# Mobile Computer System with User Friendly Environment and Security Protection

Chu-Hsing Lin[1*], Jung-Chun Liu[2], Wen-Chen Wu[3], Tsau-Wei You[4], Ming-Hung Liu[5]

[1]chlin@thu.edu.tw,[2] jcliu@thu.edu.tw,[3] pootel@gmail.com,
[4]s22216532@hotmail.com,[5] g98350038@thu.edu.tw
Department of Computer Science, Tunghai University,Taichung 407, Taiwan

*Abstract* — **In this paper, motion detection with the webcam can determine current conditions around mobile computers, which act accordingly with a variety of response methods. A good balance is achieved between sensitivity of machines and experiences of users. Many practical applications are investigated, and this paper is primarily focused on two main points: user-friendly operations and security. Our system provides dynamic detection features for suspicious objects: photos of suspected thieves are taken, saved, and uploaded to the Internet, and when necessary, warning Short Message Service messages are sent to mobile phone users. Apart from this application, many other applications are feasible, for example, connection of alternative current power cords of laptops can be used to determine whether they are at a risk of being stolen.**

**Keywords:** Motion Detection, Webcam, dynamic detection.

## 1. Introduction

As laptops are expected to surpass desktops in worldwide pc shipment in 2011, the security of laptops and their ease of use are the two most important attributes for laptop users.

As information security has become an important issue, people often notice software and network security, but ignore the risk that physical machines may be stolen [1] [2]. In addition to physical security, since laptops are used in various locations instead of a fixed place, an automatic identification feature is implemented to detect the environment and dynamically adjust the system configuration to provide useful and interesting applications [3] [4].

## 2. Methods and Features for Implementation

Most image processing programs involve use of Open Source Computer Vision Library (OpenCV) [5]~[8]. Since laptops are used in a variety of environments for different applications, in addition to the use of the OpenCV engine, algorithms used to analyze movement of users are also very important, such as motion detection,

power detection, and sound detection algorithms [9] [10].

*2.1 OpenCV*

OpenCV takes advantages of Intel ® Integrated Performance Primitives (IPP) library and provides a transparent interface for it, which means that OpenCV will automatically load processor-specific optimized IPP libraries at the run-time.

Pictures taken with the web camera using functions provided in OpenCV are dynamically analyzed to determine whether there are suspicious people around the laptop or whether the user is away from it. Pictures captured by OpenCV may result in a so-called motion blur, which is usually alleviated by using high speed cameras to capture images. In our implementation, web cameras in commercial laptops are used to take pictures, and suitable amount of pictures are taken continuously to enhance picture quality.

*2.2 Instant Messaging software*

Our system will automatically change status of the Instance Messaging (IM) software when the laptop is idle when the user is on the phone, chats with other people, or is away; and the IM software will return to its original status when the user resumes working on the laptop.

*2.3 Audio Streaming*

Our system will automatically stop replaying the music or decrease the volume of music when it detects that the user is leaving or is on the phone; and it will resume replaying or increase the volume when the user is back to use the laptop [11].

*2.4 FTP*

When the user has left and the system detects suspicious people are around the laptop, it will automatically capture pictures of the suspects and directly upload pictures of them to an FTP server to save clues and evidence of events.

*2.5 SMSGO message*

If the laptop has being stolen, the system will immediately send Short Message Service (SMS) messages in Http format provided by SMSGO to a phone number specified by the user to notify him.

*2.6 Theft alarming*

Motion detection method and power cord monitoring are used to determine any exceptional use or theft of the laptop. In addition to uploading pictures via FTP and sending SMS messages, when laptop theft events occur the system will also immediately start the BIOS speaker, which has a high pitched sound and is not easy to turn off.

## 3. System Architecture and Scenarios

We use dynamic detection methods to determine current states of the user [12]. For example: if the computer detects that a user leaves for some time, it will turns off the screen automatically to save power. Fig. 1 shows flow charts of the scenarios of applications considered in the system implementation.

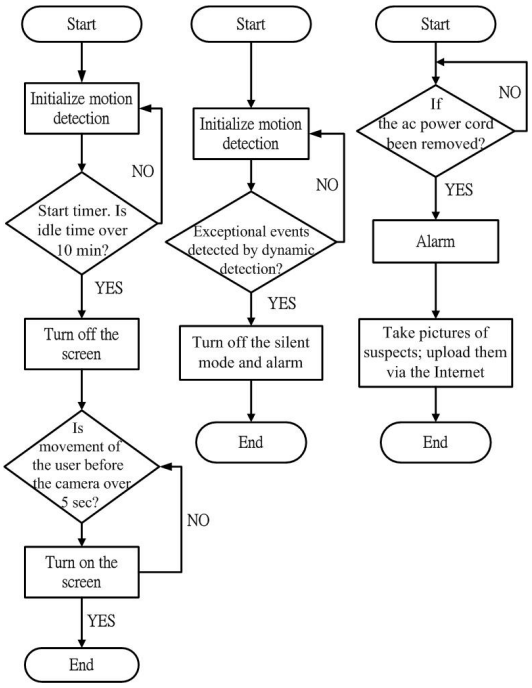


**Fig.1 Flow charts of scenarios of applications**

When the laptop is used in the library, the system will set the computer is in a quiet state (less than 20dB), and it will automatically turn off the speaker. If the user temporarily leaves, the motion detection system detects that user has left his seats and automatically closes and locks the computer screen to save power and avoid others to overlook the computer screen. When the user returns to his seat, the system detects that the user is back. It will automatically turn on the screen, and ask the user to enter passwords to determine whether he is the real user.

If the laptop is used in the user's study room or working place, for the convenience of the user the system automatically turns on the screen when it detects that the user is entering the room. If the phone rings, and the user leaves the laptop to answer the phone call, it will automatically set the computer speaker in a mute mode to avoid interfere the user with loud music. When the user leaves the room, the system automatically saves and closes current working files, and set IM status in leaving status. Then the anti-theft detection [13] program is automatically triggered, and if the alternative current power cord is removed, the alarm will sound and captured pictures of thieves will be uploaded by FTP.

## 4. Results of Motion Detection Algorithms

We implement the motion detection algorithm by comparing consecutive frames of pictures and identifying their difference in pixels. If the difference is greater than a threshold value, the alarm is triggered. Frames of the image are converted to grayscale images first. To identify areas of difference, marked in red as shown in Fig. 2, the Difference and Threshold filters in a computer vision and artificial intelligence library, AForge.Net, are used. However, since technical limitations of current Charge-Coupled Device (CCD) image sensors have noises even for static pictures, misjudgment of motion occurs due to noises on the screen [14]. To solve this problem, the Erosion filter is also used.

**Fig.2 Area of difference is marked in red, where misjudgment of motion occurs due to noises**

If a person moves at a very slow rate, each frame of pictures will show very little change in pixel values, which may be less than the threshold

value to trigger an alarm, so that thieves can exploit this vulnerability and break the system. To solve this problem, we use the following algorithm: in addition to use the current frame to compare with the previous one, the frame of a series of actions before is also used.

By comparing picture frames, the background model is built, which is used for the system to tell foreground objects from background objects. The picture frame captured at the beginning of program execution is converted to a grayscale frame and defined as the background frame. This algorithm is very effective and it can perfectly identify moving objects, as shown in Fig.3.

To optimize performance, the Pixelate filter is also used. To the human eyes, the picture quality after Pixelate filtering is not very good. This drawback does not matter, because the program itself can still accurately determine the moving object.

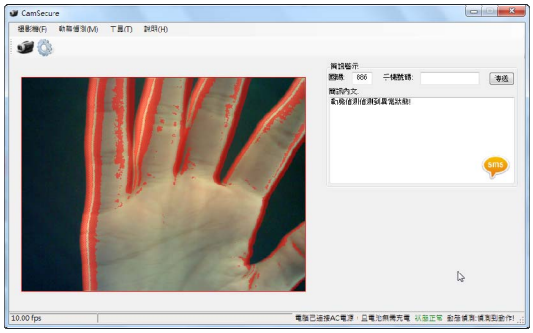

**Fig. 3 Captured picture if the object moves slowly**

## 5. Conclusion

In the past, emphasis is on data protection, including hardware and software encryption, and data transmission security, but physical protection is neglected. In this paper, a software system is implemented to perform laptop theft protection.

The web camera and other standard Laptop components are used to implement a theft protection system to increase the risk, difficulty, and time for stealing, and upload pictures of evidence of events to catch the thief and improve the probability of recovering the laptop.

The I/O devices of the laptop are also used to detect changes in the external environment. According to the detected working conditions of the laptop environment, our system can automatically switch to work in an appropriate mode to establish a friendly environment for users.

## References


[1] 2005 FBI Computer Crime Survey http://www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf

[2]http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Cost of a Lost Laptop White Paper Final 3.pdf

[3] D.E. Marple-Horvat, S.L. Gilbey, and M.A. Hollands, “A method for automatic identification of saccades from eye movement recordings,” Journal of Neuroscience Methods, Volume 67, Issue 2, August 1996, Pages 191-195

[4] M. Fatih Erden , Haldun M. Ozaktas , Aysegul Sahin , and David Mendlovic, “Design of dynamically adjustable anamorphic fractional Transformer Fourier,” Optics Communications, Volume 136, Issues 1-2, 1 March 1997, Pages 52-60

[5] Bradski, G., “Learning-based computer vision with Intel’s open source computer vision library,” Intel Technology Journal 9(2): 119, 2005

[6] OpenCV 2 Computer Vision Application Programming Cookbook, Robert Laganière

[7] Learning OpenCV: Computer Vision with the OpenCV Library, Gary Bradski , Adrian Kaehler

[8] Gary, B. “The OpenCV library,” Dr. Dobb's Journal 25(11): 120.OpenCV, 2000

[9] Wang, L., W. Hu, et al., “Recent developments in human motion analysis.” Pattern Recognition 36(3): 585-601.

[10] Samjin Choi, and Zhongwei Jiang, “Comparison of envelope extraction algorithms for cardiac sound signal segmentation,” Expert Systems with Applications, Volume 34, Issue 2, February 2008, Pages 1056-1069

[11] Chung-Ming Huang, Tz-Heng Hsu, and Yi-Wei Lin, “REDUP: a packet loss recovery scheme for real-time audio streaming over wireless IP networks,” Journal of Systems and Software, Volume 79, Issue 1, January 2006, Pages 29-42

[12] Wes Masri, and Andy Podgurski, “Application-based anomaly intrusion detection with dynamic information flow analysis,” Computers & Security, Volume 27, Issues 5-6, October 2008, Pages 176-187

[13] Soma Shekara Sreenadh Reddy Depuru, Lingfeng Wang, and Vijay Devabhaktuni, “Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft.” Energy Policy, Volume 39, Issue 2, February 2011, Pages 1007-1015

[14] J.U. Schott, M.M. Meier, K. Strauch, “A detector telescope with charge coupled devices for particle dosimetry in space .” Radiation Measurements, Volume 28, Issues 1-6, 1997, Pages 211-216