applications used to generate relevant data. Relevant data is data that is useful to an investigation excluding user-generated irrelevant data. This data may be easily accessible or further processing may be needed to make it accessible. As this digital data may have encryption, be from legacy databases, Internet data or require removal of sensitive material from relevant compressed data all these steps can prolong an investigation.

During my time as an investigator, there were many incidents where accessing and analysing data presented challenges to technical ability and without core investigative skills, key data may have been missed. The examples presented here are used to highlight issues that are faced when dealing with large complex amounts of data.

- Retrieving data from legacy tapes
- Searching graphical files for textual data
- Multiple investigators processing digital items on single case

When retrieving data from legacy tape formats specialist software is required to image and retrieve data. In this instance, it was discovered through the forensic validation process that the amount of data recovered from the image was dependant on which specialist software was used. Some software retrieved more data than others did. Tape recovery was conducted on a high specification machine in a solitary location due the time it took to recover data. When comparing the log files produced by different specialist software it was apparent that one software recovered more data. Upon discovery of this problem, emails, documentation and a copy of the image was sent to the software developers so they could replicate the problem and provide a solution (new software release).

In the meantime, uncertainty led to checking log files for other recovered tapes and other tape formats. A less experienced investigator may have not undertaken this activity as they may not have processed tapes previously. Although the process of tape recovery is automated it is the length of time it takes to recover that becomes the issue. If the process is running on your desktop machine with other resource hungry processes, it can hinder progress on these items.

Had this discrepancy not have been discovered substantial amount of data would have been missed. This would have severe implications on an investigation as others (defence teams) may have recovered information that may have proved innocence or proved guilt, discrediting the forensic investigators technical ability. Due to the complex nature of fraud investigations, it would have meant that meaningful patterns and relationships might have been missed. Even when the flaw in the software had been fixed, investigators are all too aware that data retrieved is only as good as the tool used to recover it.

In the second example we look at how manual investigations skills are applied to a science where investigations can now be done via scripts and automated jobs.

A forensic investigator using standard commercial software can find that they still need to view graphics files for text as users often scan passport photos, invoices, utility bills and bank statements from paper documents. This is because some search engines in

forensic software do not search graphics files for text. This applies to scanned documents, hand-written scanned documents and foreign language documents saved as graphic formats. On a typical image you can find that you may have a few hundred to thousands of graphic files. To get through such a large volume of files requires experience and efficient working practices.

An inexperienced investigator may decide to view each file in turn, to make sure no evidential data is missed. An experienced investigator would run hash functions to remove standard graphics files to reduce the file numbers they have to view. They would organise the file list by location and file size, thus highlighting system areas and directories where there are less likely to be data. By employing these tactics, an investigator can reduce their workload substantially. This however does not mean an investigator is not vigilant to shrewd individuals who disguise data in these areas.

To make this task manageable investigators were allocated four 21 inch screens (2 per PC) that were wall mounted and at eye level. It also meant the application could be split across both screens, one displaying the file list and the other the graphic. Anyone walking behind the investigator could see the screens clearly.

An investigator would sit facing these screens; although other investigators are less than a metre away, you would conduct your work in solitary silence. Your computers represented your colleagues and interaction was via the Internet or email. Human interaction only occurred when there was a technical problem that needed to be resolved. At this time most investigators would share their informal methods of reaching a solution. This was then formalised by adopted current working practices. This was seen as a method of increasing knowledge and saving time spent on an issue. While this particular setup may be seen as anti-social, it was a highly effective working method that yielding high output for experienced investigators.

A new investigator at this stage would proceed to view the graphics as they were displayed whereas an experienced investigator would question why certain graphics failed to render properly. This would lead to further investigation to find more appropriate file viewers to handle file types, checks of the file signature to make sure it was a graphics file or installation of software to view the graphic in its native application. The graphical analysis on a computer image can take substantial time. New investigators are often embarrassed when proceeding with this part of the investigation because of the volume of adult and sensitive material that is often on these. Once this manual part of the investigation has been completed, investigators still trawl through the remainder of the data. This example discusses one image of a computer, in a large fraud case there may be hundreds of digital media items that hold data.

This leads to the final example of how numerous items of high volume of data is amalgamated to discover evidence and new threads. Investigators have various methods that they may use to process items more speedily. In my experience, most investigators process their own cases, only requiring assistance to meet key deadlines. This provides the investigator the freedom to work in their preferred method.

Forensic software allows investigators to search through one item (image) at a time. When teaching new investigators this is the preferred model to introduce them to investigations. More experienced investigators load several images into the forensic software. This decision may be based on all items, from an individual, a single address, business or based on transactional data types. This allows an investigator to construct search strings containing keywords or numerical values to search across these numerous items, speeding up the investigation. It will also highlight relationships and communications between items.

When several investigators are working on a single case there is a tendency to work asynchronously. The digital media may be shared out according to the location from which it was received, who it belongs to, or the technical expertise required to process it. Investigators will then work through this material individually. At times the amount of digital items involved make it impractical to share information that would prevent a repetition of functions. For instance if an investigator decrypts documents and cannot practically share the password, other investigators with the same document will have to decrypt the document on their image.

From my experience of the forensic community most investigators prefer to work as individuals. This assures they are only responsible for items they have processed and can write reports or defend their actions in court. It removes the responsibility for the work of others; this applies even more so to work of offsite colleagues.

Finally when all material from a large scale investigation is processed and the relevant material extracted, the extracted material from all investigators is reviewed for patterns and evidential weight.

8. Summary

Visual Analytics could provide significant benefits to those involved in processing large scale digital forensic investigations. Making sense of data that is often unrelated and fragmented but when pieced together offers investigators further opportunities of investigative avenues more speedily than conventional tools would reduce the time it takes to complete investigations.

If visual analytics could be developed to cater for digital forensic investigators it must include the ability to:

- Read forensic image file formats
- Load multiple data types
- Open and display compressed files
- Show duplicate items of data from different media items
- Visually display patterns of communicative data between users (such as email traffic)
- Include advanced professional recognition of data types
- Allow multiple users to load data into a central repository
- Allow access to data locally and remotely in a multi-user environments
- Include the functionality to remove irrelevant data from display environment
- Allow integration of bespoke / standard software packages
- Ensure forensic integrity of data

Forensic investigators already use multiple large screens to assist them to visually view data, documents and execute queries. This move towards large visual displays has allowed investigators to process, analyse, assess data more easily. Visual analytics would provide all these benefits with the addition of technology that would analyse data patterns more concisely, joining the dots more swiftly and allowing the analysis of data to be completed far more efficiently. We believe that these requirements provide a basis for supporting analysts in transitioning from initial naturalistic sensemaking to normative forms of sensemaking which place greater demands on defensibility.

6. References

[AB in Press] ATTFIELD S. J., BLANDFORD A.: Making sense of digital footprints in team-based legal investigations: The acquisition of focus. *Human Computer Interaction Journal*, Special Issue on Sensemaking (in press).

[Der83] DERVIN B.: An overview of sense-making research: Concepts, methods and results. Paper presented at the Annual Meeting of the Int. Communication Assoc. Dallas, TX (1983).

[Kle99] KLEIN, G. A.: *Sources of Power: How People Make Decisions*. MIT Press, 1999.

[KCM89] KLEIN G. A., CALDERWOOD R., MACGREGOR R.: Critical Decision Method For Eliciting Knowledge, *IEEE Transactions on Systems, Man and Cybernetics, 19*, (1989) pp. 462-472.

[KPR*03] KLEIN G.A., PHILLIPS J.K., RALL E.L., PELUSO, D.A.: A Data-frame Theory of Sensemaking. In: *Expertise Out of Context: Proc. of the Sixth International Conf. on Naturalistic Decision Making* (Pensacola Beach, Florida, May 15-17, 2003). Lawrence Erlbaum Assoc. Inc, US, (2007) pp. 113-155, 2007.

[Heu99] HEUER R. J.: *The psychology of intelligence analysis: Center for the Study of Intelligence*, Central Intelligence Agency (1999).

[PC05] PIROLLI P., CARD S.: The Sensemaking Process and Leverage Points for Analyst Technology as Identified Through Cognitive Task Analysis, *Proceedings of the International Conference on Intelligence Analysis* (McLean, VA) (2005), https://analysis.mitre.org/proceedings/.

[Sim57] SIMON H. A.: *Models of Man: Social and Rational*. New York: Wiley, 1957.

[Spe99] SPENCE R. A:, Framework for Navigation. *International Journal of Human Computer Studies*, (1999), vol. 51, pp. 919-945.

[Wei95] WEICK K.: *Sensemaking in Organisations*. Sage, London, England, 1995.

[WB07] WONG B. L. W. and BLANDFORD A.: Extracting Information Handling Strategies. In *Proc. 8th International Conference on Naturalistic Decision Making NDM8 (2007)* , Pacific Grove, CA, June 2007, K. Mosier and U. Fischer, Eds., ed San Francisco, CA: University of San Francisco, 2007, pp. CD-ROM.