Facial Recognition Using Segmented Facial Points Algorithm for Intelligent Surveillance System

Asia Pacific Journal of Multidisciplinary Research
Vol. 8 No.2, 158-166
May 2020
P-ISSN 2350-7756
E-ISSN 2350-8442
www.apjmr.com
ASEAN Citation Index

Tracy N. Tacuban (DIT)
Iloilo Science and Technology University, Burgos St. Lapaz Iloilo City, Philippines
tracy.tacuban@isatu.edu.ph

Date Received: October 17, 2019; Date Revised: April 27, 2020

Abstract-*In this paper, the researcher presents the Facial Points Segmentation Algorithm as an improved feature matching process of Scale Invariant Feature Transform (SIFT). Because the feature matching process in SIFT would include the features of the image background, errors are automatically introduced in the matching process. In this study, instead of matching the overall features of an image, the algorithm logically divides the human face into two segments – the eye and face segment. Features from query and gallery/training images are matched only if they belong to the same segment and the similarity of the features is determined using cosine distance. The method is applied in Video Surveillance System designed for automatic face recognition using the profile of people contained therein. Based on the results of the recognition process, the precision rate of the system using F-Measure is 82.25% and considered "Good" while the functionality of the surveillance system using ISO 25010 metrics is rated "Effective" based on the evaluation of ICT professionals and expected users. The importance of the study resides in its potential application in surveillance, attendance and other related systems requiring facial recognition. Its scheduling system allows the user to set specific time and day to record surveillance video. Meanwhile, its notification system sends email and SMS message to named recipients for intrusion within its confine thereby improving the features of a surveillance system and boosts the sense of security of the user. The algorithm is terse enough to filter and compare image features within the same face segments but good enough to reduce the processing time as well as limit the possibility of matching error which is necessary for surveillance systems and specifically, for face recognition algorithms which could be further enhanced by future researchers.*

Keywords: *Facial Recognition, Segmented Facial Points, Algorithm, Surveillance System, and Biometric Technology*

INTRODUCTION

Most establishments, schools and even homes use Closed Circuit Television (CCTV) for monitoring and security purposes Da Cruz [1], because most people view CCTV systems as detection tool [2]. However, traditional CCTV systems mainly record events or activities and lacks the capacity of monitor intrusion or identify people with criminal records. Any security-related activities maybe "captured by camera" but the tedious task of detection and identification is left to the system user.

However, traditional CCTV systems mainly record events or activities and the recordings are stored in the control unit commonly a personal computer which is usually proximate to the camera. Based on Corkill [3], a researcher and expert in intelligence and security, a CCTV camera still relies on human operators but isunreliable in monitoring everything. When a security-relevant event or any anomaly is observed, these videos are viewed by its owner or operator for verification. When the control unit is subject to theft, the recordings are likewise gone.

One of the most effective ways of monitoring and identifying people is by the use of biometric technology. Recent interest in computer vision shifts towards facial recognition due probably to the fact that it is the usual way of identifying people.

As technology advances, research in the field of face recognition systems has drawn much attention owing to the difficulty of the system and its numerous applications. The difficulty especially on CCTV systems is brought by pose variations, lighting, occlusion and other factors. Meanwhile, recognition

systems are vital for security, monitoring and immediate response for relevant events**.**

According to Lin [4], Facial Recognition is one of the most used biometric methods in the field of security, psychology, and computer vision because of its high accuracy in verifying and recognizing the identity of an individual. The advance of technology ushered the way for the development of intelligent CCTV that could detect and recognize people through facial recognition.

Also, according to Yadan [5], the processes of facial recognition include the face detection, model training, and recognition. Facial recognition systems align the face before extracting the face signature to make the facial signature better. Aligning is the processes that include rotating and scaling the captured face to focus on the face key features such as the eyes, nose, mouth, jaw and other facial profiles. The face is then represented as vector floating point numbers which are represented as a ratio between the distances of the facial features.

The first recognition techniques are usually based on geometrical information owing to the fact that facial features have geometric properties. The relative distances between keypoints, such as mouth corners or eyes, were calculated and used to characterize faces [6]. The face geometry method was likewise enhanced by Fagertun [7] where the geometrical and color information were combined to discriminate each person's facial features and is able perform to facial recognition.

However, the application of facial recognition in the surveillance system remains a difficult problem since the automated facial recognition have plenty of desirable properties that need to be considered according to Wójcik, Gromaszek, and Junisbekov [8]. Moreover, as stated by De Marsico [9] and Bupe [10] facial recognition in a surveillance system is still considered as an open area of research and deep learning since all existing facial recognition algorithm poses several issues.

Most geometric approaches for facial recognition were superseded by color-based techniques, which provided better results. The early works focus on extracting global features like Eigen and Fisher faces [11] which project the whole face into a linear subspace to acquire or identify face variations. Such methods are usually computationally expensive and are not highly discriminative especially when images are subject to illumination change and other distortions.

The focus then shifts towards local features-based matching with Local Binary Pattern (LBP) [12] gaining prominence. The algorithm extracts pixel intensity to construct the histogram representing the description of the face features. But the performance of LBP and its variants are affected by changes in illumination and pose variations.

To address the preceding pitfalls, algorithms Albiol [13], Nguyen, Bai,andLinlin[14], Bay et. al [15] andLowe [16] developed fast and robust image matching algorithm is essential for video surveillance systemthat manifest robust performance in representing local features.

In 2016,Noone and Bergman [17] developed the Electronic Article Surveillance (EAS) System which utilized a method that performs electronic article surveillance which is consist of generated image data using at least one imaging device. The image data is processed in a computer processing device located at an Electronic Article Surveillance (EAS) pedestal to recognize the presence of the facial image comprising a face of a person within the image data and identify the person in the image. A notification is sent and received by the server once the system recognizes a person in the surveillance system.

This study was also anchored to Bhavani et al. [18] who developed a system that detects and recognizes people from a live stream video. The researchers collected the images of an individual person and allow the camera to detect the person's frontal face. The researchers use the Viola-Jones algorithm to perform the detection of the person's face in the live video stream. The program will then import all the person's detected images from their individual datasets. The researchers used the LBPH Face Recognizer to train the images and use a Fisher Face Recognizer in the camera's live stream to detect the faces. The system utilizes the predict method to match the image among the dataset. The system will display the closely matched image, or prompt the user that the person is unrecognized by the system.

This study is an attempt to conduct the matching of features on specific face locations using facial point's segmentation and apply the method in surveillance system which will allow the user to enter the profile of people for face recognition and enter the list of people as recipients of system notifications; detect and recognize people and when the recognized person has criminal record, send an email message to all listed recipients containing the record as well as an attached image of the person; store all captured

images and related videos for user viewing; allow the user to create a monitoring schedule and if SMS notification is enabled, send SMS notification when people are detected; and log activities and allow the user to view/ print log entries pertaining to the number of people detected and total SMS and email sent on daily, weekly and monthly basis.

Due to the incompatibility of the IP Camera with the hardware used for testing the surveillance system, the researcher initially tested the system using the laptop's built-in web cam which was later discovered to render poor quality images. It somehow slowed the researcher's time to explore on the many facets of face recognition and the proposed study in particular.

MATERIALS AND METHOD

The study Facial Recognition Using Segmented Facial Points Algorithm for Intelligent Surveillance System attempts to design a surveillance system that can recognize people and send SMS and email message to contact persons on security-relevant issues like when an intrusion is detected within its covered area.

In designing the system, the researcher chose the Prototyping methodology as the appropriate design method considering the process involved in prototyping as well as the constraints imposed on the researcher, specifically, time constraint. The prototyping model is according to Dennis, Wixom, and Roth [19], performs the analysis, design, and implementation phases concurrently. All three phases are performed repeatedly in a cycle until the system is completed. The key advantage of a prototyping-based method is that it can provide a very quick working system where users can interact and provide immediate feedback to the developer about the system's performance and features.

The functionality of the system is depicted using a Use Case Diagram as shown in Figure 1. Use Case Diagram according to Dennis, Wixom, Tegarden [20], depicts the functionality of the system and its interaction with the environment. The system has one actor denoted as the end user or CCTV operator with the task of operating the system. Login is the preliminary use case of the actor as the user is always required to provide a valid authentication token. The user has a username and password as a precondition with the assumption that the user has valid credentials. On successful completion, the user gains access to the system and initiate the other use cases. The alternative process is performed when the user is not allowed to gain access to the system if the submitted login credentials are invalid.

The Conduct Surveillance use case describes the process of taking surveillance video and viewing the result of the system's monitoring process. The user selects the camera button to initiate the surveillance process and view the video feed as well as the result of the face recognition process. On successful completion, the user may have viewed the surveillance monitor and the system had recorded a surveillance video, saved the captured images of people that were on site during the surveillance period and generated a system log for later viewing by the user.

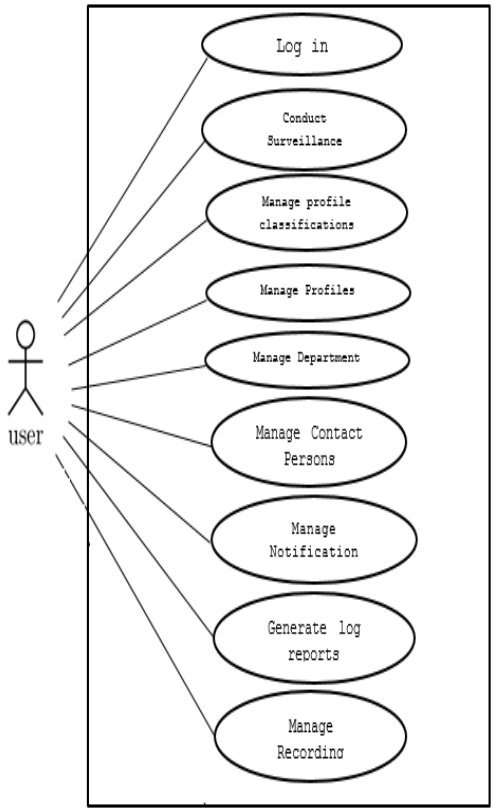

Figure 1.*Use Case Diagram of the system*

To perform recognition, SIFT was used. SIFT is superior as an object detection algorithm. When applied to face recognition, the image background would likely be included in the matching process. To filter out the keypoints that are outside the face region, the human face is logically divided into two segments – the eye and face segment. Figure 2 depicts the logical division of the face image using facial points segmentation.

The logical region of the eye segment is bounded by the bigger green rectangle and the face segment by the orange rectangle. Only keypoints located within this two segments will be used in the determining the similarity of the features. A small percentage on both sides of each bounding box would expose background features when the image is in full frontal view. The area is intended to cover the face area when the image is not fully as most likely the angle between the CCTV camera and the captured image would have some degree of orientation. There is also a small intersecting section between segments to compensate for faces looking downward or upward.

Figure 2.*Facial Points Logical Face Segmentation*

Likewise, the smaller rectangles are bounding box for validating the face detection process such that eyes detected by classifiers should "touch" this region and the detected mouth should be within the orange region. The smaller bounding box is used to validate the uploaded image of each person.

The system requires six (6) images for each personal profile. For each selected image, the image is validated using classifiers for the presence of eyes, nose and mouth. After all the images are validated, the system will save the personal profile and create a folder for saving the images. The images are then saved on that folder after which the system will generate the keypoints and descriptors for each image using SIFT algorithm by invoking the appropriate Open CV functions.

The face is considered recognized only if it has the highest match features and if the matched features in the eye segment is greater than or equal to the threshold value of the eye segment and the matched features in the face segment is greater than or equal to the threshold value of the face segment. Both the eye Threshold and face Threshold are set to 2 indicating that there should be at least 2 keypoint matches in either the face and eye segment for a query image to match the training face. Otherwise, the query image is considered "unknown".

As part of the features of the surveillance system, if the query image is recognized and is a criminal, the system will send an email to all assigned recipients with an attached image of the person.

The Manage Personal Profile Classification use case describes the process of adding and updating the classifications of the personal profile to be used in the Manage Profiles use case. On successful completion, the user added and/or updated the list of profiles.

The Manage Profile use case describes the process of adding and updating the profiles of known people to be tracked by the system. The precondition, the user has a list of profiles to be added, updated or deleted. On successful completion, the user has either added, updated or deleted profiles of people in the system's database. When adding a profile, the user adds the name of a person and the user likewise selects the department where the person belongs to. The user also selects the profile category based on the list provided in the Manage Profile Classification. The user then adds six (6) profile pictures for each individual. On successful completion, the record is either added, updated or deleted based on the action taken.

The process of adding and updating the Department names is described in the Manage Department use case. As a precondition, the user has a list of department names to add, update or delete. On successful completion, the user had either added, updated or deleted department record(s). The department name is used in Manage Profiles where the user selects where the department the person belongs.

The Manage Contact Persons is performed when adding and updating the list of contact persons that will receive notifications from the system. When adding or updating a record, the user selects whether the contact person should receive SMS and/or Email notifications. The user provides the contact person's mobile number and email address in this use case.

The Manage Monitoring schedule describes the steps performed in adding, updating or deleting the notification schedule. The schedule is used by the system to control SMS notifications to contact persons. On successful completion, the user had either added, updated or deleted the monitoring schedule.

The user initiates the Generate Log Report use case to view or generate a surveillance report of the

surveillance process. The precondition, the user wants to generate a log report. On successful completion, the user selects the period covered by the log report – either daily, weekly or monthly, and such report is generated. The report contains the number of people detected within that specified period where each report row contains the total number of people by profile category.

The user initiates the Manage Recording use case to view the system's record of its detection process. As a precondition, the system must already have started monitoring and the user may either want to view the surveillance video,or the surveillance pictures or delete the surveillance log to free up disk space. On successful completion, the user has either viewed the surveillance videos and pictures or deleted the surveillance data to increase the system's storage space.

The system is tested and evaluated using the white box and black box testing. Black box testing is also called functional testing. According to Williams [21], this is a testing technique that ignores the internal mechanism of a system or component and focuses solely on the outputs generated in response to selected inputs and execution conditions. The software tester should not have access to the source code itself. However, the tester should be knowledgeable of the software requirements that are needed in the system.

On the other hand, white box testing is a testing technique in which the tester, often the developer, knows what the code looks like and writes test cases by executing methods with certain parameters. White Box Testing is also called structural testing and glass box testing. This is a technique that takes into account the internal mechanism of a system or component.

The system was pilot tested at the Computer Department of Iloilo Science and Technology University. To select the respondents of the study, the researcher uses the purposive sampling method. As stated by research-methodology.net [22], purposive sampling involves the choice of respondents who are most advantageously placed or in the best position to provide the information required during the sampling process.

Using purposive sampling, the researcher invited 66 students from one University in the Philippines to test the system using Black Box Testing.Each student submitted 6 pictures to be used for their profile. The purpose of Black Box testing is to measure the accuracy of system's recognition process without regard to the inner workings of the system. Because the system is automated and primarily depend its output from a video source, the researcher employed Black Box's State Transition Testing to determine if the system conforms to the following rules and equivalent diagram as shown in Figure 3:

a. If the subject S1 has a record in the system, the subject should transition from unknown to recognized
b. If the subject S2 has no record in the system, the subject should remain unknown after the recognition process.

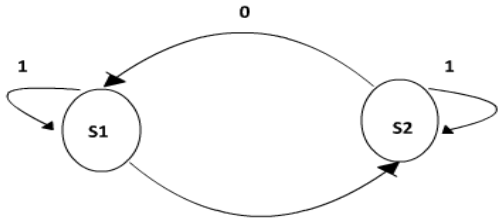

Figure 3.*State Transition of Respondents*

The students were requested to submit six (6) images with similar pose and expressions variations to serve as the referenced images during the matching process. After all the student profiles were encoded into the system, they were asked to walk through the camera and the researcher recorded how their state changes based on the aforementioned rules.

The accuracy of the system's recognition was measured using F-measure where:

a) True Positive refers to the number of samples positively or correctly identified by the system;
b) (b)False Positive are those wrongly identified as another person and
c) False Negative refers to the samples that have records in the system's database but are tagged by the system as unknown individual.

Table 1. *Scale used in Interpreting the Result of the F-measure*

Scale	Description
0.90 – 1.0	Excellent
0.80 – 0.90	Good
0.70 – 0.80	Fair
0.60 – 0.70	Poor
0.50 – 0.60	Fail

Table 1 shows the scale used in interpreting the result of F-Measure.

White Box Testing was likewise conducted to evaluate how the system processes the input to

generate the required output. More precisely, the functionality of the system was evaluated based on ISO/IEC 25010:2011 System and Software Engineering – Systems and Software Quality Requirements and Evaluation (SQuaRE).

Descriptive Statistics is used to describe the perception of the respondents towards the evaluation of the proposed system based on ISO 25010. Descriptive Statistics involves gathering data that describe events and then organizes, tabulates, depicts, and describes the data collection. [22].

The functional requirements of the system were evaluated by twelve (12) Information and Communications Technology (ICT) professionals from IloiloCity, Philippines. They are selected using purposive sampling and consist of System Analyst, System Developer, Software Engineer, Technical Support or Network Administrator. The choice of respondents only from these groups is based on the researcher's judgment as they are in best position to provide the information required in the study because they are expected to have reasonably gathered expert knowledge by virtue of their education and experience.

Likewise, 10 prospective end-users participated in the evaluation process which includes business owners, policeman, educators, and real estate broker and bank personnel.

Using a questionnaire, the respondents evaluated the system for functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability and portability. In each of this criterion, the respondents evaluated the system through the questionnaire using the scales in Table 2.

Table 2. Scale used by the respondents in evaluating the system

Scale	Description
4.50 – 5.0	Excellent
3.50 – 4.49	Very Satisfactory
2.50 – 3.49	Satisfactory
1.50 – 2.49	Good
1 – 1.49	Poor

RESULTS AND DISCUSSION

The accuracy of the recognition process of the proposed method was evaluated using F-measure and from the 66 randomly selected samples, the number of True Positive is 51 out of 66 or 77.27%, the False Positive is 11 or 16.67% and False Negative is minimal at 5 or 7.57%.

Precision is a measure of how precise the recall is [23]. The tests reveals that the system's precision rate 82.25% denoted as Good using the published threshold used by Hussain, and Saraswathi, [24]. This means that the proposed method is good in recognizing true positives or more precisely, system is able to recognize 82.25% of all the respondents.

Meanwhile, the system's Recall is 89.08% and denoted Excellent using the threshold published by Hussan and Saraswahi [24]. According to Moose [25] recall is the number of correct match found by the system. The result implies that the system is excellent in recognizing facial details within the image. This means that the system can recognize facial details of the respondents correctly in the captured images.

This research was evaluated based on ISO/IEC 25010:2011 System and Software Engineering – Systems and Software Quality Requirements and Evaluation (SQuaRE)- Systems and Software Quality Models. All eight (8) quality standards were used by both Information and Communication Technology (ICT) professionals and end user to evaluate the conformance of the application to the software standards set by ISO.

The results of the ISO 25010 evaluation are shown in Table 3. The Facial Recognition Using Segmented Facial Points for Intelligent Surveillance System was evaluated in terms of functional suitability, performance efficiency, compatibility, usability, reliability, security, maintainability, and portability. The grand mean as to the evaluation of the end users is 4.65 which is denoted as Excellent and the grand mean for the ICT experts is 4.69 which is also denoted as Excellent. The evaluation of the system as a whole has a mean rating of 4.67 which is denoted as Excellent.

According to ISO.org [26] there is a need for software to undergone evaluation for quality models which includes supporting specification and evaluation of software and software-intensive computer systems from different perspectives by those associated with their acquisition, requirements, development, use, evaluation, support, maintenance, quality assurance and control, and audit to establish its conformance to a set of standards. The results imply that Facial Recognition Using Segmented Facial Points for Intelligent Surveillance System meets the standards for specification and evaluation in terms of the acquisition requirements, development, use,

evaluation, support, maintenance, quality assurance and control, and audit.

The functional suitability characteristic of the system was evaluated and was given a mean rating of 4.57 which is denoted as excellent by the end users and a mean rating of 4.64 which is also denoted as excellent by the ICT experts. As a whole, the functional suitability characteristic of the system has a mean rating of 4.60 and is also denoted as excellent. This means that the system was able to meet the set of functions that covers the entire specified task and user objective, the system provides the correct results with the needed degree of precision and the system facilitate the accomplishment of specified task and objectives.

The Compatibility of the system is rated by the end user with a mean of 4.55 denoted as Excellent and the ICT experts rated the Compatibility of the system with the mean of 4.58 denoted as excellent. The grand mean for the system's Compatibility has a mean rating of 4.57 which is also denoted as excellent. According to Stark [27], the compatibility evaluation ensures that the system can be installed and can function on multiple environments and onlyneeds minimum computer specification to run the software. This means that the system can perform its required functions efficiently while sharing resources with other systems without detrimental impact on the product and the system can also exchange information with other system's components.

The performance efficiency of the system was rated by the end user with a mean of 4.60 denoted as Excellent and the ICT experts rated the performance efficiency of the system with the mean of 4.72 denoted as excellent. The grand mean for the system's performance efficiency has a mean rating of 4.66 which is denoted as excellent. The result of the system evaluation implies that the system response time and processing time is acceptable given that it needs to read the entire database in training data sets. This means that the system's response time, processing time and throughput rates meet the system requirements.

The evaluation of usability characteristic of the system shows that the system is easy to learn and use. The end users rated the system's usability (4.75) as excellent. The ICT experts rated the system's usability (4.74) as excellent. The overall evaluation shows that the respondents rated the usability of the system with the mean of 4.74.This means that the system is recognized by the user as appropriate for their needs, and enables the user to learn how to use the system efficiently. The system provides the user pleasing and satisfying interactive experience and the system allows the user to perform specified goals in a specified context of use.

The Reliability characteristic of the system was evaluated by the end user with the mean of 4.60 which is denoted as excellent. The ICT professionals rated the system with a mean of 4.56 which is denoted as excellent. The overall mean of the system's reliability is 4.58 which is denoted as excellent. This means that the system's component meets needs for reliability under normal operation. The system is operational and is accessible when required for use, the system operates as intended despite the hardware and software faults and the system can easily recover after a system fault. This result conforms to Jalote, Murphy, Garcia, and Errez [28] that said that system's reliability is shown when the system is failure free for a period of time under an environment and is capable to restore itself when a failure occurs.

The Security characteristic of the system was evaluated by the end user with the mean of 4.72 which is denoted as excellent. The ICT professionals rated the system with a mean of 4.77 which is denoted as excellent. The overall mean of the system's reliability is 4.74 which is denoted as excellent.This means that the system ensures that data are accessible only to those authorized to access the system.The system can prove that actions have taken place so that it cannot be repudiated later.

The result of the evaluation implies that the system was able to provide security measures to its client and data.The system was designed to have a user login to ensure that only authorized user can view and modify data within the system.The authorized person was given theprivilege to manage all the functionalities ofthe system as well as view logs, and recordings.

The Maintainability characteristic of the system was evaluated by the end user with the mean of 4.82 which is denoted as excellent. The ICT professionals rated the system (4.73) as excellent. The overall rating of the system's reliability (4.78) is considered excellent. This means that the system is composed of discrete components that a change to one component has minimal impact on other components. The system can use more than one resource, and the system can diagnose itself for deficiencies or causes of failures and identify parts to be modified.

Table 3. Summary of ISO Evaluation of Facial Recognition Using Segmented Facial Points for Intelligent Surveillance System

Characteristics	End Users		IT Experts		Entire Group	
	M	Description	M	Description	M	Description
Functional Suitability	4.57	Excellent	4.64	Excellent	4.60	Excellent
Performance Efficiency	4.60	Excellent	4.72	Excellent	4.66	Excellent
Compatibility	4.55	Excellent	4.58	Excellent	4.57	Excellent
Usability	4.75	Excellent	4.74	Excellent	4.74	Excellent
Reliability	4.60	Excellent	4.56	Excellent	4.58	Excellent
Security	4.72	Excellent	4.77	Excellent	4.74	Excellent
Maintainability	4.82	Excellent	4.73	Excellent	4.78	Excellent
Portability	4.63	Excellent	4.78	Excellent	4.70	Excellent
Grand Mean:	**4.65**	**Excellent**	**4.69**	**Excellent**	**4.67**	**Excellent**

Moreover, the system test criteria can be established for the system components and the tests can be performed to determine whether those criteria have been met.

The Portability characteristic of the system was evaluated by the end user with the mean of 4.63 which is denoted as excellent. The ICT professionals rated the system with a mean of 4.78 which is denoted as excellent. The overall mean of the system's reliability is 4.70 which is denoted as excellent. This means that the system can effectively and efficiently be adapted for different or evolving hardware, software or other operational or usage environments. The system can be successfully installed and/or uninstalled in a specified environment and the system can replace another specified software product for the same purpose in the same environment.

With a "Good" precision rate, the algorithm is able to discriminate facial features and identify 51 out of 66 respondents in the facial recognition aspect of the study. As a surveillance system, it was able to record and store surveillance videos by date and time for easy user viewing. It was able to send email and SMS notification to intended recipients. The system allows the user to manage the profile of people, extract image features and implement the algorithm to limit the feature-matching process within the confines of the facial segments. By having achieved the stated system requirements and expected output, the respondents rated the Facial Recognition Using Segmented Facial Points for Intelligent Surveillance System as excellent.

CONCLUSION AND RECOMMENDATION

Based on the results, the system has deemed to have met its specified requirements and objectives. This includes maintaining a database of personal profiles; classifying the personal profiles of the person; detecting and recognizing people within its covered area by matching the detected face with its existing database; logging the details of the recognition process; displaying the log entries and generating report; providing a scheduling system for monitoring intrusion in the covered area; and automatically sending notification to contact user for criminals detected on site if schedule to notify is enabled.Moreover, based on the perception of respondents from the Information and Communications Technology sector and potential end users the system is excellent in all the eight software quality characteristics as outlined by ISO 25010.

An enhanced method of SIFT-based face recognition system is proposed and based on logically dividing the human face into segments to shift the former algorithm from object-recognition to a more specific area matching.

Due to observations that were noted during the systems design process; the following recommendations are hereby presented to improve on the proposed study. A tracking system should be added in the video surveillance so as to constrain the system from processing the images that were identified on initial image frames. Further experiment of the most fitting value of the threshold for the cosine distance should also be made. Lastly, an enhancement of the segmented facial points algorithm should also be done to address issues on illumination change, pose and other distortions.

REFERENCES

[1] Da Cruz, G., (2015). The Importance of CCTV Security Systems in Business, from https://www.linkedin.com/pulse/importance-cctv-security-systems-business-gustavo-m-da-cruz

[2] Steffens, M., (2009). How Good are CCTV Cameras at Preventing Crime?, from http://www.abc.net.au/science/articles/2009/04/15/2543768.htm
[3] Corkill, J., (2014).When It Comes TO Monitoring, how can CCTV Help?, from townsvillelocksmith.com.au
[4] Lin, S., (2000). An Introduction to Face Recognition Technology, Informing Science Special Issues on Multimedia Informing Technologies, 3 (2), 1-7
[5] Yadan, O., (2014). How Does the Facial Recognition Technology Work?, from https://www.quora.com/How-does-the-facial-recognition-technology-work
[6] Yuille, A., Hallinan, P. & Cohen, D., (1992). Feature extraction from faces using deformable templates. International Journal of computer Vision, 8 (2), pp 99 - 111
[7] Fagertun, J., Gomez, D.,Ersbøll, B. & Larsen, R., (2005). "A face recognition algorithm based on multiple individual discriminative models", from https://pdfs.semanticscholar.org/ecbd/0c4c96010884b422478d1f7e318f52fb3509.pdf
[8] Wójcik, G., Gromaszek, K. & Junisbekov, M., (2016). Face Recognition: Issues, Methods, and Alternative Applications, from https://www.intechopen.com/books/face-recognition-semisupervised-classification-subspace-projection-and-evaluation-methods/face-recognition-issues-methods-and-alternative-applications
[9] De Marsico, M., (2014). Face Recognition in Adverse Conditions, IGI Global
[10] Bupe, C., (2015). What are some recent research directions in face analysis and recognition?, from https://www.quora.com/What-are-some-recent-research-directions-in-face-analysis-and-recognition
[11] Leutenegger S., Chli M. & Siegwart R. Y. (2011). BRISK: Binary robust invariant scalable keypoints. Computer Vision (ICCV), IEEE, pp. 2548-2555
[12] Ojala, T., Pietikäinen, M. & Harwood, D. (1996). A comparative study of texture measures with classification based on feature distributions. Pattern Recognit. 29(1), 51–59
[13] Albiol, A., Monzo, D.,Martin,A., & Sastre, J., (2008). "Face recognition using HOG–EBGM." Pattern Recognition Letters. 29 (10), pp. 1537-1543
[14] Nguyen, H.,Bai, L., & Linlin, S. (2009). "Local gabor binary pattern whitened pca: A novel approach for face recognition from single image per person." In Advances in Biometrics, pp. 269-278.
[15] Bay H. Ess A. Tuytelaars T. & Van Gool L.(2008). Speeded-up robust features (SURF), Computer vision and image understanding, 110, (3), pp. 346-359
[16] Lowe, D.(2004)."Distinctive Image Features from Scale-invariant Keypoints", International Journal of Computer Vision, 60, (20), pp. 91-110.
[17] Noone D. & Bergman, A., (2016). Facial recognition in controlled access areas utilizing electronic article surveillance (EAS) system, from http://www.google.com/patents/US9460598
[18] Bhavani K., Dhanaraj, V.,Siddesh, N., Ragav, V., & Uma, R. (2017). Real-time Face Detection and Recognition in Video Surveillance, International Research Journal of Engineering and Technology (IRJET), 4 (6),1562-1565
[19] Dennis, A., Wixom, B. & Roth, R., (2012). System Analysis and Design, 5th Ed., John Wiley & Sons, Inc.
[20] Dennis, A., Wixom, B., and Tegarden, D. (2005). Systems Analysis and Design with UML Version 2.0 An Object-Oriented Approach, 2nd Ed, John Wiley & Sons, Inc, 31.
[21] [21]William, L., (2006). Testing Overview and Black-Box Testing Techniques from agile.csc.ncsu.edu/SEMaterials/BlackBox.pdf
[22] The Association for Educational Communications and Technology., (2001). What Is Descriptive Research?, from http://www.aect.org/edtech/ed1/41/41-01.html
[23] Dandekar, N. (2017) What is the Difference Between Precision, Specificity and Accuracy. Retrieved on February 20, 2018 from www.quora.com/What-is-the-difference-between-Precision-Specificity-abd-Accuracy
[24] Hussain, C. and Saraswathi, B. (2017). Image Retrieval Using Graph Based Visual Saliency. International Research Journal of Engineering and Technology.4 (7).pp 658-666.
[25] Moose, A. (2013). What Does Recall Mean in Machine Learning. Retrieved on February 21, 2018 from stackoverflow.com/questions/14117997/what-does-recall-mean –in-machine-learning
[26] ISO.org., (2011). ISO/IEC 25010:2011, from www.iso.org/standard/35733.html
[27] Stark. M., (2014). What is Compatibility Testing, from www.ibeta.com/what-is-compatibility-testing/
[28] Jalote, P., Murphy, B., Garzia, M., and Errez., B. (2016). Measuring the Reliability of the Software Products, from www.microsoft.com/206/02