JOURNAL OF COMPUTING TECHNOLOGIES
ISSN 2278 – 3814

Available online at www.jctjournals.com
Volume 1, Issue 2 , June 2012

Theft Prevention System: An Approach to prevent Theft

Jeelan S [#1], Janardhan babu V [*2], Vijai S [#3]

Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur-518583, A.P, India
[1]jee.fuzi@gmail.com
[3]vijai.sa@gmail.com

Department of CSE, Sri Venkatesa Perumal College of Engineering & Technology, Puttur-518583, A.P, India
[2]cse.svpcet@gmail.com

Abstract— **in this paper we present a novel anti theft control system for small organizations that tries to prevent the theft of computers or computer data physically. The system makes use TCC-M, which senses the object movement during off hours and sends a text message to the owner's mobile stating that the location under observation is into theft. This is followed by the message gateway present in the organization continuously sends messages until the user enters a unique password. The password consists of few characters initialized by the authorized personnel. If the user enters the correct password two times, a text message is sent to the police with the address of the organization and the location tracked using a GPS module. The message is also sent to security personnel too about the unauthorized entry and theft. Further the entrance is closed by a secret lock gets activated and the unauthorized user gets trapped inside the organization and only the owner who is equipped with the key to the secret lock system can deactivate the mechanism. This technique helps in taking fast steps towards an attempt to steal. The design is robust and simple.**

Keywords— **Thin client computing, Computer theft control, Message server, Secret key.**

1. INTRODUCTION

This document is a template. An electronic copy can be downloaded from the conference website. For questions on paper guidelines, please contact the conference publications committee as indicated on the conference website. Information about final paper submission is available from the conference website. The Association of Certified theft Examiners (ACFE) estimates that the typical business will lose an average of six percent of revenues from employee theft. The ACFE Report indicates that small businesses suffer disproportionate losses because of the limited resources they have to devote to detect theft. The report mentions that one of the most serious threats to the success of a small business is employee theft. Misplaced trust, lax hiring and supervision, and a failure to implement basic financial controls can lead to an environment that is ripe for internal theft and theft. Both large and small companies today are now placing a renewed importance on preventing theft to help improve profitability as they face a competitive economic environment and rising costs. Large companies face a high rate of embezzlement of money that siphons off large amount of revenue, whereas small businesses face sizeable amount of inventory shrinkage.

Theft Prevention:

The value of internal control is apparent in both preventing and detecting theft as prevention is better than cure. A weak internal control creates opportunities for theft and about half of all thefts occur in the financial area (Vanasco, 1998). Internal control system has four broad objectives; those are to safeguard assets of the firm; to ensure the accuracy and reliability of accounting records and information; to promote efficiency in the firm's operation; and to measure compliance with management's prescribed policies and procedures (Haugen and Selin, 1999). The effectiveness of internal control depends largely on management integrity. Technical interventions are controls implemented to limit access to building, rooms or computer systems. Formal interventions involve horizontal expansion of the hierarchy of organization to have a flatter pyramid. Education, training and awareness programmers are some measures implemented in the informal interventions. Theft prevention procedures should have three realistic and measurable goals:

- Determine theft through proactive policies; and
- Increase the likelihood of early theft detection.

Objectives of the research

The objectives of the research are:

a) To identify a range of issues relating to shrinkage revenue and to summarize these issues into two categories, namely: detection of theft and prevent.
b) To determine types of employee theft as this shrinks revenue and wastes business efforts.
c) To profile theft offenders and examine the characteristics of the employees who commit theft, error and abuse.
d) To assess the impacts of theft in organization and to detail and assess the detection and prevention controls.
e) To build up a decision making framework for choosing the best available and proper solution.

Scope of the Study

Theft is a significant subject that probably became a big cancer for firms. There are numerous types of thefts that are prevalent to various functions in an organization. The scope of research focuses on employee theft that involves breaches of physical assets or tangible property. The research includes analysis of the modes of theft in organization and, the characteristics of perpetrators and attempt to cover the development and evaluation of strategies to prevent or detect theft.

Research Problem

Steal and theft of employees affect practically every organization across many dimensions. There are many types of theft involving different levels of management. This posed many major problems in research. There are too many known and unknown theft in business which make difficult to classify and to identify proper solutions to avoid it. There is no decision making framework for assisting managers to choose between available solutions to prevent totally this crime. There is no single straightforward test for theft investigation to show in every case that a theft had been committed; and although we can detect it, we cannot avoid theft totally as it can be committed in many ways. It is difficult to estimate in financial terms the loss to business caused by theft as most of the time thefts are unreported or under reported.

The solution

Thin client computing is a model in which an entire windowing system is executed on a server, and users interact with their applications across network from lightweight clients. The server decouples the user interface from an application's logic and sends display updates to the client, and the client renders display updates and sends input events to the server Because of its lower total cost of ownership, this model has gained wide acceptance. Data compression is particularly effective in this domain because display updates are typically highly redundant synthetic images. A synthetic image has far fewer colors than pixels, is often composed of sharply delineated solid regions with overlaid text, Sequences of display updates often contain even more redundancy for example, moving a window or scrolling its contents typically produces display updates with whole blocks occurring verbatim on the client's display. The user has just moved in the area under observation, causing the server's and client's displays to be out-of-sync. Thus, the server must send a display update coding the difference between its display and the client’s display and sends SMS to the owner.

System Architecture

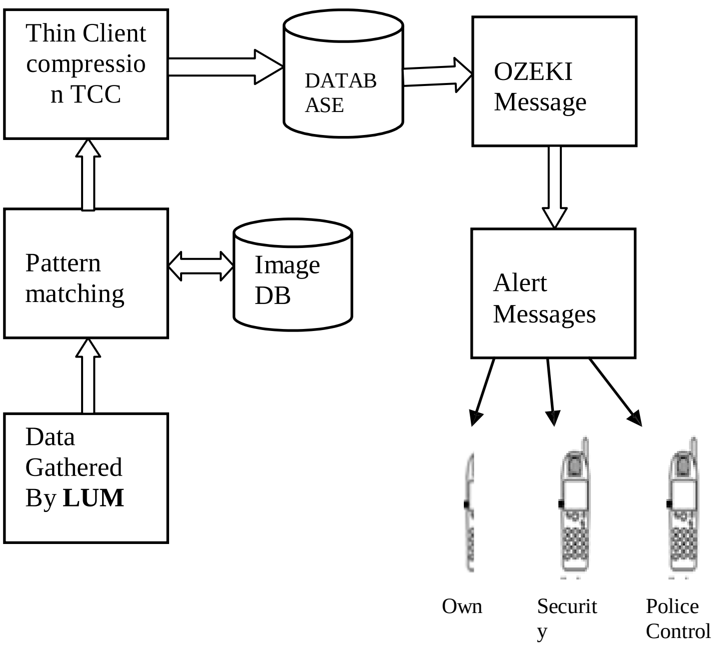

Fig. 1 Block diagram representing the system architecture.

Working Principle

Location under Monitoring.

Continuously detects the area under monitoring for any change in the captured video. If any change occurs in the screen with respect to pixels, this module will take an current change in the video and takes a snap of image.

Pattern Matching.

This module is responsible of cross checking the images in the image Database and identifies whether the change occurs due to any recognized staff, Strangers or by other than human movements like curtains or screens or even some animals like rats etc. With the residue obtained from screen changes this module will provide input to the TCC module.

TCC- Thin Client Compression.

Once the screen change residue is obtained, the TCC module compresses the image and transfers it to the server (Database server) to report that in a particular time some change occurred on the area under monitoring. Based on this report the server will updates the system regarding the change and initiates Message server module.

Message Server.

Based on the information received by the Database server (Thin Client – Server), Ozeki message server will be initiated and an alert message will sent for three different mobile numbers i.e. for owner of organization, Internal Security Officer and to the local Police Control room.

Implementation

Algorithm:

TCC-M consists of four big steps

(a) Identify features.

(b) Compute displacement vectors for those features that appear uniquely in the reference screen.

(c) For each predominant displacement vector, attempt to grow a matching block around the center of its supporting features.

(d) Compress the residue with TCC.

First, we sample each display update and the reference display only at those locations that occur in the uniform-color context. Second, for each feature, we limit ourselves to exactly one candidate displacement Vector by mapping features in the display update to only those features on the client's display that occur uniquely and, thus, are more likely to have moved. Third, we successively estimate the center of predominant motion and its displacement vector at the feature level and use these parameters to simply verify motion at the pixel level.

The ability of our algorithm to detect block motion depends on relatively unique features being uniformly distributed across the reference screen. While this is not guaranteed, we found experimentally that it is typically the case. We first evaluate the compression efficiency and over head of TCC-M by comparing it to TCC for large updates in the Netscape benchmark. Depending on the complexity of the web page being scrolled and the area of newly uncovered regions, TCC-M typically compresses individual updates between 50 to 950 times more efficiently than TCC.

The algorithm is fast enough for immediate updates because it reduces the search space of an exhaustive search in three ways. First, we sample each display update and the reference display only at those locations that occur in the uniform-color context, effectively limiting the number of source and destination locations. Second, for each feature, we limit ourselves to exactly one candidate displacement vector by mapping features in the display update to only those features in LUM display that occurs uniquely and thus, are more likely to have moved. Third, we successively estimate the centre of predominant motion and its displacement vector at the feature level and use these parameters to simply verify motion at the pixel level.

We presents Thin Client Compression (TCC) an efficient method for compressing sequences of synthetic images that outperforms state-of-the-art PWC by a factor of 2.6 and GIF by 8.2 for a sequence of screen dumps. It extends pattern matching and substitution to non-bi-level images.TCC does not have a copy command because detecting block motion on the client's display was assumed to be too slow for interactive video updates. We present an algorithm for detecting block motion in real-time and integrate it in to TCC. We call this new method TCC with block motion (TCC-M). A real-time algorithm for detecting blocks in images that occur verbatim in a reference image. In the presence of motion, TCC-M typically runs faster and compresses 50 to 950 times better than TCC. In the absence of motion, our algorithm increases TCC's runtime by only 19%. We also evaluated the interactive performance of TCC and TCC-M by simulating thin client systems based on these methods. Our analysis is complicated by the fact that two bandwidth adaptive systems generally do not compress the same sequence of display updates. We address this problem by developing a novel measurement methodology for interactive performance.

Most state-of-the-art methods for compressing synthetic images are based on sophisticated image models. These models decompose each pixel into a sequence of candidate values and ask whether the pixel equals the next candidate value until an affirmative answer has been coded. Entropy coding is typically based context modeling and arithmetic coding. The piece wise constant image model (PWC), Runs of Adaptive Pixel Patterns (RAPP) and Tem-plate Adaptive Pixel Patterns (TAPP) use fixed context quantizes to reduce model Parameters. None of these methods copies whole blocks of pixels. One of the first methods to use a copy command is Flexible Automatic Block Decomposition (FABD) which describes an image in terms of itself by decomposing it into copied and solid blocks. FABD is too slow because it maintains a data structure with an entry for each pixel maximizes a copied block for each pixel and must test a large number of candidate displacement vectors to achieve competitive compression. Baeza-Yates and Regnier describe an algorithm that is easily extended to multiple patterns. It uses one dimensional multiple string matching to search for the pattern's m rows in every n/m-th row of the text.

Fig.2 The theft scenario captured with the system.

Fast Motion Detection Algorithms for TCC

Our goal is to develop an algorithm that can quickly detect blocks in a display update that occur verbatim on the client's display and, thus, can be coded efficiently by a copy command. Ideally, the total latency introduced by updating the client's display across a network should be in the order of magnitude of the threshold of perception i.e., about 100ms. Given that any form of exhaustive search, even when applying FABD's optimizations, is too slow, it is obvious that a fast algorithm must severely reduce the search space without compromising the ability to detect motion. This is quite a challenge.

We used the algorithm based on the intuition that we can use easily detectable unique features to track any form of motion. For example, let us assume that at the client side there is a change in location under monitoring (LUM) screen contained a single yellow pixel due to change in the object position that pixel moved up, and we could easily detect the new location and compute the displacement vector of that yellow pixel in the update. Given the new location of the yellow pixel we can easily verify whether its surrounding pixels also have moved by the same displacement vector.

Ozeki Message Server 6

Ozeki Message Server 6 - SMS Server uses a GSM mobile phone attached to the PC with a phone-to-PC data cable or IP SMS technology to transmit and receive the messages. Ozeki Message Server works on Microsoft Windows XP, 2000, 2003 operating systems.

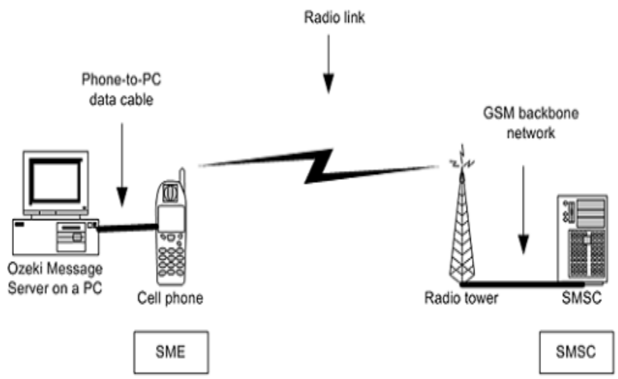

Fig. 3 Ozeki Message Server used with a mobile phone attached to the PC

we have integrated SMS messaging functionality into our application. The message will be sent, whenever an object movement takes place in LUM, a script is executed to place an entry into a database table. The Ozeki Message Server monitors this table and delivers the message. The Message Server puts all received SMS in an incoming database table.

Experimental Setup and Results

The performance of the system is tested with webcam, connected to the client P-IV Intel dual core system with windows-XP connected with GSM modem, java media framework installed in both client and server systems. TCC-M using thin client simulator, tcsim, and traces of two location sessions were recorded at the device dependent (DDX) layer.

We quantify the effect of a copy command on compression efficiency and coding speed, and study responsiveness and quality of three thin client systems based on standard TCC and an ideal version of TCC-M. The latter determines copy commands from side-information available at the DDX layer (i.e., the parameters of two successive object movements window and CopyArea) and serves as a baseline method. We recorded the LUM under different lighting conditions and tested with personnel moved at different accelerated speeds. We first evaluated the compression efficiency and overhead of TCC-M by comparing it to TCC for large updates in the database for faster object movements. For updates without blocks that have moved, TCC-M, by design, compresses as efficiently as TCC. For those updates that moves objects very fast, TCC-M dramatically outperforms . Depending on the complexity of the object movements and the area of newly uncovered regions, TCC-M typically compresses individual updates between 50 to 950 times more efficiently than TCC. On a side note, we also found that TCC-M sometimes detects motion that is not revealed by DDX function calls.

2. CONCLUSIONS

Employees surveyed in this study offer advice to prevent theft of computer & computer data internal employee or external theft that is strongly prevented with the above novel approach using TCC-M and SMS gateway for better controls and improved record keeping. From this knowledge, managers can be reassured that continued progresses with the current trends in employee theft prevention are needed and should continue to be implemented in small businesses. Further research is needed to gauge the accuracy of these findings. A broader sample is needed that explores the true depth of the employee perceptions regarding the views uncovered here, especially in light of heightened global security, rising crime rates, terrorism, and fire accidents. Variables to be potentially controlled organizational location with this additional internal surveillance and better internal control systems at companies.

As a Future Enhancement we are planning to configure an MMS server instead of this Ozeki message server to send the actual live motion picture to be sent to the registered mobile numbers, so that it could provide real time live information about the theft as MMS.

REFERENCES

[1] A. M. Tekalp. Digital Video Processing. Signal Processing Series. Prentice Hall,1995.

[2] B. O. Christiansen, K. E. Schauser, and M. Munke. A Novel Codec for Thin Client Computing. In Proceedings of the IEEE Data Compression Conference, Snowbird, UT, Mar. 2000.

[3] S. Angebranndt, R. Drewry, P. Karlton, and T. Newman. Denition of the Porting Layer for the X v11 Sample Server, Apr. 1994.

[4] S. Forchhammer and O. R. Jensen. Content Layer Progressive Coding of Digital Maps. In Proceedings of the IEEE Data Compression Conference, Snowbird, UT, Mar.2006.

[5] S.Forchhammer, X. Wu, and J.D. Andersen. Lossless Image Data Sequence Compression Using Optimal Context Quantization. In Proceedings of the IEEE Data Compression Conference, Snowbird, UT, Mar. 2001.

[6] S. J. Yang, J. Nieh, and N. Novik. Measuring Thin-Client Performance Using Slow-Motion Benchmarking. In proceedings of the 2001 USENIX Annual Technical Conference, Boston, MA, June 2001.

[7] Y. Endo, Z. Wang, B. Chen, and M. Seltzer. Using Latency to Evaluate Interactive System Performance. In Proceedings of the 1996 USENIX Symposium on Operating System Design and Implementation, 1996.