Research Paper

Fingerprint Biometrics-Enabled Database: A Collaborative Crime Information System

Emmanuel, Victoria Nkemjika[1], Victor Chibunna Enyinnaya[2]

[1]Department of Computer Science, Imo State University, Nigeria
[2]Department of Computer Science, Abia State College of Health Sciences and Management technology Aba,
Abia State, Nigeria

ABSTRACT

The widespread use of information technologies in our society today has resulted in considerable improvements in a variety of sectors, including our people's security standards. Criminal activity is a threat to the economy, politics, and social order. According to current evidence, Nigerian security services have separate systems that prevent them from cooperating effectively to combat crime. This paper developed a finger biometrics enabled database: a collaborative tool crime information system to improve security operations and capability on crime management. The modelwas developed usingObject-oriented hypermedia design methodology and the object-oriented analysis and design methodology were adopted in the system analysis using unified modeling language tools. A mobile phone emulator was also designed for crime reporting. PHP, HTML5, CSS, JavaScript, AJAX and Web 2.0 technologies were used to implement the system. A soft token that acts as a one-time password for security was used as a second-level authentication. The biometric enabled database for crime informationsystem implemented enhances the productivity of security agencies and increases society's security standard.

KEYWORDS: *Fingerprint biometrics, integrated system, model, crime, Databases, and Information system.*

I.   INTRODUCTION

Fingerprint databases are organized collections of fingerprint information that are mostly used for evaluation or operational recognition. Raw fingerprint images acquired with live-scan sensors or digitized from inked fingerprint impressions on paper are usually detached from the identities of the corresponding individuals, are publicly available for research purposes, and consist of raw fingerprint images acquired with live-scan sensors or digitized from inked fingerprint impressions on paper in databases for evaluation. These datasets serve as the foundation for research in automatic fingerprint identification, as well as a variety of technology assessments and benchmarks when combined with appropriate experimental protocols. This is the type of fingerprint database that will be developed further in this article. System integration aims to reduce a solution's overall operating costs rather than just specific parts of it. Furthermore, the system integrator is responsible for guaranteeing critical stability and security. In all of this, the ability to constantly develop the solution as a whole should be considered. The widespread use of information and web technologies in our society today has resulted in considerable improvements in a variety of sectors, including our people's security standards (Appel and Abrahamson, 2017).

Crime is a major element connected with underdevelopment and a threat to a nation's economic, political, and social security. It deters both domestic and foreign investment, slows development, and lowers the quality of life (Anthony, 2013). As a result, the global prevalence of crime necessitates immediate attention, and the degree of crime control and prevention in each society is dependent on the effectiveness of law enforcement agencies' operations (LEAs) (Bukar, 2006). LEAs are required by law to provide public-safety, defend public property and facilities, maintain order, and protect public authorities (Yunus, 2015). Security of life, property, and welfare of the citizens are the most primary duties of governments and therefore deserve top priority attention (Tafa, 2006). An integrated system is an essential tool for every government to effectively combat crime by allowing agencies to collaborate (Law enforcement, 2017). The goal of this research is to create a biometric-enabled database for law enforcement organizations that work together.

Detection and capture

The most important phase in an automated fingerprint authentication system is fingerprint image capture since it defines the final fingerprint image quality, which has a significant impact on overall system performance. There are a variety of fingerprint scanners on the market, but they all work by measuring the physical difference between ridges and valleys.Solid-state fingerprint readers and optical fingerprint readers are the two major groups of proposed methods. The technique for collecting a fingerprint with a sensor is rolling or contacting the finger onto a sensing area, which captures the difference between valleys and ridges based on the physical principle in use (optical, ultrasonic, capacitive, or thermal). The elastic skin deforms when a finger contacts or rolls across a surface. The amount and direction of pressure applied by the user, as well as the user's skin conditions

II. DATABASES OF FINGERPRINTS FOR EVALUATION

Because of its permanence and uniqueness, fingerprint recognition is the most widely used biometric technique in personal identification. Fingerprints are rapidly being employed in a variety of convenience applications, such as access control and online identity, in addition to forensic investigations. The field's expansion over the last two decades has resulted in the emergence of an increasing number of biometric databases for study and assessment, either monomodal (sensing only one biometric characteristic) or multimodal (sensing many biometric traits) (two or more biometric traits sensed). The NIST databases were the only big, publicly available datasets before the databases were gathered as part of the International Fingerprint Verification Competition series. These databases, on the other hand, were not well suited for evaluating algorithms that operate with live-scan images and will not be discussed here. The authors present some of the most important findings in this section.

III. METHODOLOGY

Integration standard

The International Organization for Standardization (ISO) defines a standard as a document authorized by a recognized entity that specifies rules, norms, or characteristics for products, processes, or services for which compliance is not required. Standards should be implemented to promote electronic information sharing between heterogeneous security agencies systems at all levels to develop an integrated system, and this is typically developed at the national level. Justice agencies with different systems can't readily develop or alter their systems to share data if there aren't any standards in place. It should give authorities the tools they need to create systems that can easily share data with other security agencies. The norm must also be regulated to ensure uniformity. The most commonly accepted standard for data transmission between heterogeneous systems is the Extensible Markup Language (XML). Currently, all major database software providers (IBM, Oracle, Microsoft, and Sybase) have made significant investments in making their software fully XML compliant (Prisoc, 2003). The communication protocol used in this project was simple object access protocol (SOAP) and the data format was XML (Indika, 2011). While XML is a data and text encoding/transfer standard, SOAP is a communication protocol that allows programs running on different operating systems to communicate utilizing the hypertext transfer protocol and its XML. SOAP is an XML-based communication protocol (Nwaeze, 2010).

3.2. Research Approach

The study used a quantitative research approach (crime statistics in ICIS databases e.g. number of crimes reported, handled, etc.). As a communication protocol, the conceptual model was created utilizing a basic object access protocol. The collaboration approach for the six agencies (Police, Immigration, DSS, EFCC, ICPC, and NCDC) was designed using a hybrid of distributed and centralized architectural technologies, and a middleware facilitated information exchange in the dispersed systems. Data was exchanged using the Hypertext Transfer Protocol (HTTP) and XML web services. The researcher visited some of these agencies during the analysis stage for information gathering. The performance of this developed system was evaluated (Ugwuishiwu*et al.*, 2017) and in terms of average-case response time, a comparison was made between the previous system and the new system (average time needed for an arrived case to be handled). The analysis was conducted using the object-oriented analysis and design methodology and the unified modeling language tool. The Integrated portal for Nigeria agencies was built using PHP, HTML5, CSS, JavaScript, AJAX, and Web 2.0 technologies. MySQL was used to create and manage the database, which included several tables. As a second-level authentication, a one-time password security token was used to grant access to the correct user. Biometric technology was utilized to authenticate criminals.

IV. SYSTEM DESIGN AND IMPLEMENTATION
4.1 Objectives of the New System

The system will provide a fingerprint biometrics-enabled database for law enforcement agencies by the following;

a.   To provide a more accurate means of accessing timely information by security agencies and users.
b.   To provide a simplified, newer and safer method or mode of operation.
c.   To effectively provide a secured platform.
d.   Accuracy in the handling of data.
e.   Fast rate of operation and excellent responses time
f.   Flexibility (i.e.) it can be accessed at any time.
g.   Better storage and fast retrieval system.

4.2 Program Menu

Its function is to define the system's full functionality, determine the performance requirements, and initiate tradeoffs and basic designs to assign functions to the various hardware and software disciplines. It is the responsibility of the specification to supply those needs as well as to initiate the partitioning of hardware and software, as well as implementation schedules. The modules on the Nigeria Security Agency system are found on the main menu. Each module is divided into two classes: system administrators and users. The system's access is controlled by the user's password, which now dictates what the user can do on the system.
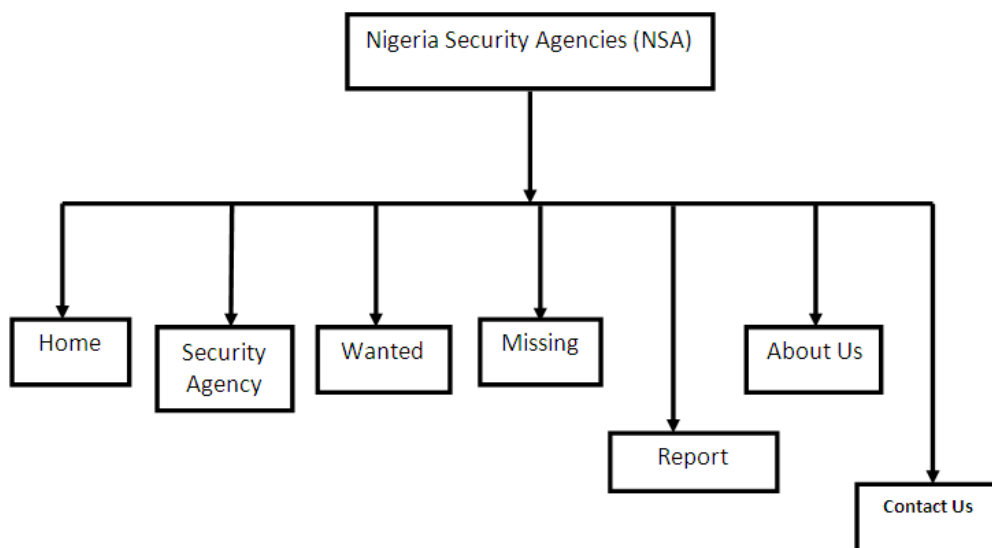

Figure 4.1 Main Menu

4.3 Submenus/Subsystems

The Nigeria Security Agencies System was divided into subsystems. It was designed using a Top-Down Approach. The system is structured in a way that each subsystem is accessed from the main menu and executed independently. The sub-menus/subsystems are as follows:

4.3.1 Home Sub System

This subsystem, as shown in Fig. 3.15, is the user's first point of contact while utilizing the software. It gives the user or the administrator access to the login forms. The subsystem system also includes information about the application's developer as well as an exit button for departing the system.
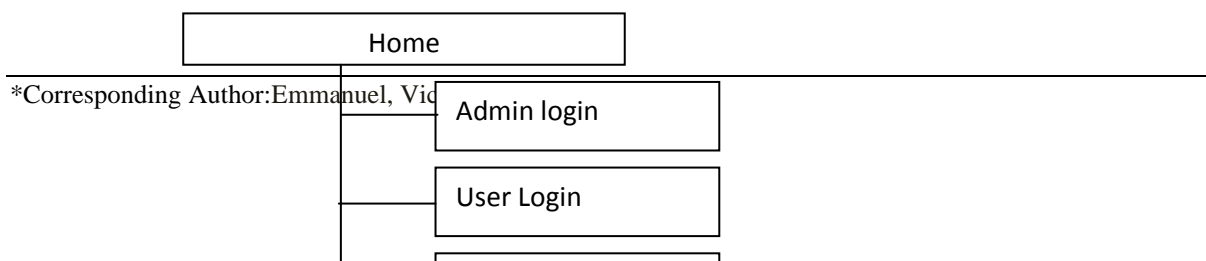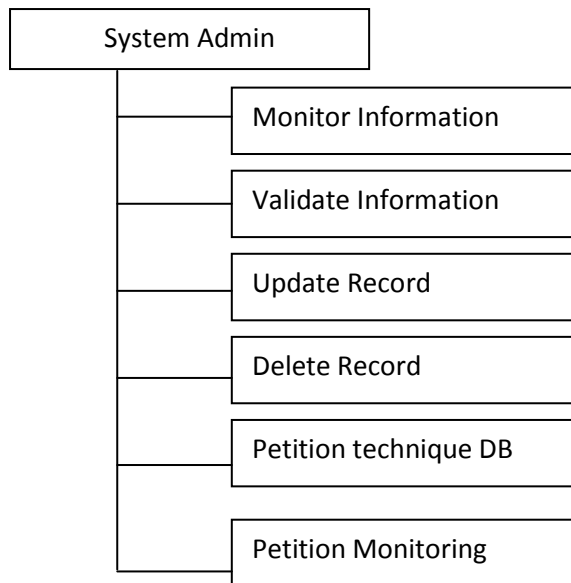
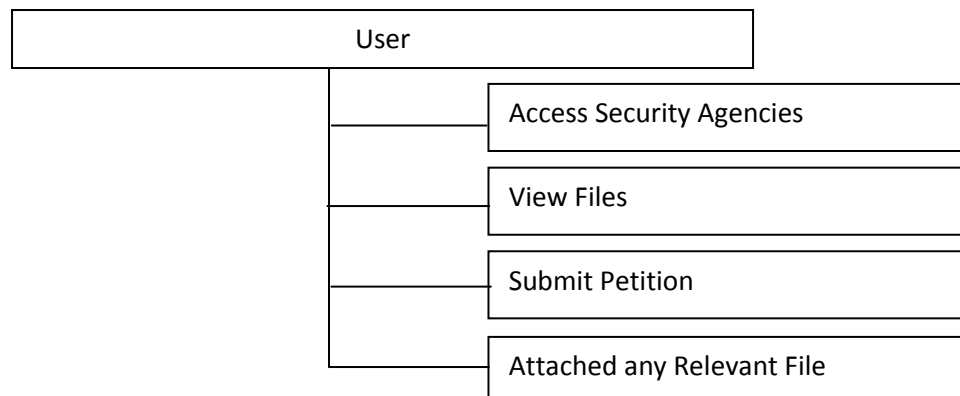**Figure 4.2: Homepage Sub System Design**

4.3.2Admin Sub System
Figure 3.16 which is the admin subsystem is accessible by the system administrator. The administrator has full control over this module's operations. Users have access control and can monitor information/petition, validate information, amend and remove records.

```
┌─────────────────────┐
│   System Admin      │
└─────┬───────────────┘
      │   ┌─────────────────────────────┐
      ├───│   Monitor Information       │
      │   └─────────────────────────────┘
      │   ┌─────────────────────────────┐
      ├───│   Validate Information      │
      │   └─────────────────────────────┘
      │   ┌─────────────────────────────┐
      ├───│   Update Record             │
      │   └─────────────────────────────┘
      │   ┌─────────────────────────────┐
      ├───│   Delete Record             │
      │   └─────────────────────────────┘
      │   ┌─────────────────────────────┐
      ├───│   Petition technique DB     │
      │   └─────────────────────────────┘
      │   ┌─────────────────────────────┐
      └───│   Petition Monitoring       │
          └─────────────────────────────┘
```

Figure 4.3: System Admin subsystem

User Sub System
The user sub-system as shown in Fig 3.17 allows the user to access the portal, view files, and submit a petition.

```
┌─────────────────────────────────────┐
│              User                   │
└─────┬───────────────────────────────┘
      │   ┌─────────────────────────────┐
      ├───│   Access Security Agencies  │
      │   └─────────────────────────────┘
      │   ┌─────────────────────────────┐
      ├───│   View Files                │
      │   └─────────────────────────────┘
      │   ┌─────────────────────────────┐
      ├───│   Submit Petition           │
      │   └─────────────────────────────┘
      │   ┌─────────────────────────────┐
      └───│   Attached any Relevant File│
          └─────────────────────────────┘
```

Figure 4.4: User Sub System

V.   CONCLUSION

Following the investigation and analysis of the many issues encountered by some of the most well-known existing security systems, a new model for information distribution was offered as a way forward for effective and strengthened national security. The suggested system was built to address the flaws of the existing system and to provide more value to security administrators, with the goal of decreasing their stress by providing quick access to information that will aid in the arrest of lawbreakers. The various steps involved in the manufacturing of the software product were carried out using object-oriented analysis and design methodology. In a single automated platform, numerous agents doing diverse activities were integrated with other functional modules. A series of functional tests were performed on the proposed portal to see if the system matched its initial aims and design goals, and the findings show that it did meets its objectives.

The Fingerprint Biometric-enabled Database for Integrated Law Enforcement Agencies is critical in maintaining the nation's security standard through crime control. However, existing crime information systems captured manually by the Nigeria Immigration Service (NIS), Nigeria Security and Civil Defense Corps (NSCDC), Nigeria Police, Independent Corrupt Practices Commission (ICPC), DSS, and Economic and Financial Crimes Commission (EFCC) lack integration for collaboration between agencies and the general public. Using a hybrid of distributed and centralized architectural technology, this article planned and created an integrated crime information system. The goal of the paper was to create an integrated system that would allow agencies to collaborate, have fast access to the relevant information, and share electronic criminal information for effective crime management. Individual agencies might have control over their data while also sharing it in a centralized repository using this hybrid approach. The designed integrated system allows the public to report crime cases through a portal, allowing for agency coordination, crime information exchange, and seamless crime case management for more effective Law Enforcement Agencies (LEAs) operations. For the LEAs, a consolidated repository including all crime data generated by the collaborating agencies was developed. To attain this goal, technological innovation would be required as a catalyst for significant changes in the police and other criminal justice practitioners' activities in Nigeria (Kent, 2001).

REFERENCES

[1]. Altameem, A. A., Aldrees A. I. and Alsaeed, N. A. (2014). "Strategic Information Systems Planning (SISP)", *World Congress on Engineering and Computer Science*, pp. 22-24.

[2]. Anthony, I. A. (2013). Social Factors Affecting Effective Crime Prevention and Control in Nigeria. International Journal of Applied Sociology: 3(4),71-72.

[3]. Appel, J., Abrahamson, D.: The Role of State Law Enforcement (2017). [Online]. Available: http://www.safeaccessnow.org/the_role_of_st

[4]. Bukar, M. (2006). The Role of Law Enforcement Agencies In The Promotion And Sustainability Of Participatory Democracy And Rule Of Law 1. [Online]. Available: http://mafng.org/symposium1/role_law_enforcement_agencies.pdf(Current Dec. 2017)

[5]. Cappelli, R., Maio, D., Maltoni, D., Wayman, J.L., Jain, A.K. (2006). Performance evaluation of fingerprint verification systems. IEEE Trans. Pattern Anal. Mach. Intell. 28, 3–18

[6]. Emmanuel, V. N. (2021). Development of Integrated Portal for Nigeria Security Agencies. Ph.D. Thesis, Imo State University, Owerri, Imo State.

[7]. Emmanuel, V. N., Chukwudebe G. A., and Agbakwuru, O. A (2019). Development of an Integrated Portal for Nigeria Security Agencies. *International Journal of Advanced Research in Science, Engineering, and Technology*. **Vol. 6,** 9978 - 9981

[8]. Indika: Difference between XML and SOAP (2011). [Online]. Available: http://www.differencebetween.com/difference-between-xml-and-vs-soap/(Current Dec. 2017)

[9]. Kent, R. Use of Information Technology by Law Enforcement (2001). [Online]. Available:www.sas.upenn.edu/jerrylee/programs/fjc/paper_dec01.pdf (Current Dec.2012)

[10]. Law Enforcement Article: What are the responsibilities of a law enforcement officer? pp1 (2012). [Online]. Available: http://www.lawenforcement.com/article/5735937--What-are-the-responsibilities-of-a-law-enforcement-officer/ (Current Dec. 2017)

[11]. Maltoni, D., Maio, D., Jain, A., and Prabhakar, S. (2003) Handbook of Fingerprint Recognition. Springer, New York

[12]. NIST Special Databases and Software from the Image Group, http://www.itl.nist.gov/iad/894.03/databases/defs/dbases.html

[13]. Nwaeze, R. I.: Vigilantism and Crime Control in Contemporary Nigeria: A Study of Udenu Local Gov. Area of Enugu State. M.sc. Thesis, university of Nigeria, Nsukka(2010). [Online]. Available: Http://repository.unn.edu.ng:8080/jspui/bitstream/123456789/703/1/richard's%20project.pdf(Current Oct, 2016)

[14]. Prisoc, S.: Justice Systems Integration: A Definition (2001). [Online]. Available: http://www.icjia.state.il.us/iijis/public/pdf/WP/iijis_defined.pdf (Current April 2016)

[15]. Tafa, A.: National Summit on Crime and Policing in Nigeria with the Network on Police Reform on Nigeria (Noprin) (2006). [Online]. Available: http://www.noprin.org/index.html APRIL 26-29(Current March 2013)

[16]. Ugwuishiwu, C. H, Okoronkwo M. C. and Asogwa C. N., (2017). "Performance Evaluation of Law Enforcement Agency on Crime Information Management Using QNM". A Journal published in International Journal of Physical Sciences, Vol. 12(4).

[17]. Yunus, U. U. S.: Nigeria: The Role of Law Enforcement Agencies in Developing New Mechanism in the Fight Against Corruption (2015). [Online]. Available: http://allafrica.com/stories/201506300436.html(Current March 2015)