

MES COLLEGE OF ENGINEERING-KUTTIPPURAM
DEPARTMENT OF COMPUTER APPLICATIONS
20MCA244 - SEMINAR

PRO FORMA FOR THE APPROVAL OF THE FOURTH SEMESTER SEMINAR

(Note: All entries of the pro forma for approval should be filled up with appropriate and complete information. Incomplete Pro-forma in any respect will be rejected.)

Roll No :MES20MCA-2031

Name :MUBEENA C

Academic Year : 2021-2022

Year of Admission : 2020

Proposed Topic: (At least 3 topics to be given in the order of preferences. Abstract of each topic is to be attached separately)

Topic-1: BIOMETRIC RECOGNITION OF INFANTS

References::

- Lacey Best-Rowden, YovahnHoole, Anil K. Jain, *“Automatic Face Recogni- tion of Newborns, Infants, and Toddlers: A Longitudinal Evaluation,”* 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), 1-8, 2016.
- Youtube videos

Topic-2: SECURING HEALTH INFORMATION USING MODULAR ENCRYPTION STANDARD

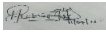
References:

- J. C.-W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, and M. Aloqaily, “Privacy preserving multi-objective sanitization model in 6G IoT environments,” *IEEE Internet Things J.*, early access, Oct. 21, 2020, doi:
- J. C.-W. Lin, Y. Shao, Y. Djenouri, and U. Yun, “ASRNN: A recurrent neural network with an attention model for sequence labelling,” *Knowledge Based Syst.*, vol. 212, Jan. 2021, Art. no. 10654

Topic-3: SYNCHRONOUS HEAD MOVEMENT AS A CROWD BEHAVIOUR -BASED SECURITY SYSTEM

References:

- I. Serrano, O. Deniz, J. L. Espinosa-Aranda, and G. Bueno, “Fight recogni- tion in video using Hough forests and 2D convolutional neural network,” *IEEE Trans. Image Process.*, vol. 27, no. 10, pp. 4787–4797, Oct. 2018, doi: 10.1109/TIP.2018.2845742.
- M. Perez, A. C. Kot, and A. Rocha, “Detection of real-world fights in surveillance videos,” in *Proc. IEEE Int. Conf. Acoust., Speech Signal Pro- cess. (ICASSP)*, May 2019, pp. 2662–2666, doi: 10.1109/ICASSP.2019. 8683676.

Dated signature of the student : 

FOR DEPARTMENT USE ONLY:

1. Topic allotted :
2. Date of Presentation :
3. Date of Submission of the Draft Report :
4. Date of Submission of Final Report :

COMMENTS

Seminar Coordinator

TOPIC-1:BIOMETRIC RECOGNITION OF INFANTS

INTRODUCTION:

Recognition of infants and minors precisely from birth is becoming ubiquitous. The choice of biometric modality to use for infants and minors has always been a bottleneck due to imaging devices and uncooperative nature of infants. To mitigate these challenges a research project has been started with the aim of developing a prototype biometric recognition system to acquire biometric data from young children, and determine or verify the identities of these children from birth until they apply for their identification documents (which can be done at the age of 16 years in South Africa). To assess the performance of the existing and newly developed biometric acquisition and recognition systems for children and achieve the aim of the project, it is required to acquire biometric data from children and successfully compare this biometric data. The benefits of developing such a system are manifold. The output of this research is meant to address issues of identity theft and fraud against children, help combat child trafficking, assist with reuniting small children who are lost with their parents, and improve healthcare management systems for children [1]–[5]. The unique challenge that is posed is that existing technologies are not capable of acquiring biometric information from newborn infants and successfully matching it to the same individuals during growth and adulthood with accuracy and reliability, thus leaving children vulnerable to exploitation in various ways, such as identity theft and child trafficking. As a first step in solving this challenge, this paper addresses the acquisition of biometric information from children during the first year of life. There has been some research into developing biometric recognition systems for children. However, there are still challenges to overcome in creating a complete biometric system for infants and minors.

RELEVANCE:

Biometric recognition is often used for adults for a variety of purposes where an individual's identity must be ascertained. However, the biometric recognition of children is an unsolved

challenge. Solving this challenge could protect children from identity theft and identity fraud, help in reuniting lost children with their parents, improve border control systems in combatting child trafficking, and assist in electronic record-keeping systems. In order to begin the development of biometric recognition systems for children, researchers collected fingerprint, iris, and outer ear shape biometric information from infants. Each modality provides different challenges. Where possible, the performance of existing hardware and software that was developed for adults was assessed with infants. Where necessary, novel hardware or software was developed. For the ear modality, existing hardware and software which have previously been applied to adults were applied to children. For the iris modality, existing hardware was used to acquire the images, while adjustments to the existing preprocessing algorithms were applied to cater for the localisation and segmentation of infant irises. For the fingerprint modality, novel hardware and image processing software were developed to acquire fingerprints from infants, and convert the images into a format which is backward compatible with existing international standards for minutiae extraction and comparison. The advantages and disadvantages of using each of these modalities during the first year of life were compared, based on both qualitative assessments of usage, and quantitative assessments of performance. While there is no conclusively best modality, recommendations of usage for each modality were provided.

REFERENCE

- Lacey Best-Rowden, YovahnHoole, Anil K. Jain, *“Automatic Face Recognition of Newborns, Infants, and Toddlers: A Longitudinal Evaluation,”* 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), 1-8, 2016.
- Youtube videos

Topic-2: SECURING HEALTH INFORMATION USING MODULAR ENCRYPTION STANDARD

INTRODUCTION:

As computing technologies have rapidly growth, cloud computing has earned a lot of popularity in recent years through applications, services, storage, and computing over the Internet. It is commonly utilized in many domains like Medical Science, Agriculture, Business, Information Technology, and many others. Additionally, it encourages resource provisioning flexibility and cost-effective decoupling administrations. Smart devices like smartphones and tablets are progressively turning into a fundamental constituent of human life as a convenient and effective tool for communication that is not limited by place and time. Smart device users assemble rich experience of different administrations from mobile apps such as Google Applications and iPhone applications which run on the remote servers using wireless connectivity to the network. The integration of cloud computing with mobile phones is known as Mobile Cloud Computing (MCC).As MCC can offer a few significant benefits, for example, expanded battery life and high-level storage capability, scalability, adaptability, and a few key demands keep on being a significant hindrance to MCC. An overview of MCC is depicted in FIGURE 1. One of the leading difficulties incorporates the security and privacy of confidential information. Nowadays, MCC is highly involved in cloud based-health monitoring, but due to lack of proper security, it is not getting as much attention as it should be. Such challenges need to be addressed to appeal to the mobile cloud user towards MCC.

RELEVANCE:

Despite the numerous and noticeable inherited gains of Mobile Cloud Computing (MCC) in healthcare, its growth is being hindered by privacy and security challenges. Such issues require the utmost urgent attention to realize its full scale and efficient usage. There is a need to secure Health Information worldwide, regionally, and locally. To fully avail of the health services, it is crucial to put in place the demanded security practices for the prevention of security breaches and vulnerabilities. Hence, this research is deliberated on to provide requirement-oriented health information security using the Modular Encryption Standard (MES) based on the layered modelling of the security measures. The performance analysis shows that the proposed work excels, compared to other commonly used algorithms against the health information security at the

MCC environment in terms of better performance and auxiliary qualitative security ensuring measures.

REFERENCE:

- J. C.-W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, and M. Aloqaily, “Privacy preserving multi-objective sanitization model in 6G IoT environments,” IEEE Internet Things J., early access, Oct. 21, 2020, doi:
- J. C.-W. Lin, Y. Shao, Y. Djenouri, and U. Yun, “ASRNN: A recurrent neural network with an attention model for sequence labelling,” Knowledge Based Syst., vol. 212, Jan. 2021, Art. no. 106548.

Topic-3: SYNCRCHRONOUS HEAD MOVEMENT AS A CROWD BEHAVIOUR -BASED SECURITY SYSTEM

INTRODUCTION:

Closed-circuit television (CCTV) systems first appeared in 1942. Ever since, the technology has been in constant development, transforming from mere visual and audio recording machines for security personnel to smart CCTV and surveillance systems that can understand a situation and report it to security personnel or take immediate action. Advances in AI, and specifically deep learning, made it possible for surveillance systems to detect fighting , an abandoned suitcase in an airport, the possession of a weapon, a robbery taking place and the movements of thieves , and suspicious activity and Predictive systems can predict car accidents and the next few seconds of movement , to list a few applications. However, if a visual or auditory incident takes place outside the range of the CCTV system, current systems will fail to detect and report it. In this paper, we propose SHMOV, a smart security system that analyses crowds' reactive behaviour in a defined time and location to predict a nearby security incident outside of the range or field-of-view .In SHMOV, we investigate the ability to detect heads as objects utilizing deep learning technology, then detect head direction and movement speed. We hypothesize that when people synchronously move their heads from various directions to be locked in one direction at a predefined speed and time, a security incident might be taking place outside of the range or field-of-view. We evaluated the system's accuracy by introducing an accompanying sound deviation metric as well as facial expressions that occur during the detected synchronous head movement. We employed an alert stage approach, where each triggered stage increases the probability of an incident taking place. The scope of this paper is to detect an incident outside the range or field-of-view by analysing the crowd's reactive behaviour that is triggered by human sensing capabilities.

This paper presents the following contribution to the smart CCTV surveillance security systems:

- 1)To provide a crowd-behaviour-based SHMOV security system, which allows for detecting outside of field-of- view incidents
- 2)To provide a detection method for out-of-range incidents using the crowd's sensing capabilities that result in reactive behaviour. The elected method is by detecting head synchronous movements towards the source of the out of range incident.
- 3)To evaluate the SHMOV system's accuracy in correctly detecting the existence of an out-of-range incident and the location of the incident

The SHMOV system's benefit may also contribute in the possibility of requiring less than planned camera systems as it projected to detect out of range incidents saving organizations from needing to install extra cameras

RELEVANCE:

Individuals react in response to internal or external stimuli, whether visual, auditory, gustatory, olfactory, cutaneous, kinesthetic or vestibular. This behaviour is not fully utilized to infer possible security incidents taking place or about to take place in a defined geographical area outside of the range or field- of-view of security systems. Sensors are in place in the form of human senses. If these natural sensors are utilized together with advances in deep learning technology, researchers will be equipped to build advanced security solutions. In this paper, we propose a security system based on the crowd behaviour of synchronous head movement (SHMOV). The system provides an alert of a possible security incident if synchronous head movement occurs among a crowd in a specific area by analysing the video stream from a camera. We assessed the proposed SHMOV system using an experiment on 20 participants in auditory, visual, and olfactory settings. This experiment demonstrated the technology's potential, with 100%, 100%, and 80% incident detection accuracy and alerts issued 9, 24, and 47 seconds after the start of each incident, respectively.

REFERENCE:

- I. Serrano, O. Deniz, J. L. Espinosa-Aranda, and G. Bueno, "Fight recognition in video using Hough forests and 2D convolutional neural network," *IEEE Trans. Image Process.*, vol. 27, no. 10, pp. 4787–4797, Oct. 2018, doi: 10.1109/TIP.2018.2845742.
- M. Perez, A. C. Kot, and A. Rocha, "Detection of real-world fights in surveillance videos," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, May 2019, pp. 2662–2666, doi: 10.1109/ICASSP.2019. 8683676.