Chapter 16
Security System for Smart Homes to Prevent Theft

Anitha Mary
Karunya University, India

P. Kingston Stanley
Karunya Institute of Technology and Sciences, India

V. Evelyn Brindha
Karunya Institute of Technology and Sciences, India

J. Jency Joseph
Krishna College of Technology, India

ABSTRACT

The chapter intends to create a system that alerts the victim of theft in real time. The current system does not distinguish between people and objects; instead, it uses a methodology to identify the burglar after the theft has taken place. The internet of things and advancements in wireless sensor networks make it possible to create a smart, safe home that can detect burglars in real time and notify the homeowner while the theft is occurring. The suggested approach is better than the current ones that use CCTV cameras for surveillance.

1. INTRODUCTION

Security is a significant concern for both homes and offices, especially in light of recent theft activities. There is a clear need for a security system capable of detecting intruders in real-time during theft incidents. The current approach relies on CCTVs and DTRs, but these systems cannot distinguish between humans and objects. Additionally, they can only analyze stored images after an incident has occurred, requiring human intervention. In contrast, the proposed system not only detects intruders live but also promptly alerts homeowners or office occupants via a GSM module, notifying them of the theft immediately. This

DOI: 10.4018/979-8-3693-5767-5.ch016

solution is both cost-effective and efficient, offering a reliable security measure for properties without the need for surveillance cameras.

2. RELATED WORKS

The absence of smart devices and sophisticated facial recognition software at home is contributing to an increase in theft tracking (Ahmed et.al. 2010). The inaccuracy of face detection techniques acquired by CCTV cameras arises from theft victims hiding their faces, either completely or partially, using materials made of leather or cloth. Numerous researchers have directed their efforts towards improving face recognition technology (Jian et.al.2018). For example, Zhiwei et al. (Zhang et.al.2012) introduced a regularization technique aimed at enhancing face identification across different spectrums. Additionally, many researchers have focused on refining face and eye detection using the Haar classifier algorithm. Xin et al. (Xin et.al 2018) proposed a system for person face recognition, claiming it offers superior security compared to unimodal biometric systems. Nguyen et al. Nguyen et.al. 2018 suggested employing deep learning techniques, while Cho et al. Cho et.al 2018 advocated for the use of convolutional neural networks to improve image features in face recognition systems, particularly those equipped with visible light camera sensors. Binary pattern techniques were used in the creation of the face detection system by Alobaidi et al.2018. Zhang et al.'s approach to face detection in a stable environment combines model-driven and data-driven methods. Using support vector machines, Omid et al. created a face recognition system that works in the presence of cosmetics like contact lenses and facial makeup (Sharifi et.al.2018). Door and window security is a major consideration when it comes to house security. These days, digital doors that don't require a physical key are employed because to advancements in IoT technology. Nevertheless, it is simple to damage digital doors, and the owners are only aware of theft once they get home. Huth et al. devised a wirelessly connected security system employing a physical key generation method, demonstrating its application in smart homes (Andreasa et.al.2019). To enhance energy efficiency, WiFi modules, temperature sensors, and door sensors are commonly employed.

Intruder detection systems often utilize laser and LDR sensors to detect movement, with alerts sent to homeowners via SMS (Cristian et.al.2016). However, this method may fail to transmit messages through a GSM module in areas lacking internet coverage. Anitha et al. proposed an artificial intelligence-based home system (Anitha 2016).

Patel et al. introduced a modern door lock system for homes, incorporating a Raspberry Pi system-on-chip (SoC), a camera, and an infrared sensor (Jay Patel et.al.2019). This system operates by granting access to individuals whose images are stored in the cloud. Nivo Suranth et al. implemented a home security system utilizing a PIR sensor, an Arduino microcontroller, and a Raspberry Pi 3 SoC (Nicosurantha 2018). The Raspberry Pi processes images captured by a webcam connected to the SoC, along with sensor data from the Arduino microcontroller. Additionally, intruders can be identified using a support vector algorithm, capable of detecting intruders within 2 seconds.

Beyond home security, several researchers have developed anti-theft systems for vehicles. Kiruthiga et al. devised a system employing a global system and a PIC microcontroller (Kiruthigara et.al 2015). This controller identifies unauthorized access and notifies the owner via SMS. Although GPS technology is utilized for vehicle tracking (win et.al.2011), it may encounter limitations at the receiver end, resulting in inaccurate location data due to limited sky view. Radio frequency identification (RFID) is another method used for theft tracking, allowing access to the card, which poses a risk of theft.