Security Surveillance and Intelligence Alerting System for Crime Control and Prevention Using Multiple Representations Approach (SSIASCPMRA)

OLOJIDO JOSEPH[1], ALUKO AUGUSTINE OLI[2], OLOGUNAGBA GRACE[3], OJAJUNI OLOWATOYIN JAMES[4], OLADIMEJI BANJI JULUS[5]
[1, 2, 3, 4, 5] *Rufus Giwa Polytechnic, Owo, Ondo State Nigeria*

Abstract- ***Policing and security surveillance of our environment as the world evolving is beyond sticking to the old traditional method of human monitoring and placing surveillance on our surroundings for security alertness. The two major challenging factor is securing an environment are the surveillance methodology and identification of a suspect or intruder. Effective human surveillance for 24 hours daily has proven non achievable over the year. Identification of an intruder or suspect by human has several limitations such as difficulty in memory management when data sets are in large number, wide error merging in comparism within objects of similar resemblance, low processing speed among others. Information technology based knowledge in assisting human in security surveillance will improve the watchman job. The development of a security surveillance and intelligence alerting system for crime control and prevention using multiple representations approach will solve several shortcomings of human method of security surveillance. Our model was developed to capture and recognize object in both digital and non-digital format, perform required security checks and alert the command center in real time. In the process of developing our system, active shape model, low level analysis model, motion base model, feature analysis model, constellation method, linear sub space method and statistical approach method were adopted while Djisktra's algorithm was considered to enhance real-time system performance due to multiple implementations of several complex algorithms involved. The use of PDA object analyzer, Microsoft Visual studio, MySQL database was used as developmental tools during implementation.***

Indexed Terms- ***PDA object analyzer. Algorithms, MySQL, Model, Biometrics.***

I. INTRODUCTION

Personal identification is since the earliest times, a felt issue and, at the same time, does not have a simple solution. Nowadays, it is becoming a very important social aspect and its importance enormously grew for security and policing of the society such as recognizing people who poses security threat to public places such as schools, banks, airports, recreational centres, and other public places in which terrorists or other criminals could access as soft spot and carry out their heinous acts[1]. In the quest to tackle identity related challenges, a quantum leap beyond the traditional identification system is required in human identity management. The use of password, smart card, contact based biometric factors such as finger print, footprint, palm print, and other means of identification of persons are considered static and easily lost. Nevertheless, password, smart card may be lost, stole, forgot or easily forged. On the other hand, an approach of biometric techniques for identification is not based on knowledge or possession but on biological characteristics and features such as: finger print, eyes lens, facial shapes, foot prints, voice wave patterns etc) and ways to do things such as: talk, write, move, etc,these characteristics could be considered unambiguous sincere they are nature inbuilt. Therefore, biometrics is the physiological and behavioral human characteristics, and it offers protection to the user from identity theft and manipulations [2]. The biometric systems few years ago are used only in specific environments with high security level but now, are much required in many sectors.

Moreover, the drastic costs reduction of these systems in the last years makes more interesting biometric technologies for businesses and education environment too. Biometrics has properties which could help in the identity proving, the identification process consists in associating a certain identity to a person. This identification can be positive or negative. In positive, the person to be identified declares her/his identity. In this case, the identification process must verify that claimed identity and person corresponds. This kind of identification is often called identification of one to one. In negative aspect, the identification process requires a comparison between the person to be identified and other persons in a database, in order to find his/her identity. This kind of identification is often called identification of one-to-many [3].

Using biometrics recognition techniques to solve the real time identity challenges attached to security surveillance in Nigeria higher institutions, government ministries, agencies, military base, among others has not gain much popularity. The major and popularly biometric used is finger print biometric identification system. The shortcomings of this system such as environmental and biological threat, human compromised among others is mitigating against safety of humans and materials. Hence, a twenty-four-hoursecurity surveillance and intelligence alerting system to aid crime control and prevention using multiple representation approach is needed Nigerian Institution of learning.

II. REVIEW OF EXISTING WORK

From a very young age, most humans recognize each other easily via familiar voice, face, ormanner of movement which helps to identify members of the family such as mother, father, or other caregivers and can give us comfort, comradeship, and safety. When we find ourselves among strangers, when we fail to recognize the individuals around us, we are more prone to caution and concern about our safety. This human faculty of recognizing others is not fool proof. We can be misled by similarities in appearance or manners of dressing, detecting differences between identical twins, among others. However, these mechanisms can sometimes lead to error. It also remains a way for members of small communities to identify one another [4]

Biometrics has been widely used for criminal investigations and prisoners control from long time. The first system based on biometrics was proposed by Alphonse Bertillon in 1882. It was based on anthropological measures which were used at the Leavenworth prison until 1903, when such system failed in distinguishing two twins, [5]. So far, many automatic identification systems based on biometrics have been proposed: in some case, the biometric technologies are notably improved from the first attempts and now they are very promising [6]. Recently, automated verification systems based on fingerprint or face acquisition has been installed in airports and banks. Although such systems actually serve as deterrent, because their performance is yet low, their “active” presence could be considered an important step for the diffusion and the increase of the interest around the biometrics.

[7] presented a Complex Derivative Filters, which uses Gaussian filter to remove the noise in the pre-processed facial images for high facial recognition accuracy. A convolution matrix produced by a Gaussian function is used to smooth the facial images. The limitation of their system is that it functions more effectively with images that are not more than 68 x 68 pixels. However, for images with larger pixels, complex derivative filters will not function well for facial recognition biometric identification.

[8] proposed a histogram equalization algorithm to mitigate the effect of lighting in facial pattern presentation. His algorithm was able to successfully replace the pixel values by using a function designed to spread the repartition of the histogram. His model was able to enhance the contrast of the detected facial images. The limitation of their model was the challenges of handling large amount of rows and columns for respective facial images.

[9] proposed the use of neural networks in the use of facial detection. The survey review presented the advantages of using neural networks solving many pattern recognition problems object recognition, and autonomous robot driving among others is the

feasibility of training a system to capture the complex class conditional density of face patterns. However, one demerit is that the network architecture has to be extensively tuned (number of layers, number of nodes, learningrates, etc.) to get exceptional performance.

[10]developed one of the earliest neural networks for face detection. Their network consists of layers with 1,024 input units, 256 units in the first hidden layer, eight units in the second hidden layer, and two output units. His system was able to present a model that gives multiple outputs as a result of it corresponding merging of biometric factors. The limitation to his model was that neural networks cannot be used with a data set minimum than 500 samples to avoid memorization.

Biometrics offers several advantages over traditional security measures[11] these include:

i. Non-repudiation: With token and password based approaches, the perpetrator can always deny committing the crime pleading that his/her password or ID was stolen or compromised even when confronted with an electronic audit trail. There is no way in which his claim can be verified effectively. This is known as the problem of deniability or of 'repudiation'. However, biometrics is indefinitely associated with a user and hence it cannot be lent or stolen making such repudiation infeasible;
ii. Accuracy and Security: Password based systems are prone to dictionary and brute force attacks. Furthermore, such systems are as vulnerable as their weakest password. On the other hand, biometric authentication requires the physical presence of the user and therefore cannot be circumvented through a dictionary or brute force style attack. Biometrics have also been shown to possess a higher bit strength compared to password based systems and are therefore inherently secure [6];
iii. Screening: In screening applications, we are interested in preventing the users from assuming multiple identities (e.g. a terrorist using multiple passports in entering various country). This requires that we ensure a person has not already enrolled under another assumed identity before adding his new record into the database. Such screening is not possible using traditional authentication mechanisms and biometrics provides the only available solution.

[12] the various biometric modalities can be broadly categorized as: -

a. Physical biometrics: these involve some form of physical measurement and include modalities such as face, fingerprints, iris-scans, hand geometry etc;
b. Behavioral biometrics: these are usually temporal in nature and involve measuring the way in which a user performs certain tasks. This includes modalities such as speech, signature, gait, keystroke dynamics etc;
c. Chemical biometrics: this is still a nascent field and involves measuring chemical cues, such as odor and the chemical composition of human perspiration.

III. RESEARCH OBJECTIVES

This research work focuses on solving security challenges in Nigeria Higher Institution of learning using multiple representations approachin keeping environmental surveillance.

IV. METHODS

Unlike the conventional ways of security surveillance using human personnel in monitoring environmental via the use of CCTV camera images, our security surveillance and intelligence alerting system will automatically capture images of events, analyse images and report the emergence of any flagged images of such persons or objects using multiple representations approach. In the process of developing this system, active shape model, Low level analysis model, Motion base model, Feature analysis model, Constellation method, Linear sub space method and statistical approach method were adopted while Djisktra's algorithm was considered to enhance real-time system performance due to multiple implementations of several complex algorithms involved as shown below.

1. Let T = {A, B, C, D, E, F} = number of nodes in the mapped area
2. S = source;
3. node = A;

4. N = set of nodes that have been processed so far;
5. K(i,j) = link distance from node i to node j if two nodes are directly connected
6. While ∞ if there is no link route between i and j
7. D (v) = route to the shortest path (shortest path) from node s to node v that is currently known so far.
8. When the algorithm terminates,

i. D(v) is the distance of the shortest path from source s to destination v in the mapped areas;
ii. P(v): predecessor node along path from source s to v, that is the nextv

4.1 SSIASCPMRA flowchart

Security surveillance and intelligence alerting system for crime control and prevention using multiple representations approach (SSIASCPMRA) was designed into two modules. The first part of SSIASCPMRA was implemented to allow security personnel capture the facial image of a crime suspect, therein flagged it as threat to such environment as shown in figure 1 below.

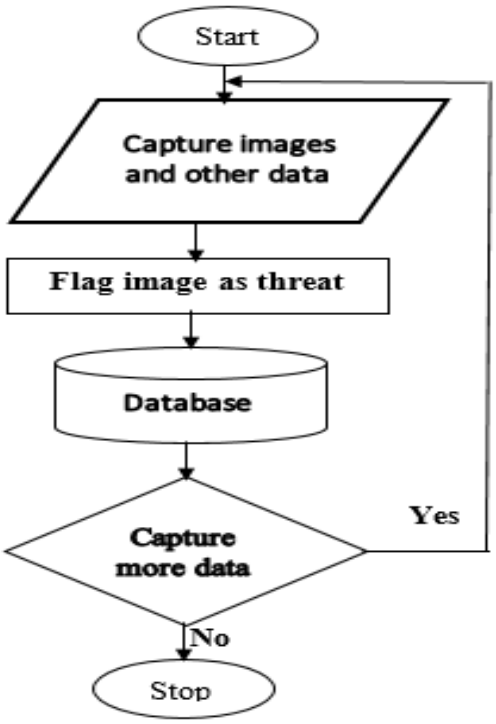

Figure (1) system registration flowchart

The second aspect of SSIASCPMRA was implemented as shown in figure 2 below. This aspect acquired images from the nodes (cameras) attached to the server system. The system captures all living images and analyze using various algorisms stated. The outcome of this process returns “1” to trigger alarming system for securities personnel for actions while if outcome is “0”, kill the process of comparing with such images. SSIASCPMRA has the capacity for individual node to send information for the server for processing and report such notes port connection respectively to determine the location of the image as show in figure 2 below

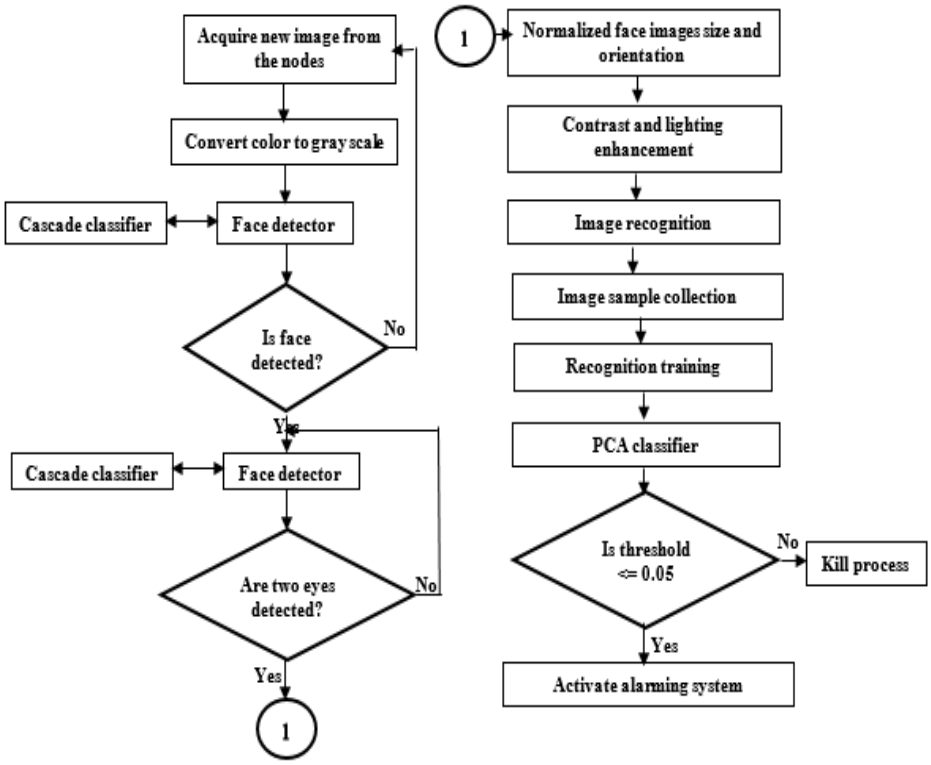

Figure (2) system surveillance system flowchart

V. RESULTS

Security surveillance and intelligence alerting system for crime control and prevention using multiple representations approach was tested on living and nonliving images. The system was able to capture, analyze and identify images flagged as threat and alerting relevant personnel by alarming such quarters. The sample space of 200 persons taking was all identified and alarm triggered within various lighting resolutions and distances. The location of each respective node were also identified via the system server port which was preregistered as location of sense for easy identification.

CONCLUSION

The population of human movement in and out of any higher institution of learning are in their thousands daily especially public owned institutions where admission enrolment is highly competitive. To monitor and secure such huge number of persons, beyond the traditional method of surveillance system is required. The use of a carefully selected information technology driven tools such as security surveillance and intelligence alerting system for crime control and prevention using multiple representations approach will provide the needed complement to human security personnel. Security surveillance and intelligence alerting system for crime control and prevention using multiple representations approach will inculcate the attitude of security consciousness into the mind of individuals in such an environment where this system is installed. It will also send a no go area signals to criminally mind persons for security safety and control.

REFERENCES

[1] Divyarajsinh N. P., and Brijesh B. M. (2014): Face Recognition Methods & Applications, Computer Technology & Applications, Vol 4 (1),84-86

[2] Tolba, A. S., El-Baz, A. H., and El-Harby, A. A. (2014): Face Recognition: A Literature Review, International Journal of Signal Processing Volume 2 Number 2

[3] Zhang, X., Gon-not, T. and Saniie, J. (2017): Real-Time Face Detection and Recognition in Complex Background. Journal of Signal and Information Processing, 8, 99-112.

[4] Kitili Jackson Mwendwa (2016) "Automated Attendance Machine Using Face Detection And Recognition". B.Sc. Project report submitted to the Electrical and Electronic Engineering department at the University of Nairobi 13/05/2016

[5] Elets News Network (ENN). (2019, August). Biometrics Expanding Horizons. Retrieved September 12, 2012, from http://egov.eletsonline.com/2012/04/biometrics-can-be-used-for-electronic-service-delivery

[6] Jea , T., Chavan, K., Govindaraju, V. and Schneider, J. K. (2004). Security and matching of partial finger print recognition systems. In Proceeding of SPIE, number 5404, pages 39–50, 2004.

[7] Reisert, M. and Burkhardt, H. (2008) Complex Derivative Filters. IEEE Transactions on Image Processing, 17, 2265-2274.

[8] Peddigari, V.R., Srinivasa, P. and Kumar, R. (2015) Enhanced ICA Based Face Recognition Using Histogram Equalization and Mirror Image Superposition. 2015 IEEE International Conference on Consumer Electronics, Las Vegas, 9-12 January 2015, 625-628.

[9] Sundararajan, K., and Woodard, D.,. (2018). Deep Learning for Biometrics: A Survey. ACM Computing Surveys. 51. 1-34. 10.1145/3190618.

[10] Sarkar, E., (2019). "Optimizing Facial Information Extraction and Processing using Convolutional Neural Networks" A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science in Data Science, Department of Computer Science, University of Bath.

[11] Sharath, C., Govindaraju, S., Pankanti, R., Bolle, N and Ratha, N. (2005). "Novel Approaches for Minutiae Verification in Fingerprint Images", Seventh IEEE Workshop on Applications of Computer Vision (WACV/MOTION'05)-Volume1, Breckenridge, CO, USA, 2005, pp. 111-116, doi@ 10.1109/ACVMOT. 2005.85

[12] Joseph, N. P., and Lynette I. M. (2010): Whither Biometrics Committee; National Research Council, National Academy of Sciences, National Academies Press, http://www.nap.edu/catalog.php?record_id=12720