IJSGS

FEDERAL UNIVERSITY
GUSAU-NIGERIA

INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL SUSTAINABILITY

The Use of Facial Identification in Bank Verification Number (BVN) System in Nigeria

Abubakar Usman Mohd*, Mansur Mohammed

Department of Mathematical Science Federal University Gusau

Corresponding author: absadiq_2@yahoo.com.

Received: November 2015 Revised and Accepted: December 2015

Abstract

This paper is aimed at itemising the limitations attached to the system of bank verification number (BVN) in the banking sector of Nigeria, and a perfect solution was designed to alleviate the short comings by introducing facial recognition in to the system.

Keywords: *Bank, Verification Number, Facial Recognition System, Challenges, Solutions*.

1.0 INRODUTION

With the increasing incidents of compromise on conventional security systems (i.e password and PIN), there is a high demand for greater security for access to sensitive or personal information in the Banking System of Nigeria. In recent times, biometric technologies have been used to analyze human characteristics as an enhanced form of authentication for real-time security processes. The Central Bank of Nigeria through the Bankers' Committee and in collaboration with all Banks in Nigeria on February 14, 2014 launched a centralized biometric identification system for the banking industry tagged Bank Verification Number (BVN). Biometrics refers to identifying an individual based on physiological or behavioural attributes – fingerprint, signature etc. Bank Verification Number, BVN, is part of the Central Bank of Nigeria, CBN's, cashless policy to capture customers' data and check fraud in the banking system. It is an initiative of the CBN to give every customer in the Nigerian banking system a unique identification number that can be verified across all banks in Nigeria. (BVN, 2015).

1.1 Objectives of the study

The objectives of the study are to:

1) Provide a unique identity that can be verified across the Nigerian Banking Industry (not peculiar to one Bank) through facial Identity.

2) Fully protect Customers Bank Accounts from unauthorized access.

3) Address issues of identity theft, thus reduce exposure to fraud

4) Reduce queue in Banking Halls during BVN enrolment

1.2 RESEARCH QUESTIONS

The present BVN system uses fingerprint as a means of identification in running analysis.

a) What if an individual hand is amputated, it means the bank cannot run analysis on that individual.
b) The second case if in case by accident an individual that already enrolled has surgery, the authentication may not work on such an individual.

c) The people in remote areas like peasant farmers, the finger print scanner hardly recognise their finger prints because of the nature of their work.
d) When it comes to women that uses Rani for fashion in their hands, which can take long period before it fade the scanner cannot detect their finger prints. But with facial recognition system all these drawback would be eliminated.

2.0 THE BANKING SYSTEM

Banks and other depository institutions channel funds from depositors to borrowers. In conducting these intermediation activities, banks also produce services, such as the processing of checks or electronic funds transfers, bookkeeping, protection of deposited funds, and investment services. Payment for these services may involve explicit charges or they may take the form of implicit charges--if the banks pay depositors lower rates of interest than they would otherwise earn on these funds. By paying lower rates of interest on deposits than they receive on loans, banks can cover their expenses and earn a profit, yet avoid charging for each service provided. In the national accounts, a service charge is imputed for the services that banks furnish without payment in order to provide a meaningful measure of their value added and gross output as well as to keep gross domestic product (GDP) invariant to whether banking services involve an explicit or implicit service charge (Brent, 2015).

2.1 System Analysis of BVN

The method of collection and analysing facts in respect of any method of operation procedures prevailing, so that an automated method could be design and implemented if proved feasible. (Dennis, 2012)

2.1.1 Unique features Of BVN Enrolment process

i. A unique ID number shall be issued to every Bank customer at enrolment and linked to every account that the customer has in ALL Nigerian Banks.

ii. Individuals shall be required to submit an acceptable means of identification as prescribed for enrolment.

iii. Customers of banks shall be required to enrol within a fixed period after which they shall no longer be able to operate their Bank accounts.

iv. Capturing of all ten (10) fingers and facial image will be adopted.

v. For authentication purposes, individuals performing banking transactions (e.g applying for loans) shall be required to identify themselves using their biometric features which will be matched against information in the central database.

vi. Update of customer information shall be done at their Bank Branches physically.

vii. Banks shall be prompted during account opening and credit check if a customer has been blacklisted by ANY Nigerian Bank.

viii. The BVN and unique features of an individual shall be used in conjunction with a PIN on a point of transaction.

2.1.2 BVN SYSTEM PROCEDURE

The customers are provided with instruction to comply with the following guidelines.

1. The enrolment process for acquiring your BVN is simple.

2. Visit any branch of the bank you have an account with. Registration by proxy not acceptable.

3. Collect and fill the BVN enrolment form with all personal data about you.

4. Submit the completed form to a designated official at your bank, who would then transfer the information given into a computer data base.

5. The official will take your photograph and finger prints.

6. You will sign your signature that will be captured electronically into the data system.

7. A small temporary registration acknowledgement slip will be issued to you, followed by an email or SMS conveying a similar information.

8. A BVN identification card with a computer chip bearing your embedded personal information will be issued to you for collection at your designated bank branch.

9. BVN registration exercise is mandatory for all individual customers.

10. Registration must be completed on or before June 30, 2015.

11. After deadline, you may not be able to do any financial transaction in any bank in the Nigerian banking system as you will require your fingerprint for authentication.

12. BVN registration is for individual account holders for the meantime till further notice.

13. Registration in one bank covers all accounts the individual might have in all other banks.

2.2 Biometric verification

Biometric verification is any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits. Unique identifiers include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures. The oldest form of biometric verification is fingerprinting. Historians have found examples of thumbprints being used as a means of unique identification on clay seals in ancient China. Biometrics is the measurement and statistical analysis of people's physical and behavioural characteristics. The technology is mainly used for identification and access control, or for identifying individuals that are under surveillance. The basic premise of biometric authentication is that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioural traits. The term "biometrics" is derived from the Greek words "bio" meaning life and "metric" meaning to measure. Biometric verification has advanced considerably with the advent of computerized databases and the digitization of analog data, allowing for almost instantaneous personal identification (Tech Target, 2008).

Iris-pattern and retina-pattern authentication methods are already employed in some bank automatic teller

machines. Voice waveform recognition, a method of verification that has been used for many years with tape recordings in telephone wiretaps, is now being used for access to proprietary databanks in research facilities. Facial-recognition technology has been used by law enforcement to pick out individuals in large crowds with considerable reliability. Hand geometry is being used in industry to provide physical access to buildings. Earlobe geometry has been used to disprove the identity of individuals who claim to be someone they are not (identity theft). Signature comparison is not as reliable, all by itself, as the other biometric verification methods but offers an extra layer of verification when used in conjunction with one or more other methods (Tech Target, 2008). No matter what biometric methodology is used, the identification verification process remains the same. A record of a person's unique characteristic is captured and kept in a database. Later on, when identification verification is required, a new record is captured and compared with the previous record in the database. If the data in the new record matches that in the database record, the person's identity is confirmed.

There are two main types of biometric identifiers:

1. Physiological characteristics: The shape or composition of the body.

2. Behavioural characteristics: The behaviour of a person.

Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odour. Behavioural characteristics are related to the pattern of the behaviour of a person, such as typing rhythm, gait, gestures and voice. Certain biometric identifiers, such as monitoring keystrokes or gait in real time, can be used to provide continuous authentication instead of a single one-off authentication check (TechTarget , 2008).

Other areas that are being explored in the quest to improve biometric authentication include brainwave signals, electronic tattoos, and a password pill that contains a microchip powered by the acid present in the stomach. Once swallowed, it creates a unique ID radio signal that can be sensed from outside the skin, turning the entire body into a password. (Tech Target, 2008).

2.2.1 OTHER FEATURES OF BIOMETRIC VERIFICATION

Authentication by biometric verification is becoming increasingly common in corporate and public security systems, consumer electronics, and point-of-sale applications. In addition to security, the driving force behind biometric verification has been convenience, as there are no passwords to remember or security tokens to carry. Measuring someone’s gait doesn’t even require a contact with the person.Biometric devices, such as fingerprint readers, digital cameras, consist of:

- A reader or scanning device.
- Software that converts the scanned information into digital form and compares match points.
- A database that stores the biometric data for comparison.

2.2.2 ACCURACY OF BIOMETRICS

The accuracy and cost of readers has until recently been a limiting factor in the adoption of biometric authentication solutions but the presence of high quality cameras, microphones, and fingerprint readers in many of today's mobile devices means biometrics is likely to become a considerably more common method of authenticating users, particularly as the new FIDO specification means that two-factor authentication using biometrics is finally becoming cost effective and in a position to be rolled out to the consumer market (TechTarget , 2008).

The quality of biometric readers is improving all the time, but they can still produce false negatives and false positives. One problem with fingerprints is that people inadvertently leave their fingerprints on many surfaces they touch, and it's fairly easy to copy them and create a replica in silicone. People also leave DNA everywhere they go and someone's voice is also easily captured. Dynamic biometrics like gestures and facial expressions can change, but they can be captured by HD cameras and copied. Also, whatever biometric is being measured, if the measurement data is exposed at any point during the authentication process, there is always the possibility it can be intercepted. This is a big problem, as people can't change their physical attributes as they can a password. While limitations in biometric authentication schemes are real, biometrics is a great improvement over passwords as a means of authenticating an individual (TechTarget , 2008).

Like any authentication data, biometric information needs to be protected against identity theft. However, not all biometric technologies are architected or handled the same way. In the example of an iPhone, the biometric information is encrypted and stored locally on the phone, so an organization isn't required to store the biometric information to authenticate the user. Therefore, in the case of the iPhone, an attacker would have to obtain the actual device -- rather than your fingerprint scan -- to make fraudulent purchases.

Biometric technologies include more than just fingerprint readers. Face and voice recognition are also becoming popular. The good news is, just like the iPhone fingerprint reader, the biometric authentication systems are moving toward locally stored and encrypted architectures for biometric data, making it unlikely that there would be a biometric database to be hacked. In addition, frameworks like the FIDO Alliance Universal Authentication Framework (UAF) are being rolled out to support local biometric validations. With that said, until the security industry more fully adopts UAF, organizations need to continue to protect any biometric information they collect. Fortunately, like standard password storage, biometric storage methods normally use strong encryption hashes to obfuscate the information. However, to date there aren't any security standards that address minimum encryption hashes for biometric information protection, so it would be wise to ensure any selected vendor supports a well-known, strong hash as part of its product offering (TechTarget , 2008).

As far as what actions users and organizations can take if biometric data is compromised goes, already-defined investigation and remediation processes for personally identifiable information (PII) need to be followed. This includes: working with law enforcement if the information is stolen; engaging the public relations/communications team for any interactions with outside entities; working with clients and customers on any actions they should take; and any additional steps your organization has defined for loss of PII (TechTarget , 2008).

3.0 FACIAL RECOGNITION SYSTEM

Face recognition technology is the least intrusive and fastest biometric technology. It works with the most obvious individual identifier – the human face. Instead of requiring people to place their hand on a reader (a process not acceptable in some cultures as well as being a source of illness transfer) or precisely position their eye in

front of a scanner, face recognition systems unobtrusively take pictures of people's faces as they enter a defined area. There is no intrusion or delay, and in most cases the subjects are entirely unaware of the process. They do not feel "under surveillance" or that their privacy has been invaded (Ex-Sight, 2015).

Development through history Face recognition is one of the most relevant applications of image analysis. It's a true challenge to build an automated system which equals human ability to recognize faces. Although humans are quite good identifying known faces, we are not very skilled when we must deal with a large amount of unknown faces. The computers, with an almost limitless memory and computational speed, should overcome human limitations. Face recognition remains as an unsolved problem and a demanded technology. A simple search with the phrase "face recognition" in the IEEE Digital Library throws 9422 results. 1332 articles in only one year - 2009. There are many different industry areas interested in what it could offer. Some examples include video surveillance, human-machine interaction, photo cameras, virtual reality or law enforcement. This multidisciplinary interest pushes the research and attracts interest from diverse disciplines. Therefore, it's not a problem restricted to computer vision research. Face recognition is a relevant subject in pattern recognition, neural networks, computer graphics, image processing and psychology. Using computers to recognize human faces (Bledsoe, 1964; 1966; 1968). Because the funding of these researches was provided by an unnamed intelligence agency, little of the work was published. He continued later his researches at Stanford Research Institute (Bledsoe,1966). Bledsoe (1996) designed and implemented a semi-automatic system. Some face coordinates were selected by a human operator, and then computers used this information for recognition. He described most of the problems that even 50 years later Face Recognition still suffers - variations in illumination, head rotation, facial expression, and aging. Researches on this matter still continue, trying to measure subjective face features as ear size or between-eye distance (Golstein, etel., 1971). They described a vector, containing 21 subjective features like ear protrusion, eyebrow weight or nose length, as the basis to recognize faces using pattern classification techniques. The Face Recognition Problem Fischler and Elschanger tried to measure similar features automatically. Their algorithm used local template matching and a global measure of fit to find and measure facial features. There were other approaches back on the 1970's. Some tried to define a face as a set of geometric parameters and then perform some pattern recognition based on those parameters (Kanade, 1973). He designed and implemented a face recognition program. It ran in a computer system designed for this purpose. The algorithm extracted sixteen facial parameters automatically. In his work, Kenade (1973) compares this automated extraction to a human or manual extraction, showing only a small difference. He got a correct identification rate of 45-75%. He demonstrated that better results were obtained when irrelevant features were not used. In the 1980's there were a diversity of approaches actively followed, most of them continuing with previous tendencies. Some works tried to improve the methods used measuring subjective features (Nixon, 1985). The template matching approach was improved with strategies such as "deformable templates". This decade also brought new approaches. Some researchers build face recognition algorithms using artificial neural networks (Stonham, 1986). The first mention to eigen faces in image processing, a technique that would become the dominant approach in following years, was made by Sirovich and Kirby in (1986). Their methods were based on the Principal Component Analysis. Their goal was to represent an image in a lower dimension without losing much information, and then reconstructing it. (Kirby and Sirovich, 1990). Their work would be later the foundation of the proposal of many new face recognition algorithms. The 1990's saw the broad recognition of the mentioned eigen face approach as the basis for the state of the art and the first industrial applications. In 1992, Mathew Turk and Alex Pentland of the MIT presented a work which used eigen faces for recognition. Their algorithm was able to locate, track and classify a subject's head. Since the 1990's, face recognition area has received a lot of attention, with a noticeable increase in the

number of publications. Many approaches have been taken which has lead to different algorithms. Some of the most relevant are PCA, ICA, LDA and their derivatives. Different approaches and algorithms will be discussed later in this work. (Sirovich and Kirby, 1987).

4.0 BVN NEW SYSTEM PROCEDURE

The same procedure of enrolling BVN should be conducted as earlier stated but with the addition of Facial recognition that will analyze the characteristics of a person's face images input through a digital video camera. It measures the overall facial structure, including distances between eyes, nose, mouth, and jaw edges. These measurements are retained in a database and used as a comparison when a user stands before the camera. This biometric has been widely, and perhaps wildly, touted as a fantastic system for recognizing potential threats (whether terrorist, scam artist, or known criminal) but so far has not seen wide acceptance in high-level usage. It is projected that biometric facial recognition technology overtake fingerprint biometrics as the most popular form of user authentication (Ex-Sight, 2015).

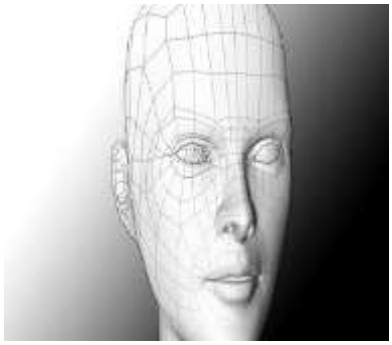
Every face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features. Each human face has approximately some nodal points. Some of these measured by the Facial Recognition Technology are:

- **Distance between the eyes.**
- **Width of the nose.**
- **Depth of the eye sockets.**
- **The shape of the cheekbones.**
- **The length of the jaw line.**

Example are presented as figure 1, 2 and 3 shown below.

These nodal points are measured creating a numerical code, called a face print, representing the face in the database (Ex-Sight, 2015).

Figure 1: Example 1 of the scanning process.



Example 2: of the scanning process.

Figure 3. Example 3 of the scanning process.

4.1 Facial Recognition Algorithm (FRA)

The following four-stage process illustrates the way biometric systems operate:

start

Capture - a physical or behavioural sample is captured by the system during enrolment

read (source, image);

Extraction - unique data is extracted from the sample and a template is created

insert (image in frame);

Comparison - the template is then compared with a new sample

do while noteof(data file)

compare image with image_in data_file

counter=c=ounter+1

loop

Matching - the system then decides if the features extracted from the new sample are matching or not

When the user faces the camera, standing about two feet from it. The system will locate the user's face and perform matches against the claimed identity or the facial database. It is possible that the user may need to to move and reattempt the verification based on his facial position. The system usually comes to a decision in less than 5 seconds. One of the strongest positive aspects of facial recognition is that it is non-intrusive. Verification or identification can be accomplished from two feet away or more, and without requiring the user to wait for long periods of time or do anything more than look at the camera. Face recognition is also very difficult to fool. It works by comparing facial landmarks - specific proportions and angles of defined facial features - which cannot easily be concealed by beards, eyeglasses or makeup.

5.0 CODING

The code below is a method in java which can be integrated in to computer.

Facedetection;

```
import org.opencv.core.Core;
import org.opencv.core.Mat;
import org.opencv.core.MatOfRect;
import org.opencv.core.Point;
import org.opencv.core.Rect;
import org.opencv.core.Scalar;
import org.opencv.highgui.Highgui;
import org.opencv.objdetect.CascadeClassifier;
public class FaceDetector {
   public static void main(String[] args) {
      System.loadLibrary(Core.NATIVE_LIBRARY_NAME);
```

```
        System.out.println("\nRunning FaceDetector");
        CascadeClassifier faceDetector = new
        CascadeClassifier(FaceDetector.class.getResource("haarcascade_frontalface_a
        lt.xml").getPath());
    Mat image = Highgui
          .imread(FaceDetector.class.getResource("shekhar.JPG").getPath());
     MatOfRect faceDetections = new MatOfRect();
    faceDetector.detectMultiScale(image, faceDetections);
        System.out.println(String.format("Detected %s faces",  faceDetections.toArray().length));
     for (Rect rect : faceDetections.toArray()) {
       Core.rectangle(image, new Point(rect.x, rect.y), new Point(rect.x + rect.width,  rect.y  +
rect.height),
              new Scalar(0, 255, 0));
    }
    String filename = "ouput.png";
    System.out.println(String.format("Writing %s", filename));
    Highgui.imwrite(BVNfile, image);
  }
}
```

The code shown above does the following:

1. It loads the native OpenCV library so that we can use it using Java API.
2. Creates an instance of CascadeClassifier passing it the name of the file from which the classifier is loaded.
3. Next we convert the image to a format which the Java API will accept using the Highui class. Mat is the OpenCV C++ n-dimensional dense array class.
4. Then call the *detectMultiScale* method on the classifier passing it the image and MatOfRect object. After processing, the MatOfRect will have face detections.
5. It loops over all the face detections and mark the image with rectangles.
6. Finally, writes the image to the *output.png* file.

6.0 CONCLUSION /RECOMENDATIONS

With the increase in advance technology, such as motion captured, visual reality and so-on, I recommend that bank should try to incorporate facial recognition in their system of BVN so that the limitations and drawbacks highlighted earlier can be eliminated, which will make their system robust, reliable and compatible with modern technology.

7.0 REFERENCE

Bank Verification Number (BVN, 2015). An initiative of the Central Bank of Nigeria. Available at http://www.bvn.com.ng accessed on 10th November, 2015.

Bledsoe. W. W. (1964). The model method in facial recognition. Technical report pri 15, Panoramic Research, Inc., Palo Alto, California.

Bledsoe. W. W. (1966). Man-machine facial recognition: Report on a largescale experiment. Technical report pri 22, Panoramic Research, Inc., Palo Alto, California.

Bledsoe. W. W. (1966). Some results on multicategory Pattern recognition. Journal of the Association for Computing Machinery, 13(2):304–316.

Bledsoe. W. W. (1968). Semiautomatic facial recognition. Technical report SRI-project 6693, Stanford Research Institute, Menlo Park, California.

Brent R. (2015). Measurement of banking services in the U.S national income and product account: recent charges and outstanding issues. Available at: http:// www.bea.gov/papers/pdf/bankpdf. Accessed on 9th November 2015.

Bruner J. S. and Tagiuri. R. (1954). The perception of people. Handbook of Social Psycology, 2(17).

Dennis, Haley, W. & Roberta, R. (2012). System Analysis and Design (5th ed). John Wiley & Sons, Inc. pages 10-155.

Ex-Sight (June, 2015): Tomorrow's Technology, Today-facial Recognition Solutions. Available at: http://www.ex-sight.com/technology.htm. Accessed on 15th November, 2015.

Goldstein, A. Harmon L. and Lest. 1971. A. Identification of human faces. Proceedings of the IEEE, 59:748–760.

Kirby M. and Sirovich. L. (1990). Application of the karhunen-loeve procedure for the characterization of human faces. IEEE Transactions on Pattern Analysis and Machine Intelligence, 12(1):103–108.

Kenade. T. (1973). Picture Processing System by Computer Complex and Recognition of Human Faces. PhD thesis, Kyoto University, November, 1973.

Nixon. M. (1985). Eye spacing measurement for facial recognition. Proceedings of the Society of Photo-Optical Instrument Engineers, SPIE, 575(37):279–285.

Stonham. T. J. 1986. Practical face recognition and verification with wisard. In H. D. Ellis, editor, Aspects of face processing. Kluwer Academic Publishers.

Sirovich L. and Kirby. M. (1987). Low-dimensional procedure for the characterization of human faces. Journal of the Optical Society of America A - Optics, Image Science and Vision, 4(3):519–524.

Tech Target: (2008). Biometric Verification definition. Available at http://www.searchsecurity.techtarget.com/definationj/biometric-verification. Access on May, 2008.

Turk M. and Pentland. A. (1991) Eigenfaces for recognition. Journal of Cognitive Neuroscience, 3(1):71–86.

Zhao W., Chellappa R., Rosenfeld A. and Phillips P. (2003). Face recognition: A literature survey. ACM Computing Surveys, pages 399–458.