Improving Knowledge Availability of Forensic Intelligence through Forensic Pattern Warehouse (FPW)

Vivek Tiwari
Maulana Azad National Institute of Technology, India

R. S. Thakur
Maulana Azad National Institute of Technology, India

INTRODUCTION

The forensic examination and analysis of the forensic digital data is a pivot point of any investigation. Nowadays, most of the research concentrating only examination of digital data in particular case wise. It will help only find out and get proof against criminals. Nowadays, forensic data are huge and dynamic. As a result a lot of different and complex patterns are extracted. Thus, more elaborate techniques are required in order to extract the hidden knowledge and make these data valuable to the end-users (Manolis & Panos, 2003). Data mining was developed to help to extract Knowledge from the raw data, using algorithms that could discover several statistic properties in the original data (Romero & Abelló, 2010). In order to someone to be able to exploit these patterns, an efficient and general Forensic Pattern Warehouse Management System (FPWMS) is required for handling (storing/processing/retrieving) patterns. Pattern is interesting because it describes a recurrent behavior (Schneider & Wilke, 2012). In conventional system, forensic digital data are stored in some undedicated system. This system is lacking behind when patterns are required for forecasting, prediction and decision making. At this time, we need to perform analysis (apply some data mining or knowledge retrieval methods). This is very time and resource consuming. The main focus behind this article is design a dedicated system which is able to store forensic digital data patterns permanently. System consist results or knowledge which is already an analysis of forensic data. In other words, we can say that system gives the ability to retrieve 'ready to use' knowledge or patterns. There is introduced forensic pattern warehouse (FPW) concept. There are various data mining techniques which work on forensic digital data to get the patterns. These forensic digital data stored in data warehouse. The downside of data mining techniques is on-demand analysis. This means, at the moments we need knowledge; need to initiate analysis on forensic digital data warehouse and then patterns get lost when system out of memory. This is time consuming and not feasible always. There is no way to store the forensic knowledge (forensic pattern) permanently till date. The proposed introduced concept "pattern warehouse" enables to store forensic patterns permanently. This gives the knowledge on-demand in understandable format. Forensic Pattern Warehouse (FPW) allows to access patterns on-demand. A forensic pattern warehouse (FPW) enhanced forensic intelligence through better forensic data quality, consistency and availability. Government and investigation agencies can obtain various kinds of trend reports e.g. the crime with the most general, rare in a particular area/country for the given period of time etc. The concept of pattern warehouse itself very new and little emphasis has been given to it till date. This article will discuss issues, challenges and pyramid architecture for developing forensic pattern warehouse for betterment of forensic prediction and forecasting.

Many government and private forensic databases can help to both law enforcement investigators and the scientists who support their work in the lab. Forensic Pattern Warehouse (FPW) is a centralized forensic data repository that integrates forensic data from various transactional, legacy, applications and external sources. The Forensic Pattern warehouse provides an environment that is separate from the operational sys-

DOI: 10.4018/978-1-4666-5888-2.ch126

tems and is completely designed for decision-support, analytical-reporting, ad-hoc queries, and data mining. This isolation and optimization enables queries to be performed without any impact on the daily transactional and operational systems (Tiwari & Thakur, 2014). Figure 1 depicted various data sources of forensic pattern warehouse. Benefits with a successful implementation of a forensic pattern warehouse include:

- Enhanced forensic intelligence
- Increased processing of large and complex queries
- Forensic intelligence from multiple sources
- Instant access to forensic pattern (Save Time)
- Enhanced forensic pattern quality and consistency
- Provide historical forensic pattern intelligence
- Convert forensic data into actionable form
- Increase scope of forensic data availability
- Generates a high ROI (return on investment)
- Provide wide variety of forensic patterns
- Provide various kinds of trends report
- Decrease computational cost and increase productivity

Decision making on forensic data is very crucial. Decisions that affect the strategy and operations of organizations will be based upon credible facts and will be backed up with evidence and actual data (Geradts & Bijhold, 2002; Tiwari, 2010). Insights will be gained by using forensic pattern warehouse (FPW) through improved information access. A data warehouse is designed for storing large volumes of data and being able to rapidly query the data but forensic pattern warehouse is designed and constructed with a focus on speed of knowledge retrieval and analysis. Pattern warehouse does not concentrate for creation and modification of forensic data. In contrast, the forensic pattern warehouse is built for analysis and decision making. In conventional ways, forensic data are stored around transactional database and have limited accessibility (Geradts & Bijhold, 2001; Mikkonen & Astikainen, 1994). It is almost impossible to any organization to share their transactional databases. There are large amount of forensic data in country but scattered in organization and institute wise. They hardly exchange their forensic data for analysis purpose (Sibert, 1994). The result of any analysis process is directly depends on amount of quality data. Decision making process lies on credibility of analysis. Analysis on single organization's forensic data cannot bring such credibility. For many organizations, forensic information systems are comprised of multiple subsystems, physically separated and built on different Platforms and formats. Moreover, gathering data from multiple disparate data sources is a common need when conducting forensic data analysis for decision making. We need to gather forensic data from various small or big organizations time to time and need to put in central repository system (Werrett, 1997). We perform integration of existing disparate data

Figure 1. Data sources of forensic pattern warehouse