The use of self-organising maps for anomalous behaviour detection in a digital investigation

B.K.L. Fei[a], J.H.P. Eloff[a], M.S. Olivier[a] and H.S. Venter[a]

[a]Information and Computer Security Architectures (ICSA) Research Group, Department of Computer Science, **University of Pretoria**, Pretoria 0002, South Africa

Abstract

The dramatic increase in crime relating to the Internet and computers has caused a growing need for digital forensics. Digital forensic tools have been developed to assist investigators in conducting a proper investigation into digital crimes. In general, the bulk of the digital forensic tools available on the market permit investigators to analyse data that has been gathered from a computer system. However, current state-of-the-art digital forensic tools simply cannot handle large volumes of data in an efficient manner. With the advent of the Internet, many employees have been given access to new and more interesting possibilities via their desktop. Consequently, excessive Internet usage for non-job purposes and even blatant misuse of the Internet have become a problem in many organisations. Since storage media are steadily growing in size, the process of analysing multiple computer systems during a digital investigation can easily consume an enormous amount of time. Identifying a single suspicious computer from a set of candidates can therefore reduce human processing time and monetary costs involved in gathering evidence.

The focus of this paper is to demonstrate how, in a digital investigation, digital forensic tools and the self-organising map (SOM) – an unsupervised neural network model – can aid investigators to determine anomalous behaviours (or activities) among employees (or computer systems) in a far more efficient manner. By analysing the different SOMs (one for each computer system), anomalous behaviours are identified and investigators are assisted to conduct the analysis more efficiently. The paper will demonstrate how the easy visualisation of the SOM enhances the ability of the investigators to interpret and explore the data generated by digital forensic tools so as to determine anomalous behaviours.

Article Outline

1. Introduction

Computer forensics has been around for a while. It can be traced back as early as 1984 when the Federal Bureau of Investigation as well as other law enforcement agencies began developing programs to assist in the examination and analysis of computer evidence [1]. However, the rise in Internet and computer-related crime has brought computer forensics increasingly to the fore.

Computer forensics deals with the identification, extraction, preservation and documentation of digital evidence [2]. Digital forensics is perhaps a better term than computer forensics since many devices beyond those traditionally called “computers” are involved in today's digital world. Digital evidence may be sought in a wide range of computer-related crimes. What is unique about digital evidence is the fact that it is fragile by nature and can easily be altered or destroyed.

Digital forensic tools have been developed to assist digital forensic investigators in conducting a proper investigation into digital crimes. Examples of such tools are EnCase [3], Forensic Toolkit [4], ProDiscover [5] and many more. However, current state-of-the-art digital forensic tools are not capable of handling large volumes of data in an efficient manner [6].

Since storage media are steadily growing in size, this poses two problems to digital forensic investigators. Analysis of a single machine is becoming more cumbersome, which also makes the process of analysing or investigating a large number of machines more difficult or even impossible. What is important, however, is the detection of suspicious behaviour and the subsequent finding of related digital evidence. By analysing only the appropriate computer system (the one that displays suspicious behaviour), one can greatly reduce the amount of processing time that would have been required by a human or reduce monetary costs involved in gathering the necessary evidence.

Therefore, employing data mining techniques to aid in digital investigations will offer many potential advantages [7]. Data mining is the synthesis of statistical modelling, database storage and artificial intelligence technologies [8]. It has produced good results in giving insight into large volumes of data. One ultimate goal of data mining is the prediction of human behaviour [8]. As a result it could assist in detecting and deterring offenders.

An earlier study involved the analysis of data generated by digital forensic tools on a single computer system by using a data mining technique known as the self-organising map (SOM) [9]. The current paper will demonstrate how the different SOMs (one for each computer system) can aid digital forensic investigators during a digital investigation to identify anomalous behaviours (or activities) among employees (or computer systems) [16]. It will also introduce the main advantage of the SOM, namely the graphical and visual representation of large data sets.

The remainder of the paper is structured as follows: Section 2 will provide a brief overview of the SOM. Section 3 demonstrates how anomalous behaviours can be detected by using a digital forensic tool and a SOM application when analysing multiple computer systems. Section 4 contains a number of concluding remarks.

2. The self-organising map

The self-organising map (SOM) [10] and [11] is a neural network model for clustering and visualising high-dimensional data. Clustering is the process of locating “interesting” groups from among the data [12]. It is a technique to group data with similar characteristics. The purpose of visualisation is to map data onto a graphical representation to provide a qualitative idea of its properties. The SOM is used to map high-dimensional data onto a low-dimensional space that is usually two-dimensional. It is based on unsupervised competitive learning, meaning that the learning process is entirely data driven.

The architecture of the SOM is shown in Fig. 1. The input layer is fully connected with units (or neurons) at the output layer and each unit in the input layer represents an input signal. The output layer generally forms a two-dimensional grid of units where each unit represents a unit of the final structure.

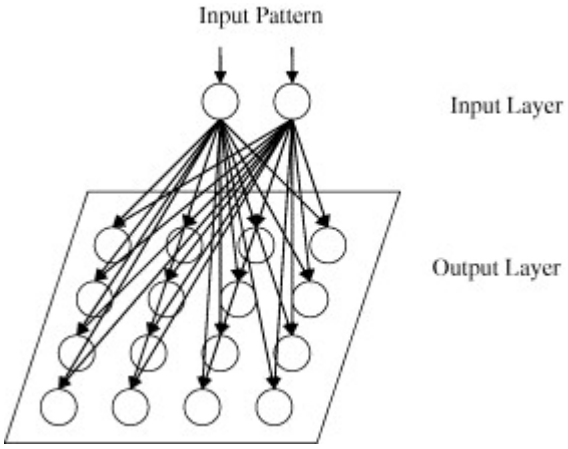

Fig. 1. The architecture of the SOM.

The effect of the learning process is to cluster together similar patterns while preserving the topology of input space. It involves two major steps:

• *Finding the winning unit*. When an input pattern is presented to the input layer, the units in the output layer will compete with one another. The winning unit in the output layer will be the one whose weights are closest to the input pattern in terms of Euclidian distance [13].

• *Updating weights*. Once the winning unit has been determined, the weights of the winning unit and its neighbouring units will be adjusted, i.e. shifted in the direction of the input pattern.

This learning process is repeated until the SOM reaches an accurate result or until a given maximum number of iterations has been reached. After the learning process has been completed, an orderly map is formed in such a way that the topology of the original data is preserved. With this map, component maps [14] can be generated to aid in inspecting possible correlations between dimensions in the input data [15]. Each component map visualises the spread of values of a particular component (or dimension). As a result, possible correlations are revealed by comparing different component maps with one another [9].

3. Detecting anomalous behaviours

Many employees who have access to a computer have, with the advent of the Internet, been given the opportunity to explore new and interesting possibilities on the World Wide Web. However, as stated earlier, excessive Internet usage for non-work purposes and deliberate misuse of the Internet, such as employees who access Web sites that

promote pornography and other unethical (or illegal) activities, have become a serious problem in many organisations.

During a digital investigation, an analysis of the temporary Internet files can be very useful when evidence of excessive or inappropriate Internet access is to be gathered. Temporary Internet files are those files that are “image captures” of the sites that the user visits when accessing the Internet [2]. They reveal a substantial amount of evidence about a user's browsing history, and analysing them can be useful in proving a pattern of logon and duration times.

This section will demonstrate how anomalous browsing behaviours can be detected in a more efficient manner when analysing multiple computer systems. This will be done by using a commonly deployed digital forensic tool such as Forensic Toolkit, together with a SOM application. The SOM application employs an unsupervised neural network based on the concept of the SOM.

A feature that several digital forensic tools offer is the ability to display all the files that are found in a spreadsheet-style format. This allows digital forensic investigators to view at a glance all the files on a particular storage medium, as well as the information regarding each file. This information includes the name of the file, the date it was created, the logical size of the file and other information about it.

The remainder of Section 3 is structured as follows. Section 3.1 explains the way the demonstration was setup; Section 3.2 briefly discusses the analysis process, and a detailed discussion of the results of the analysis process follows in Section 3.3.

3.1. The setup of the demonstration

The demonstration was setup as follows:

• Four computer users or systems were selected from an organisation. All were operating on the Windows platform and were used by individuals who have been given a similar work task.

• Forensic Toolkit was used to create images of the four independent hard drives found in each computer system. Note that an image is an exact copy of all the data on a media device (e.g. hard drive, compact disk, flash disk, etc.).

• Once the image was created, it would be analysed to extract the evidence that one would wish to present. Forensic Toolkit was used to create a text file containing information about all the files found in the temporary Internet files folder.

• The four text files (one for each computer system) were subsequently processed by the SOM application independently.

• Once the learning process of the SOM has been completed, maps were generated. The time taken to produce these maps was approximately 10–20 min. These maps could be used as an important visualisation aid as they yielded a complete visual picture of the data. The two-dimensional maps were displayed in the form of hexagonal grids where each hexagonal grid could be referred to as a unit.

3.2. The analysis process

The Internet behaviour of each computer user was observed by analysing the different component maps. The component maps revealed the value variation of components (or dimensions) across the map. Since visualisation techniques were applied, small values would be indicated by the colour blue, red would indicate large values and other colours (such as green or yellow) would represent intermediate values. As mentioned earlier, a comparison of component maps with one another could reveal possible correlations.

For each computer system, three component maps were presented (see below). The first component map represented the file type (e.g. documents or graphical images). Blue would indicate that the majority were documents, while red would indicate that the majority were graphical images. The second component map represented the time when the temporary Internet files were created (i.e. the time of day when Internet activities occurred). Here, blue would indicate the early hours of the morning (just after midnight). As the time of day progressed, the colour would change from blue to green, and eventually to red. The third component map represented the day of the week on which the temporary Internet files were created. The colour blue would indicate that the majority of the files were created at the beginning of the week (i.e. Monday or Tuesday), while green would indicate that the majority of the files were created in the middle of the week and red would reveal that the majority of the files were created later in the week (i.e. Friday, Saturday or Sunday).

Note that the objective was to study the behaviour of each computer user. It would therefore be appropriate to analyse the second and third maps in greater detail, because only the time and day of the week were of interest in determining the behaviour of the different computer users.

3.3. Results of the analysis process

3.3.1. First computer user

In Fig. 2b, three major portions are encircled in black. The blue portion (located at the bottom right) of the map denotes the period between 12 a.m. and 6 a.m., the green portion (located at the middle) points to the period between 6 a.m. and 7 p.m., and the red portion (located at the top left) represents the period from 7 p.m. to 12 a.m. (This information is displayed when selecting the units in the map).

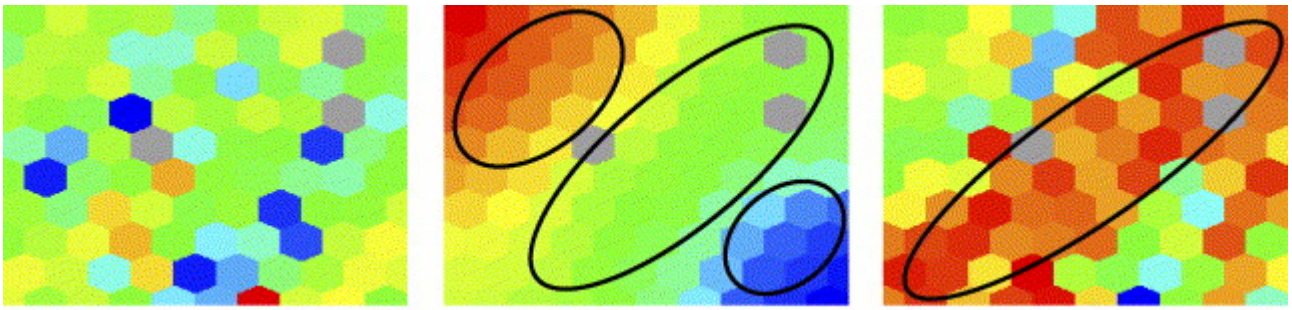

Fig. 2. First computer user: (a) the component map of file type, (b) the component map of time created, and (c) the component map of day of the week (for interpretation of the references to colour in this figure legend, the reader is referred to the web version of the article).

In Fig. 2c, a significant portion is encircled. It indicates that the majority of the Internet activities occurred on Fridays, Saturdays and Sundays (shown in red). By analysing (or comparing) Fig. 2b and c, one can see that the green portion in Fig. 2b correlates with the red portion in Fig. 2c. This means that during weekends, the majority of Internet activities took place in daytime, between 6 a.m. and 7 p.m., while during the weekdays most Internet activities took place at night, between 12 a.m. and 6 a.m. and again from 7 p.m. to 12 a.m.

3.3.2. Second computer user

In Fig. 3b, three major portions in the map are encircled in black. The blue portion (located at the top right) of the map represents the period from 7 a.m. to 12 p.m., the green (located at the middle) portion refers to the period between 12 p.m. and 4 p.m., and the red (located at the bottom left) portion denotes the period from 4 p.m. to 8 p.m. Through the use of colours, one can immediately see that the green portion is significantly larger than the rest—thus implying that Internet usage is heaviest in the afternoons, from 12 p.m. to 4 p.m.

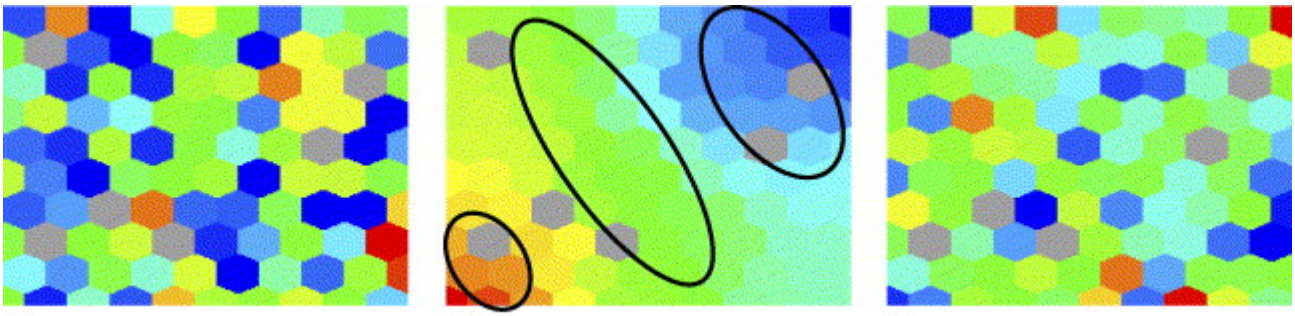

Fig. 3. Second computer user: (a) the component map of file type, (b) the component map of time created, and (c) the component map of day of the week (for interpretation of the references to colour in this figure legend, the reader is referred to the web version of the article).

Fig. 3c shows that the Internet activities of the second user seem to be spread evenly across the different weekdays, except that not many Internet activities occurred on Fridays. This is clearly shown on the map as only a few red units can be found.

3.3.3. Third computer user

Fig. 4b shows that three major portions in the map are encircled in black. The blue portion (located at the bottom right) of the map represents the period from 8 a.m. to 12 p.m., the green portion (located at the middle) stands for the period from 12 p.m. to 3 p.m. and the red portion (located at the top left) represents the period between 3 p.m. and 6 p.m.

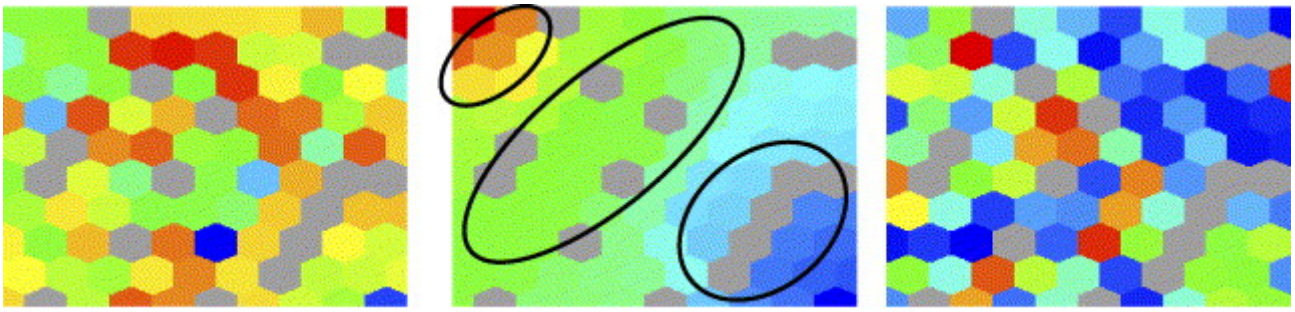

Fig. 4. Third computer user: (a) the component map of file type, (b) the component map of time created, and (c) the component map of day of the week (for interpretation of the references to colour in this figure legend, the reader is referred to the web version of the article).

In Fig. 4c, more than half of the map is covered in blue (or shades of blue). This means that over 50% of the Internet activities took place on Mondays and Tuesdays. Later on in the week all use of the Internet seemed to dwindle.

3.3.4. Fourth computer user

In Fig. 5b, three major portions in the map are highlighted by being encircled. The blue portion (located at the bottom right) of the map represents the period from 7 a.m. to 12 p.m., the green portion (located at the middle) denotes the period from 12 p.m. to

4 p.m. and the red portion (located at the top left) indicates the period between 4 p.m. and 9 p.m.

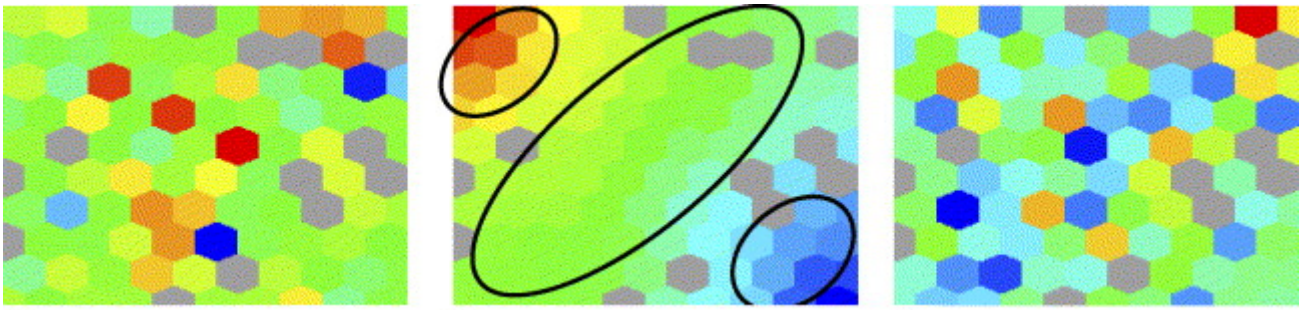

Fig. 5. Fourth computer user: (a) the component map of file type, (b) the component map of time created, and (c) the component map of day of the week (for interpretation of the references to colour in this figure legend, the reader is referred to the web version of the article).

According to Fig. 5c, the Internet activities of the fourth user seem to be distributed evenly across the different days of the week.

3.4. Discussion

After analysing the four independent computer systems with the SOM application, the behaviour of each computer user was noted. As mentioned previously, the four computer systems were used by individuals who had a similar work task. Therefore, it would be expected that the four computer systems would display similar behaviours. Based on the above observations, it is clear that anomalous behaviour was found in the first computer system. This is because the behaviour of the user of the first computer system deviates significantly from that of the users of the other three computer systems, who share similar behaviours.

Dealing with temporary Internet files can be an issue at times since not all the files of every Web site visited will be cached. However, given that an anomalous behaviour has been discovered, further investigation is now needed to determine the reasons for such an anomaly. The individual using the first computer system could well be using the Internet for inappropriate or illegal activities. The reasons for these anomalies are, however, beyond the scope of this investigation. Nevertheless, this paper will make a highly significant contribution to large-scale forensic analysis and will greatly simplify digital forensic investigators' task during the analysis phase of an investigation.

4. Conclusion

Data mining has been employed to analyse large volumes of data, as are often encountered in a typical digital investigation. As the task of examining multiple computer systems can be tedious and time consuming, an analysis of only the appropriate computer system – the one that is suspicious – can greatly reduce human processing time and reduce the monetary costs involved in gathering evidence. Once the suspicious computer system has been identified, digital forensic investigators can quickly proceed to the next step in their search.

This paper has shown that SOMs are quite efficient at aiding digital forensic investigators who are conducting a digital investigation to determine anomalous behaviours among the Internet browsing behaviour of individuals within an organisation. An application that employs an unsupervised neural network based on the concept of the SOM was demonstrated. It has shown that the easy visualisation of the maps can give immediate insight into large volumes of data. In addition, it offers a new perspective from which investigators may view the data, allowing investigators to detect anomalous behaviour in a far more efficient manner.

Future work will be on the analysis of Web proxy logs using the SOM. The purpose of a Web proxy is to relay a request in the form of a uniform resource locator from a client to a server, receive the response of a server and send it back to the client. What is significant about analysis of data on a Web proxy than on a single computer system or on multiple computer systems is that computer users can delete traces of their request to the Internet from their computer system while with a Web proxy, it maintains all requests made by each computer user. This will pose several benefits when conducting a digital investigation.

References

[1] M. Noblett, M. Pollitt and L. Presley, Recovering and examining computer forensic evidence, *Forensic Sci. Commun.* **2** (2002) (4).

[2] A. Marcella and R. Greenfield, Cyber Forensics: A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes, Auerbach (2002).

[3] Guidance Software Inc., 2004. http://www.guidancesoftware.com.

[4] Access Data Corp., 2004. http://www.accessdata.com.

[5] Technology Pathways, LLC, 2004. http://www.techpathways.com.

[6] V. Roussev and G. Richard III, Breaking the performance wall: the case for distributed digital forensics, *Proceedings of the Digital Forensic Research Workshop* (2004).

[7] N. Beebe, J. Clark, Dealing with terabyte data sets in digital investigations, Advances in Digital Forensics, Springer (2005) 3–16.

[8] J. Mena, Investigative Data Mining for Security and Criminal Detection, Heinemann, Butterworth (2003).

[9] B. Fei, J. Eloff, H. Venter and M. Olivier, Exploring forensic data with self-organising maps, *Advances in Digital Forensics, Springer* (2005), pp. 113–123.

[10] T. Kohonen, The self-organising map, *Proc. IEEE* **78** (1990) (9), pp. 1464–1480.

[11] T. Kohonen, Self-organising Maps, Springer-Verlag (2001).

[12] J. Vesanto, Using SOM in data mining, Licentiate Thesis, Helsinki University of Technology, 2000.

[13] A. Engelbrecht, Computational Intelligence: An Introduction, Wiley (2002).

[14] J. Vesanto, Data exploration process based on the self-organising map, Doctoral Thesis, Acta Polytechnica Scandinavica, Mathematics and Computing Series 15, Helsinki University of Technology, 2002.

[15] J. Vesanto, SOM-based data visualisation methods, *Intell. Data Anal.* **3** (1999) (2), pp. 111–126.

[16] B.K.L. Fei, J.H.P. Eloff, M.S. Olivier, H.M. Tillwick, H.S. Venter, Using self-organising maps for anomalous behaviour detection in a computer forensic investigation, in: Proceedings of the Fifth Annual Information Security South Africa Conference.

Corresponding author. Tel.: +27 12 420 2504; fax: +27 12 362 5188.