REVIEW PAPER

EMBEDDED SYSTEM-BASED ENHANCED SMART SECURITY SYSTEMS FOR INTELLIGENT MONITORING APPLICATIONS : A REVIEW

By

P. LOKESH

Department of Electronics and Communication Engineering, Vemu Institute of Technology, Pakala, Andhra Pradesh, India.

Date Received: 22/11/2023 *Date Revised: 11/12/2023* *Date Accepted: 22/12/2023*

ABSTRACT

The advanced smart security system uses palm vein technology and machine learning to enhance authentication. It combines biometric data with behavioral analysis, continuously adapting to improve security. AI integration allows for anomaly detection, distinguishing normal user interactions from suspicious activities. The user-friendly interface makes it accessible for various applications, ensuring resilient protection against evolving threats. The palm vein technology not only enhances security but also minimizes the risk of false positives and negatives, ensuring a reliable and efficient authentication process. In practical scenarios, the proposed system's versatility extends to securing confidential information in various sectors such as finance, research institutions, and government facilities. Its adaptability and compatibility with existing infrastructure make it a seamless and effective solution for organizations seeking to bolster their security measures. Moreover, the system's integration with mobile devices enables users to receive real-time notifications, allowing for prompt action in the event of a security breach. This feature contributes to the overall responsiveness and effectiveness of the security system, especially in remote locations where immediate intervention may be crucial. In conclusion, the advanced smart security system with palm vein technology not only introduces a novel approach to authentication but also addresses the limitations of existing models. The incorporation of machine learning, behavioral analysis, and real-time notifications significantly enhances its overall security features, making it a cost-effective and reliable solution for a wide array of applications.

Keywords: Security, Recognition, Phone Message, Authentication, Palm Vein Technology, Smart Security System, Intelligent Monitoring, Security Enhancement.

INTRODUCTION

In the rapidly evolving landscape of modern security challenges, the need for intelligent and proactive monitoring systems has become paramount. An Embedded System-Based Enhanced Smart Security System emerges as a cutting-edge solution, integrating advanced technologies to address the complexities of contemporary security requirements. This innovative system is designed to provide heightened surveillance and monitoring capabilities, catering to a diverse range of applications where intelligent security measures are indispensable. Embedded systems, at the core of this advanced security paradigm, offer a compact and efficient platform that seamlessly integrates hardware and software components. These systems are specifically tailored to perform dedicated functions with precision, making them ideal for applications demanding real-time responsiveness and resource optimization. Leveraging the power of embedded systems, the Enhanced Smart Security System stands out as a robust and adaptive solution for intelligent monitoring applications.

The key strength of this security system lies in its ability to employ a multitude of sensors and actuators to gather

and process data from the environment in real time (Prasad & Suneel, 2015). Through the integration of state-of-the-art technologies such as Artificial Intelligence (AI), Machine Learning (ML), and computer vision, the system transforms raw data into actionable insights. This intelligent processing capability enables the system to differentiate between routine activities and potential security threats, facilitating a proactive and preventive approach to security monitoring. Moreover, the Enhanced Smart Security System goes beyond traditional surveillance methods by incorporating connectivity features that enable remote monitoring and control. Utilizing the Internet of Things (IoT) protocols, the system can be accessed and managed through networked devices, providing flexibility and accessibility to security personnel. This interconnectedness not only enhances the system's overall efficiency but also facilitates timely response to emerging security situations.

This paper delves into the intricacies of the Embedded System-Based Enhanced Smart Security System, exploring its components, functionalities, and the manifold applications it can cater to. By delving into the technical aspects and practical implementations of this innovative security solution, we aim to shed light on its transformative potential in the realm of intelligent monitoring applications. The convergence of embedded systems, artificial intelligence, and connectivity defines a new era in security solutions, and the Enhanced Smart Security System stands at the forefront of this technological advancement, poised to redefine the standards of intelligent surveillance and monitoring.

1. Literature Review

Zhai and Cheng (2011) introduces a smart home system which could supervise household appliances remotely and realize real-time monitoring of home security status through mobile phone. The paper also describes the realization of system hardware and software in detail. This System combined embedded technique with GSM. Design adopted the Liod platform for master control system with core processor PXA270 Xscale and singlechip expansion module to realize the information collection, analysis and processing. GSM module is communicated to transmit all the information gathered by this system. Design also realized the video data acquisition, which can be transmitted via wireless or cable network to monitoring center to remotely understand the house condition. On the whole, through this system we can remotely and real-time monitor house status.

Taiwo et al. (2022) presents an intelligent home automation system for controlling home appliances, monitoring environmental factors, and detecting movement in the home and its surroundings. A deep learning model is proposed for motion recognition and classification based on the detected movement patterns. Using a deep learning model, an algorithm is developed to enhance the smart home automation system for intruder detection and forestall the occurrence of false alarms. A human detected by the surveillance camera is classified as an intruder or home occupant based on his walking pattern. The proposed method's prototype was implemented using an ESP32 camera for surveillance, a PIR motion sensor, an ESP8266 development board, a 5V four-channel relay module, and a DHT11 temperature and humidity sensor. The environmental conditions measured were evaluated using a mathematical model for the response time to effectively show the accuracy of the DHT sensor for weather monitoring and future prediction. An experimental analysis of human motion patterns was performed using the CNN model to evaluate the classification for the detection of humans. The CNN classification model gave an accuracy of 99.8%.

Indumathi et al. (2020) explain the smart security system built on the Internet of things. The system is a lightweight, low cost, extensible, flexible wireless IoT-based-smart security system which will permit the mobile devices and computers to remotely trail the happenings at the location, record the activities and save them in the prefixed cloud storage account. The system uses the hardware (things) to sense and fetch the data which is processed by the embedded software. On the occurrence of an abnormal activity (like breaching by an intruder), a valid signal is detected, and it sends signal to the board directing it to run the alert module. The alert

module activates the GSM API to immediately alert the end-user by mobile. This system thus provides a wireless, incessant service to all the stakeholders by phone regarding the breaches occurring in the environment. This implemented smart security system using IoT with mobile assistance also integrates the various alarms, sends alert as pre-programmed, tracks the movements automatically, uses the state-of-the-art appropriate latest technologies to alert the concerned stakeholders and waits for actions to be taken.

Tistarelli and Schouten (2011) explain biometrics in ambient intelligence. This paper analyses the potential of biometric technologies within the general scope of ambient intelligence, attempting to identify key technological issues that may address privacy concerns. Various example applications are considered, where the exploitation of information contained in biometric data, such as facial expressions or other non-visual measurements, allows for a better understanding of the user's relationship with the environment. This, in turn, provides a substantial input to drive the services offered without compromising the user's privacy.

Arriany and Musbah (2016) discuss the application of voice recognition technology in smart home networks. This paper provides a comprehensive review of the concept of a smart home, its applications, system components, and the technologies used, including networking methods. The review is then extended to introduce voice recognition technology, which enables the control of any device through voice or speech commands. Furthermore, the paper proposes a design for a simple model of a miniature smart home network controlled by voice recognition technology. The various stages of the design and implementation of the proposed model are discussed, followed by a basic evaluation of the model's performance. Evaluation results confirm the superior performance of this design in a short-distance quiet environment using an external microphone configuration.

Kak et al. (2010) explicate Iris recognition system. In a biometric system, a person is identified automatically by processing the unique features posed by the individual. Iris Recognition is regarded as the most reliable and accurate biometric identification system available. In Iris Recognition, a person is identified by the iris, using pattern matching or image processing concepts of neural networks. The aim is to identify a person in real-time with high efficiency and accuracy by analysing the random patterns visible within the iris from some distance, by implementing a modified Canny edge detector algorithm. The major applications of this technology so far have been substituting for passports (automated international border crossing), aviation security, and controlling access to restricted areas at airports, database access, and computer login.

Zhu et al. (2020) explain indoor intelligent fingerprint-based localization, its principles, approaches, and challenges. In particular, fingerprinting localization has recently garnered attention due to its promising performance. The development of indoor localization technology should possess the ability for self-adaptation and self-learning in the future. The architecture demonstrates how to make localization more "smart" through advanced techniques. The working principles of state-of-the-art localization systems are summarized and compared in terms of their accuracy, latency, energy consumption, complexity, and robustness. It also discuss the challenges of existing indoor localization technologies, potential solutions to these challenges, and possible improvement measures.

Mustafah et al. (2007) explicate about an automated face recognition system for intelligence surveillance, with smart cameras recognizing faces in the crowd. Smart cameras are rapidly finding their way into intelligent surveillance systems. Recognizing faces in the crowd in real-time is one of the key features that will significantly enhance intelligent surveillance systems. The main challenge is the fact that the high volumes of data generated by high-resolution sensors make it computationally impossible for mainstream computers to process. In the proposed technique, the smart camera extracts all the faces from the full-resolution frame and sends the pixel information from these face areas to the main processing unit as an auxiliary video stream -

potentially achieving massive data rate reduction. Face recognition software running on the main processing unit then performs the required pattern recognition.

2. Existing Systems

2.1 Biometrics

Biometrics is used to identify or recognize a person based on the given input data, whether it is of physiological or behavioral characteristics. This technology has become an interesting area for implementing security systems, despite being one of the oldest technologies. Biometric systems use fingerprints, iris scans, voice recognition, and facial features to create secure digital signatures tied to an individual's unique traits. They offer enhanced security over traditional methods like passwords. Biometrics have expanded beyond security to sectors like healthcare and finance, with smartphones showcasing their integration into daily life. Despite benefits, concerns about privacy and data security persist, prompting efforts to establish regulations. Researchers explore innovative applications, like emotion recognition. The evolving synergy between biometrics and AI is likely to improve identification accuracy, paving the way for secure and convenient authentication methods. As an example, the biometric device is shown in Figure 1.

2.2 Signature Identification

The signature identification shown in Figure 2 utilizes a high-copying or manipulation technology. The procedure used by biometric systems to verify the signature is called Dynamic Mark Configuration (DMC). In this technology, there is no need for higher-level master

Figure 1. Biometric Device

Figure 2. Signature Identification Device

planning for forgery of the signature, and it can be copied by anyone. This is a major drawback in this technology. The vulnerability of Dynamic Mark Configuration (DMC) raises concerns about signature identification reliability. Lacking robust security, unauthorized individuals may exploit weaknesses for fraud. Insufficient authentication adds challenges, and reliance on high-tech copying highlights the need for advanced security in biometric systems. Addressing these issues is crucial for enhancing trust. Implementing extra security layers, encryption, and continuous monitoring can fortify against misuse. Prioritizing robust and secure methodologies is essential for maintaining the integrity of signature verification in advancing biometrics.

2.3 Voice Recognition

This technology was implemented by acoustic elements of discourse that had been found to vary among people. Here, the focal points are easy to utilize, and this system is now used as voice printers in mobile phones instead of typing. However, the drawbacks are that people can mimic others easily, be manipulated, and, furthermore, people's voices may not remain consistent; they may change with age. Advancements in voice recognition tech, powered by machine learning, enhance adaptability. Privacy and security concerns arise due to potential unauthorized access through voice imitation. Researchers are addressing voice variability issues for improved accuracy. Efforts focus on minimizing susceptibility to manipulation, ensuring a secure user experience. Ethical discussions emerge regarding responsible voice data use and algorithm biases.

Ongoing collaborative efforts aim to establish guidelines prioritizing user privacy and preventing discrimination. Despite its convenience, continuous research is crucial to address limitations and ensure a secure, reliable, and ethical integration into daily life. A voice recognition pattern is shown in Figure 3.

2.4 Iris Scans

Iris scans are located at the part of our eye, which is the colored textured tissue that surrounds the pupil of the eye. This scan security system operates with high accuracy, verification time is maximum 5 seconds to recognize a person. However, by scanning our eye, there is a chance of affecting our eyesight, and it contains a large amount of data to preserve, making it a high-cost effective solution. Here, the positioning of the eye pattern is more important, so taking more time for the exact position may affect the eyes. Eye-scanning tech enhances security through unique iris patterns, deterring replication. Colored iris complexity improves recognition but raises eyesight concerns, prompting ongoing research for risk reduction. Robust measures address data security due to large stored information. Ongoing efforts aim to enhance data management and encryption protocols. A balanced approach is crucial, considering trade-offs involving eyesight impact, data security, and cost-effectiveness in implementing this technology.

2.5 Finger Print Technology

Nowadays, biometric systems, as shown in Figure 5, are being used in colleges to track student attendance. They are also employed in ration shops, for bank

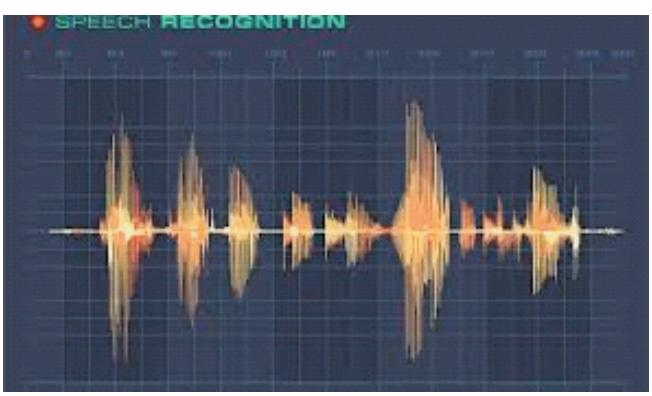

Figure 3. Voice Recognition Patterns

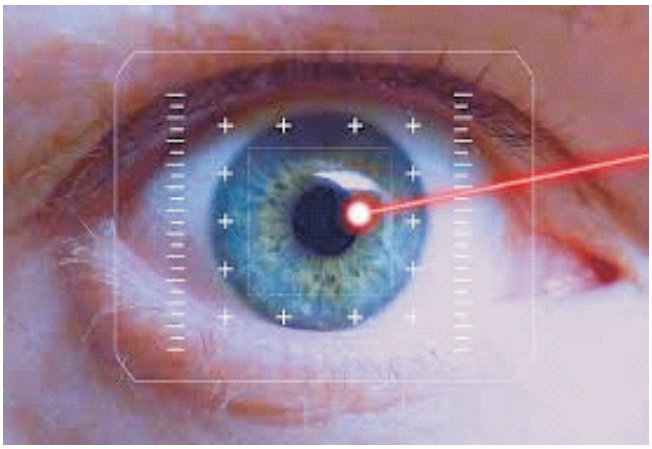

Figure 4. Iris Scanning

Figure 5. Biometric Machine

authentication, and to enhance phone security (Manjunath et al., 2015). Additionally, in processes such as land settlements, fingerprints are utilized for assurance, ensuring security against various factors such as dry skin, wet conditions, powders, dust, soil, mud, transparent cello tape, oily surfaces, sand scratches, ink drops, etc. These features constitute the fingerprint security system, but there are drawbacks. If a crack or cut occurs, especially during activities like kitchen or mud work, the fingerprint may fail. This means that the layers of the finger won't appear, making it soft to touch. During such instances, attempting authentication will result in a message indicating that the thumb is not detected, rendering the authentication process unsuccessful. Another significant drawback is the emergence of artificial fingers in the market, mimicking real finger features. This makes the system vulnerable to hacking, as unauthorized access

becomes easier. Figures 6 and 7 show a visual representation of how biometric devices scan and authenticate fingerprints.

2.6 Recognition of Face

Face recognition is a highly secure system in current technology, safeguarding our accounts from hackers. Manipulating one's face with specific measurements is challenging, and the system incurs a high cost. Despite the expense, the face recognition system is readily accepted by the public. However, in CCTV, individuals often cover their faces while committing crimes in various sectors such as banks, libraries, railway stations, airports, and ATM centers. This poses a drawback, making it relatively easy to integrate with other security systems. The main challenge lies in accommodating changes that occur to the human face over time, including aging, facial hair, and skin tone. Nowadays, many people undergo plastic surgeries for specific features like lips, nose, and cheeks, which can potentially corrupt or hack the system. It is essential to note that a person's age is not constant for many years, highlighting a significant drawback of the existing system. The face recognition system is shown in Figure 8.

Figure 6. Scanning Pattern

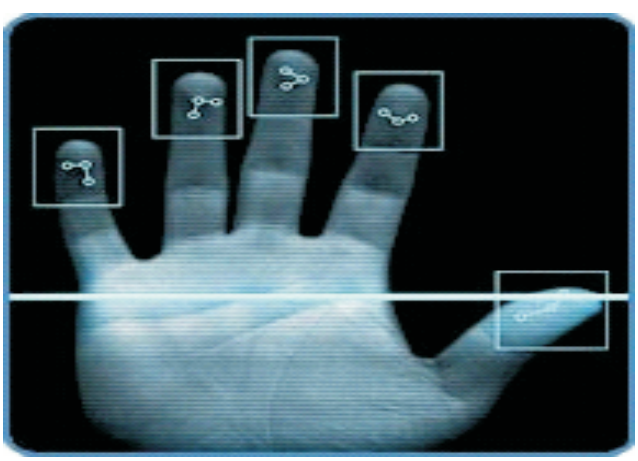

Figure 7. Finger Tips Scanned by the Device

2.7 Eye Recognition

This method is similar to the Iris scan method discussed. However, this system can potentially damage our eyes. Additionally, it takes a considerable amount of time to identify. Furthermore, the prolonged exposure to intense light during the eye recognition process may raise concerns about potential harm to the retina. Despite its potential drawbacks, this method offers a high level of accuracy in identifying individuals based on unique patterns in the iris. It is crucial for developers and researchers to address the safety and efficiency concerns associated with this technology before widespread implementation. The eye recognition pattern is shown in Figure 9.

3. Proposed System

The proposed system aims to overcome all the drawbacks in the existing systems. This proposed system is designed to provide high security with efficiency, making

Figure 8. Face Recognition Patterns

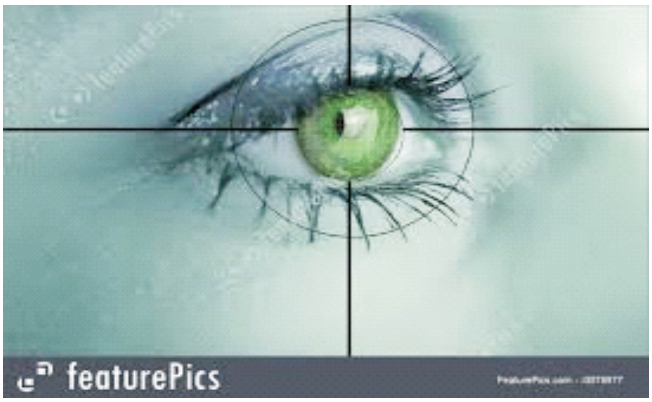

Figure 9. Eye Recognition Pattern

it a perfect solution for saving and protecting individuals from the hassle. The system is highly accurate and stands as the world's first contactless personal identification system, utilizing the vein patterns in human palms, as shown in Figure 10, to confirm a person's identity. Another notable feature is its contactless nature, giving it a hygienic advantage over other biometric authentication technologies. In this method, when Infrared Rays (IR) are reflected on the palm as shown in Figure 11, the sensor emits a near-infrared beam towards the palm of the hand. Blood flowing through the veins absorbs this radiation, causing the veins to appear as a black pattern. Oxygenated blood passes through the arteries, and deoxygenated blood passes through the veins, returning to the heart. These veins, responsible for pumping blood internally from the heart, appear blue in color. Considering the hygiene requirements necessary for use in public environments, this technology is applied in various vertical markets, including security, financial, banking, healthcare, commercial enterprises, educational facilities, and other industries with specific applications (Malhotra, 2014).

Figure 10. Human Palm

The operation of the vein recognition system is explained with the help of a proposed block diagram. Figure 12 shows the block diagram of proposed architecture.

This paper also describes some examples of financial solutions and markets that have been developed based on this technology. Generally, people worry about security problems. Individuals also face the risk that others can easily access their accounts at any time or anywhere due to this vulnerability. Personal identification technology, which can distinguish between registered legitimate users and impostors, is now generating interest in the proposed method. Currently, a 4-digit PIN number or any identification cards can be stolen, and the numbers can be easily forgotten. To address these problems, the vein technology shown in Figure 12 is proposed by Fujitsu in R&D biometric authentication technology, focusing on four methods: fingerprints, voice prints, face recognition, each of which has drawbacks. However, palm vein technology is the best in Fujitsu's research, specifically in vascular pattern authentication.

3.1 Operation of Proposed System

When the palm is illuminated with near-infrared light, the image seen by the human eye shows deoxygenated

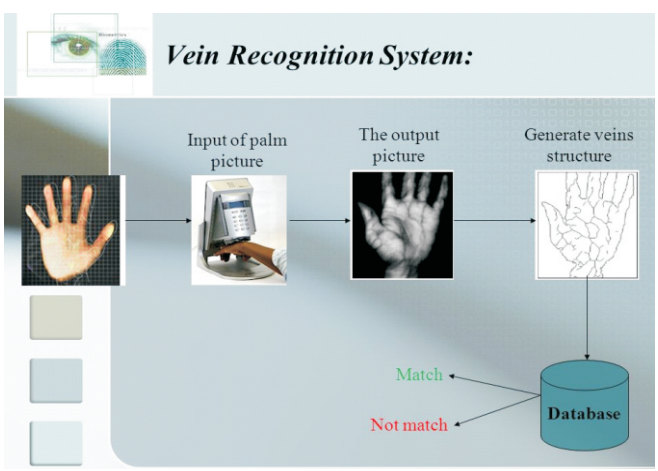

Figure 11. Vein Recognition System

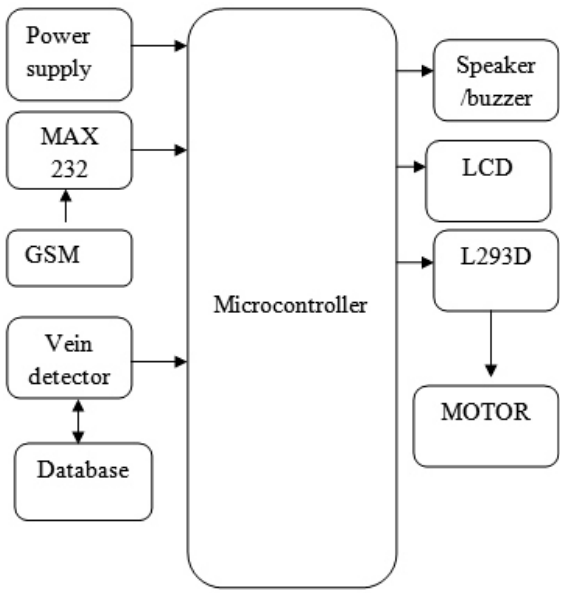

Figure 12. Block Diagram of Proposed Architecture

hemoglobin in the palm absorbing this light, thereby reducing the reflection rate and causing the veins to appear as a black pattern. First, we need to take an image of the palm and register it. During authentication, the palm is photographed with near-infrared light, and the vein pattern is extracted through image processing, which is then compared with the registered vein pattern. Another advantage is that there is no hair in the middle of the palm, making it easy to photograph. The palm also exhibits minimal variations in skin color compared to fingers or the back of the hand, where color can darken in certain areas. When the body temperature is lowered, placing the hand on the particular screen captures a photograph. On the screen, black blood vessels become visible due to the decreased blood flow through the body, increasing the hand's light transmittance. Light passes through it more easily. The false acceptance rate for this system is 0.00008%, and the false rejection rate is 0.01%, provided the hand is held over the device three times during registration, with one retry for comparison during authentication.

This system can be used for entry and exit in rooms and buildings in companies, advanced locker systems (Srinivasan et al., 2015), and outsourcing centers where important customer data is stored. Due to increasing concerns about security, it is user-friendly and also enhances our account savings techniques by establishing connectivity between a mobile device through GSM (Hanumanthu & Chandra, 2013) and the palm vein system. If anyone attempts to touch the locker screen, it will automatically respond and send a message to phone using signals, or we can connect through WLAN WiFi settings.

4. Discussion

The Embedded System-Based Enhanced Smart Security System is a state-of-the-art solution integrating advanced technologies for proactive and precise security monitoring. This compact system combines embedded systems for efficient performance, addressing contemporary security needs.

Biometric systems enhance security through physical or behavioural traits, but privacy and data security concerns persist, requiring regulations. Integrating biometrics and AI improves identification accuracy for secure authentication. Signature identification faces challenges in reliability and vulnerability, necessitating additional security layers and continuous monitoring. Voice recognition technology is user-friendly but raises concerns about mimicry. Ongoing research focuses on minimizing manipulation susceptibility and addressing privacy concerns. Iris scans offer high accuracy but raise eyesight impact and data management concerns. Efforts aim to enhance data security while considering trade-offs. Fingerprint technology, widely used, faces challenges from environmental factors and artificial fingers. Face recognition systems are highly secure but face challenges with changes over time, emphasizing the need for ongoing research. Eye recognition, like iris scans, offers high accuracy but raises concerns about potential harm and prolonged exposure to intense light, requiring safety and efficiency considerations.

The proposed system aims to overcome the drawbacks of existing biometric systems by utilizing vein patterns in human palms for contactless personal identification. This system boasts high accuracy, contactless operation, and applicability in various sectors, including security, finance, healthcare, and education. The integration of Infrared

Rays (IR) ensures hygienic advantages, making it suitable for public environments. The proposed system operates by illuminating the palm with near-infrared light, capturing the vein pattern through image processing for authentication and offers advantages such as minimal variations in skin color, ease of photographing, and high accuracy with low false acceptance and rejection rates.

The Embedded System-Based Enhanced Smart Security System, with its integration of advanced technologies and focus on contactless palm vein recognition, stands at the forefront of transformative security solutions. As the paper delves into the technical aspects and practical implementations, it sheds light on the system's potential to redefine standards in intelligent surveillance and monitoring. The proposed system addresses the limitations of existing biometric technologies, offering a secure, efficient, and hygienic solution for diverse applications in the evolving landscape of security challenges.

Conclusion

The landscape of security challenges in the modern era demands innovative and intelligent solutions. The Embedded System-Based Enhanced Smart Security System emerges as a cutting-edge response, integrating advanced technologies to meet the complexities of contemporary security requirements. This system's utilization of embedded systems, artificial intelligence, and connectivity defines a new era in security solutions, poised to redefine the standards of intelligent surveillance and monitoring. The existing biometric systems, such as biometrics, signature identification, voice recognition, iris scans, fingerprint technology, face recognition, and eye recognition, each have their strengths and weaknesses. While they enhance security through physical or behavioural traits, concerns about privacy, vulnerability, and reliability persist. The proposed system, utilizing vein patterns in human palms for contactless personal identification, aims to overcome these drawbacks. It offers high accuracy, contactless operation, and hygienic advantages, making it suitable for various sectors.

In the realm of security solutions, the Embedded System-Based Enhanced Smart Security System, with its integration of advanced technologies and focus on contactless palm vein recognition, stands out as a transformative and robust solution. As technology continues to evolve, this system is positioned to redefine the standards of intelligent surveillance and monitoring, providing a secure, efficient, and hygienic solution for the diverse challenges in the ever-changing security landscape.

References

[1]. Arriany, A. A., & Musbah, M. S. (2016, September). Applying voice recognition technology for smart home networks. In 2016 *International Conference on Engineering & MIS (ICEMIS)* (pp. 1-6). IEEE.

[2]. Hanumanthu, G., & Chandra, D. (2013). Wireless Identification of RFID, Fingerprint & IRIS. *International Journal of Innovative Research and Development*, 2(5).

[3]. Kak, N., Gupta, R., & Mahajan, S. (2010). Iris recognition system. *International Journal of Advanced Computer Science and Applications,* 1(1).

[4]. Indumathi, J., Asha, N., & Gitanjali, J. (2020). Smart security system using IoT and mobile assistance. In *Emerging Research in Data Engineering Systems and Computer Communications: Proceedings of CCODE* (pp. 441-453). Springer Singapore.

[5]. Malhotra, S. (2014). Banking locker system with odor identification & security question using RFID & GSM Technology. *International Journal of Advances in Electronics Engineering–IJAEE*, 4(3), 156-159.

[6]. Manjunath, M. P., Kumar, P. R., Kumar, P., Gopinath, N., & Haripriya, M. E. (2015). NFC based bank locker system. *International Journal of Engineering Trends and Technology (IJETT)*, 23(1), 15-19.

[7]. Mustafah, Y. M., Azman, A. W., Bigdeli, A., & Lovell, B. C. (2007, September). An automated face recognition system for intelligence surveillance: Smart camera recognizing faces in the crowd. In 2007 *First ACM/IEEE International Conference on Distributed Smart Cameras* (pp. 147-152). IEEE.

[8]. Prasad, S., & Suneel, D. (2015). Proximity sensor based

security lock and theft detection. *International Journal of Science Technology and Management*, 4(12), 81-88.

[9]. Srinivasan, R., Mettilda, T., Surendran, D., Gobinath, K., & Sathishkumar, P. (2015). Advanced locker security system. *International Conference on Information Engineering, Management and Security (ICIEMS)*, 4(1), 1465-1471.

[10]. Taiwo, O., Ezugwu, A. E., Oyelade, O. N., & Almutairi, M. S. (2022). Enhanced intelligent smart home control and security system based on deep learning model. *Wireless Communications and Mobile Computing*, 1-22.

[11]. Tistarelli, M., & Schouten, B. (2011). Biometrics in ambient intelligence. *Journal of Ambient Intelligence and Humanized Computing,* 2, 113-126.

[12]. Zhai, Y., & Cheng, X. (2011). Design of smart home remote monitoring system based on embedded system. In 2011 *IEEE 2nd International Conference on Computing, Control and Industrial Engineering*, (Vol. 2, pp. 41-44). IEEE.

[13]. Zhu, X., Qu, W., Qiu, T., Zhao, L., Atiquzzaman, M., & Wu, D. O. (2020). Indoor intelligent fingerprint-based localization: Principles, approaches and challenges. *IEEE Communications Surveys & Tutorials,* 22(4), 2634-2657.

ABOUT THE AUTHOR

P. Lokesh, Department of Electronics and Communication Engineering, Vemu Institute of Technology, Pakala, Andhra Pradesh, India.