Use of Biometric-Based Identification and Automated Visual Surveillance to Checkmate Terrorist Activities in Nigerian Tertiary Institutions

Zauwali Sabitu Paki, Abubakar Sani, Mansur Babagana

Abstract: The current security challenges being faced in Nigeria is of public concern. Our institutions of higher learning are the prime targets of terrorist as it is evident in recent years. Several methods are used by the terrorist to gain access to the institutions one of which is by identity fraud (claiming to be guanine students/staff of such schools possibly by presenting students'/staff ID cards). In this paper we propose a framework that combines the use of biometrics in user identification and visual surveillance to monitor activities in real-time fashion in our institutions. We also conducted a survey in some institutions in northern Nigeria that were ravaged by the terrorist attacks in the recent past. The survey revealed that majority were of the opinion computerised security measures could significantly improve security situation in their institution. Majority also expressed readiness to accept the proposed initiative. More than 81% expressed preference of fingerprint biometric to other biometrics (iris, retina etc.).

KEYWORDS: Access Control, Authentication, Biometrics, CCTV, Video Camera, Visual surveillance, security

1 Introduction

The rate of terrorist activities in Nigeria is on the increase in recent times. Attacks are being made on public places such as schools, markets, financial institutions, and places of worship. Our school campuses must provide reliable means of protection at entry and exit points [1]. It is clear to virtually all Nigerians that the traditional physical security measures are grossly inadequate in tackling insecurity in Nigeria. There is, therefore, the need for better strategies. The use of computer-based security strategy and other related technologies is a viable way of improving security of lives and property of citizenry. There is need for organisations, institutions and other financial settings to save guard their employees, customers and IT infrastructure [1].

To his end, we propose a strategy that marries biometrics and automated visual surveillance technologies. The biometric technology is intended to be used to authenticate individuals needing access to strategic places that are considered vulnerable to terrorist attacks. Automated visual surveillance on the other hand will be used to continuously monitor movements of people in those place vulnerable to attacks with view to spotting out persons perceived to be of suspicious movements so that efforts could be made to apprehend them before they execute their treacherous plan.

- *Zauwali Sabitu Paki, Department of Computer Science, Northwest University Kano – Nigeria. zauwalispaki@gmail.com*
- *Abubakar Sani, Department of Computer Science, Northwest University Kano – Nigeria. abuabakar_sani@yahoo.com*
- *Mansur Babagan, Department of Computer Science, Bayero University Kano – Nigeria. mbabagana.cs@buk.edu.ng*

2 Biometric Technology in Access Control

Biometrics, in recent time, is the automated way of identifying an individual using his/her physical or biological characteristics [2], [3], [4], [5]. The unique human features used for the purpose of personal identification are iris, retina, fingerprint and facial image [3], [6], [4]. A good example of this type of biometric system is the United States Visitor and Immigration Status Indicator and Technology (US-VISIT) program [3], [7], [2], [8]. This system had been installed in some airports of the United States of America (USA) and is used to verify the identity of people entering the country through ports of entry to help in apprehending criminals already in the watch list.

Biometric-based personal authentication can either be verification or identification. In the verification process, the claimed identity is normally compared with the already stored templates on records; that is, a one-to-one comparison is performed. This happens, mostly, when the person to be authenticated presents something such as smartcard on which his/her biometric data had been stored. The system then uses this feature to retrieve his/her records from database (i.e. one-to-one comparison is performed). If there is a match, access is granted, otherwise, access is denied. Identification, on the other side, performs exhaustive one-to-many comparison of the just collected user sample with the biometric templates stored in the database acquired during enrolment. Identification system receives only the biometric sample of the person being identified.

There are a lot of problems associated with the traditional

method of establishing personal identity. In this respect, [2] succinctly writes "Unfortunately, passports, keys, badges, tokens, and access cards can be lost, duplicated, stolen, forgotten, and passwords, secret codes, and personal identification number (PIN) can easily be forgotten, compromised, shared, or observed (p. 11065)." These problems have caused a lot of concern and fear and hence the need for effective, reliable and secure strategy to supplement/replace the traditional identification system. At the forefront is the biometric-based identification system [2]. Biometric-based personal identification is very promising alternative/supplement to conventional identification scheme nowadays and is being embraced the world over.

3 Automated Visual Surveillance

Visual surveillance is a way of placing event monitoring devices in some strategic locations in order to capture the ongoing activities. The use of closed circuit television (CCTV) has been widely employed [9] by many governments and financial institutions to help in ensuring safety and security of people. Countries such great Britain and United States of America have high number of CCTV cameras installed at strategic places for security purpose. CCTV basically comprises set of cameras for the purpose of capturing video streams of the activities taking place within their fields of views (FOVs). These video frames are transmitted to a central control location for display, storage, and analysis by assigned personnel [1], [10]. These video clips are stored on tapes. The major shortcoming of CCTV system is the need for a constant watching and analysing of the video frames by dedicated personnel [10], [1] which makes it very tedious for human to effectively watch a multi-channel display monitor for 24 hours. The limited number of personnel to watch the video clips also seriously affects the efficiency of the CCTV system [11]. Automated visual surveillance solves this problem by employing some advanced image processing techniques [11], [12]. These techniques make it possible for the system to determine whether and unwanted event occurs based on the video frames captured by the cameras and automatically initiates alarm so the necessary physical security measures could be taken.

4 Surveillance in Nigeria

Information Technology has the potentials to strengthen the Nigeria's security as noted by [16]. The predominant security strategy in Nigeria is the use of guards at strategic places to provide the needed secutity by checking the identity of people requesting access. With the increased security challenges in Nigeria, these guard people heve been provided with metal detector to scan people as they come to such places; only few places such as commercial banks and offices of top government functionaries employed the use of CCTV technology for surveillance purposes.

At the intitution's level, almost all the institutions that we conducted the survey either did not employ the use of computer based security measures such as CCTV or had been employed only in very few locations such as the administrative buildings where institution's leaders situtate. Theses devices were mostly poorly managed.

5 Architecture of the Proposed System

The proposed system comprises the fingerprint sensor, digital cameras, and central control server as depicted in Fig. 1 below.

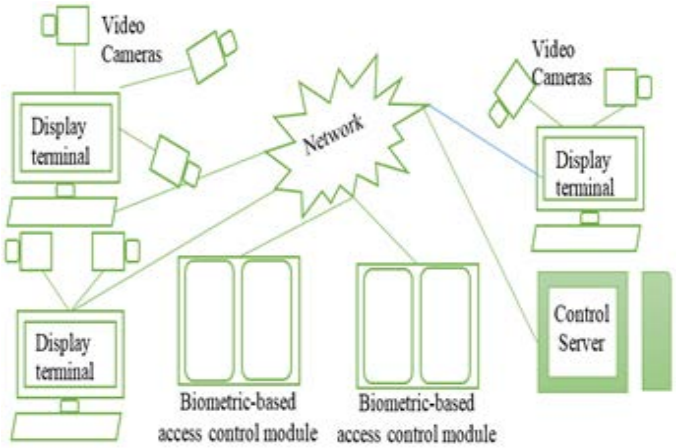

Fig. 1 Proposed System Outline

5.1 The Video Cameras

Digital video cameras will be installed at various locations to capture video frames of the ongoing events and send them to the appropriate display terminal and the central control server for analysis and eventual storage. As depicted in the figure, these cameras will be installed in as many locations as required depending on the places considered vulnerable to physical attacks by terrorist. The transmission of the videos captured by the cameras to the central control server will be through a local area network. A group of cameras will have a common display terminal located in a given security office and monitored by the security personnel.

5.2 The Display Terminal

The display terminal is a computer system, a PC or laptop, to which a given number of digital cameras are connected. The number of cameras to be attached to this system will depend on the size of the area to be covered. These terminals are installed at various security offices within an institution mostly located at various entry and exit points and at various strategic places. The security personnel within that office are responsible to their display terminal. These terminals are connected to a central server through a network through which they transmit their videos to the server for final analysis and backup storage.

5.3 Biometric-based Access Control Module

This module comprises the fingerprint scanning device and

electronic gate. Before this module could be used, the intended users of the system have to be enrolled into the system. The enrolment phase will acquire the biometric templates (fingerprint) of the users and store them in the biometric database for use during authentication phase. For physically challenged persons whose biometric templates were unavailable for capture during enrolment phase, special provision will be made to grant them access.

5.4 The Central Control Server

The central control server is a high end computer system that monitors and control the overall system. It is located at a secured location and serves as the central backup storage location for the videos captured by the various digital cameras and as biometric database. It will be under the control of the central security office.

5.5 The Network

The network will connect the various components of the system and it is a local area network (LAN). The reason for making it LAN is to avoid the burden of securing system data against unauthorised access.

6 User Perception on the Proposed System

Although In this section, we present the results of the survey we conducted in some of the institutions that were recently ravaged by the terrorist attacks. The respondents were either staff and/or student of those institutions. A total of 200 questionnaires were administered but 195 were successfully retrieved. 127 of the respondents were male and 74 were female. The following tables give summary of the survey's results.**Error! Not a valid link.Error! Not a valid link.Error! Not a valid link.**

Error! Not a valid link.Error! Not a valid link.

6.1 Discussion

The results of this survey revealed that respondents believed that the existing security measures were grossly inadequate and sought the need for improvement. From the results of this survey (tables 1 and 2), it is evident that a large percentage of the respondents were highly optimistic the security situation of their institution could be improved by complementing the existing measures with biometric based.

On the user acceptability of the system, it is worthy of note that 87.17949% were ready to accept the system while 12.82051% were unwilling to accept it (table 3).

However, majority of the respondents preferred fingerprints biometrics (table 5). This concurs with other researchers' results such as [13], [3], [6], [14], [15] that fingerprint biometrics is the most widely used and acceptable biometrics. Even though respondents were not asked reasons for preferring one biometrics over the others, preference of fingerprint over the rest could be attributed to convenience.

On the privacy issue, only 30.76923% did not fear the possibility of the system being a breach to their privacy especially the video surveillance aspect. There is, therefore, the need for proper user education before deploying the system to their working environment. This is very important because it largely determines the entire success of the system. If people mistrust the system its acceptability to them will drastically drop.

References

[1] S. Russo, *Digital video surveillance: Enhancing physical security with analytic capabilities*, IBM Global Services, 2008.

[2] W. Shen and T. Tan, "Automated biometrics-based personal identification," in *Proceeding of National Academy of Science USA*, 1999.

[3] S. C. Dass and A. K. Jain, "Fingerprint-based recognition," *Technometrics*, vol. 49, no. 3, pp. 262-276, 2007.

[4] M. G. Milon, "Biometric surveillance: Searching for identity," *The Business Lawyer*, vol. 57, no. 1, pp. 497-512, 2001.

[5] Y. Mei, H. Sun and D. Xia, "A gradient-based combined method for the computation of fingerprints' orientation field," *Image and Vision Computing*, vol. 27, pp. 1169-1177, 2009.

[6] M. El-Abed, R. Giot, B. Hemery and C. Rosenberger, "A study of users' acceptance of biometric system," 2010.

[7] J. Wayman, A. Jain, D. Maltoni and D. Maio, Biometric systems technology, design and performance evaluation, Springer, 2005.

[8] L. M. Vein, M. Baveja and B. H. Singer, "Using fingerprint image quality to improve the identification performance of the U.S. Visitor and Immigrant Status Indicator Technology program," in *Proceedings of the National Academy of Sciences of the United States of America*, 2005.

[9] H. U. Keval, "Effective, Design, Configuration, and Use of Digital CCTV (PhD Thesis)," University College London, London, 2009.

[10] Y. Nam, S. Rho and J. H. Park, "Intelligent video surveillance system: 3-tier context-aware surveillance system with metadata," *Multimed Tools Appl*, 2010.

[11] M. Shah, O. Javed and K. Shafique, "Automated visual surveillance in realistic scenarios," IEEE Computer Society, 2007.

[12] R. Vezzani, "Computer Vision for People Video Surveillance (PhD Thesis)," UNIVERSIT`A DEGLI STUDI DI MODENA E REGGIO EMILIA, 2008.

[13] J. Ashbourn, Practical biometric from aspiration to implementation, London: Springer, 2004.

[14] A. Ross and A. Jain, "Biometric sensor interoperability: A case study in fingerprints," in *Proceeding of International ECCV Workshop on Biometric Authentication*, Prague, 2004.

[15] A. M. Bazen, "Fingerprint identification - feature extraction, matching, and database search," PhD Thesis, University of Twente, 2002.

[16] P. M. Ogedebe and B. P. Jacob, "The Role of Information Technology In Combating Security Challenges In Nigeria," *Academic Research International*, vol. 2, no. 1, pp. 124-130, January 2012.