Supported by tetfund TERTIARY EDUCATION TRUST FUND

SECURED BIOMETRICS-CRYPTO AUTHENTICATION SYSTEM OVER COMPUTER NETWORK

O. K. Oyetola*, A. A. Okubanjo, M. O. Osifeko, P. O Alao and O. O. Olaluwoye
Computer and Electrical & Electronics Department, Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria
*Corresponding author: okubanjo.ayodeji@oouagoiwoye.edu.ng

Received: September 03, 2019 **Accepted:** January 14, 2020

Abstract: Unprecedented access to data and information through complex communication networks across the world had engendered development of various approaches in securing data to prevent unauthorized access to confidential information. In essence, cryptography and biometrics have been generally accepted as means of securing data and information. Cryptography and biometrics are not without pitfalls, the main shortcoming of cryptography is weak character or forgotten password while interclass similarities in the feature sets used to represent trait and storing of biometric templates in clear unprotected format had been the shortfalls in biometric. This paper presents a novel hybrid of cryptography and biometrics; a bimodal biometric Cryptosystem, using fingerprint and face as trait for authentication over computer network. Subjects' information were encrypted using Advanced Encryption Standard (AES) and biometric templates were stored as Binary Large Object (BLOB) in MYSQL database secured with Message Digest 5 (MD 5) Hashing Algorithm. The system was developed and implemented to operate on one-try, two-try and three-try configurations at varying threshold values for stand-alone and network-based implementation. Furthermore, the developed system's performance was evaluated using False Reject Rate (FRR), False Accept Rate (FAR) and Receiver Operating Characteristic Curve (ROC graph) as performance metrics. On ROC graph, three-try configuration gave optimal performance at all threshold values for the two implementations.

Keywords: Cryptography, authentication, biometric, data security, encryption

Introduction

Authentication systems are generally design to restrict access to data and sensitive information. This is usually achieved by providing credentials which are compared with user's data saved on a database (Mahitthiburin, 2015). Conventionally, database can either be on the same machine as the client application (two-tier model) or on a remote machine (distributed architecture). Although, two-tier model is effective and has been used for many applications, it can only be used for offline purposes, which is a major drawback for modern day applications requiring ubiquitous access. Consequently, authentication over distributed architecture has gained tremendous attention lately due to advancement in internet technologies and telecommunication systems. However, data transfer across communication networks are prone to security threats such as information theft, identity theft, data loss and disruption of services (Barman *et al.*, 2015).

Cryptography algorithms had been used as an essential tool to secure transmission of data over communication networks and to prevent unauthorized access to privy information. Cryptographic authentication systems are possession based; that is, user is required to present a decrypting key to establish authenticity (Jain *et al.*, 2006). These systems are password, electronic code card or One Time Password (OTP) based, which can be forgotten, misplaced or stolen by an infiltrator to access confidential information. Therefore, these drawbacks in the cryptographic systems had prompted researchers to seek for further methods in protecting vital information. Recently, biometrics had been recognized as a means of mitigating the challenges of data and information security in all human endeavors. In essence, biometric entails the use of unique physiological or behavioral characteristics such as face, voice, fingerprints, gait and writing style to identify individuals. Apparently, any physiological or behavioral traits pertaining to human can be used to make a personal recognition provided that it satisfies features such as universality, uniqueness, permanence and collectability (Falohun *et al.*, 2016).

Nevertheless, widespread adoption of biometrics for weighty security system had provoked new interest in researching and discovering methods of attacking biometric systems, making biometric system, like cryptography, vulnerable to security threats (Oyetola *et al.*, 2017). Several researches have analyzed the possibilities of security breaches in relation to biometric and potential approaches to counter these vulnerabilities (Galbally *et al.*, 2007; Alaswad *et al.*, 2014; Hadid, 2014). Attack targeted at biometric templates saved on the database is considered to be most practically damaging attack on biometric systems. Inherently, template is a set of invariant features of the biometric sample used for comparison during authentication. Sizeable biometric authentication systems transfer templates across computer networks in clear unprotected format that permit possibilities of sniffing, stealing, and modification of identity. In addition to aforementioned vulnerabilities, possible large similarities in the feature sets used to represent traits could hamper the uniqueness provided by the biometric trait. Hence, single biometric trait will not be suitable for effective authentication. In light of the vulnerabilities and limitations of existing methods, this paper presents a hybrid scheme which can use the benefits of different protection schemes to lessen the drawbacks of existing systems. In this approach, we combined two biometric modalities, cryptography techniques and database management system (DBMS) technology in developing a secure authentication system over a computer network.

The database is installed on a server which is accessible to clients across the network. Using a three-tier architecture, we developed a business logic app for the system called "*Comm Robot*". The robot runs as a service between the client's application and the DBMS. Within the robot is the SQLEngine object, which handles all queries to the database and supporter objects for each table in the database. Also, access to the database is secured with MD5 Hash algorithm. Authors (Jain *et al.*, 2004; Shukla and Mishra, 2012) proved that biometric system is more efficient when multimodal approach is employed as compared to unimodal approach network security from cancelable fingerprint template of both communicating parties. By concatenating both templates at features extraction level to create a fused template, a unique session key is generated using shuffle key and hash of shuffled fused template. In this approach, revocable key for symmetric cryptography is generated from irrevocable fingerprint and privacy of the fingerprints is protected by the cancelable transformation of fingerprint template. Contrarily, a cryptosystem uses cryptography to secure data which essentially involves encryption (i.e. the use of specific mathematical algorithm to change plain text to an unintelligible text called cipher text) and decryption (i.e. conversion from cipher text to plain text). Also, it allows secure transfer of crucial information across unsafe networks such as the Internet (Cryptosystem *et al.*, 2014; Selvarani and Visu, 2015).

In addition to an algorithm, a key (Ke) is compulsory for encryption and key (Kd) for decryption. As a matter of fact, the strength of the keys is tantamount to the integrity afforded by the cryptosystem. In relation to the keys, cryptosystem can broadly be categorized into two, namely; symmetric cryptography and asymmetric cryptography. In symmetric cryptography (e.g., Data Encryption Standard (DES), Advanced Encryption Standard (AES)), Ke = Kd i.e. same key is used to encrypt and decrypt. In asymmetric cryptography (e.g., Rivest-Shamir-Adleman (RSA) Algorithm) Ke ≠ Kd i.e. two different keys are used, Ke is the public key used to encrypt a message and Kd is private key used to decrypt the ciphertext into plaintext. A biometric-crypto system combines cryptography and biometric to secure information. In biometric-crypto systems, certain template's information also known as helper data is made public. However, it is important to underscore that while the helper data is useful during the matching process to generate the cryptographic keys, it does not reveal any meaningful information about the original template.

Generally, biometric-crypto systems are categorized into two main types, key release and key generation. In the former, users' biometric data is used to randomly create cryptographic key to deter unauthorized access to information; while in the later, key is generated from extracted biometric features. A biometric-crypto system combines cryptography and biometric to secure information. In biometric-crypto systems, certain template's information also known as helper data is made public. However, it is important to underscore that while the helper data is useful during the matching process to generate the cryptographic keys, it does not reveal any meaningful information about the original template. Nandakumar *et al.* (2008) pointed out that in a key generating cryptosystem; the cryptographic key is actually generated from the helper data derived from the original biometric template.

Moreover, a number of researches had employed cryptosystem to secure information. Jagadeesan *et al.* (2010) proposed an approach based on multimodal biometrics using Iris and fingerprint to generate a protected cryptographic key. In their study, security is further improved with the difficulty of factoring large numbers. In a view to achieve this, minutiae points and texture properties are extracted from the fingerprint and iris images, respectively. At the feature level, the extracted features are fused to obtain the multi-biometric template. Lastly, a multi-biometric template is used for generating a 256-bit cryptographic key. Similarly, (Abuguba *et al.*, 2015) presented cryptographic key generation from iris and face biometric traits in which biometric features extracted from preprocessed face and iris images are fused at the feature level and the multimodal biometric template is constructed from the Gabor filter and Principal Component Analysis outputs. This template is used to generate strong 256-bit cryptographic key. Viola and Jones (2001) proposed an approach to generate cryptographic key for communication.

Materials and Methods

The proposed biometric-crypto system consists of several modules to authenticate or verify subjects over computer network. Fig. 1 shows the stages involved in the model. In our approach, biometric features are extracted from fingerprints and face image on clients system while cryptography key are generated using minutiae points from fingerprints before transferring to the server. Consequently, information are encrypted based on individual's unique traits and to further enhance the integrity of the system, templates and encrypted data are store in MySQL DBMS secured with MD Hash 5 algorithm.

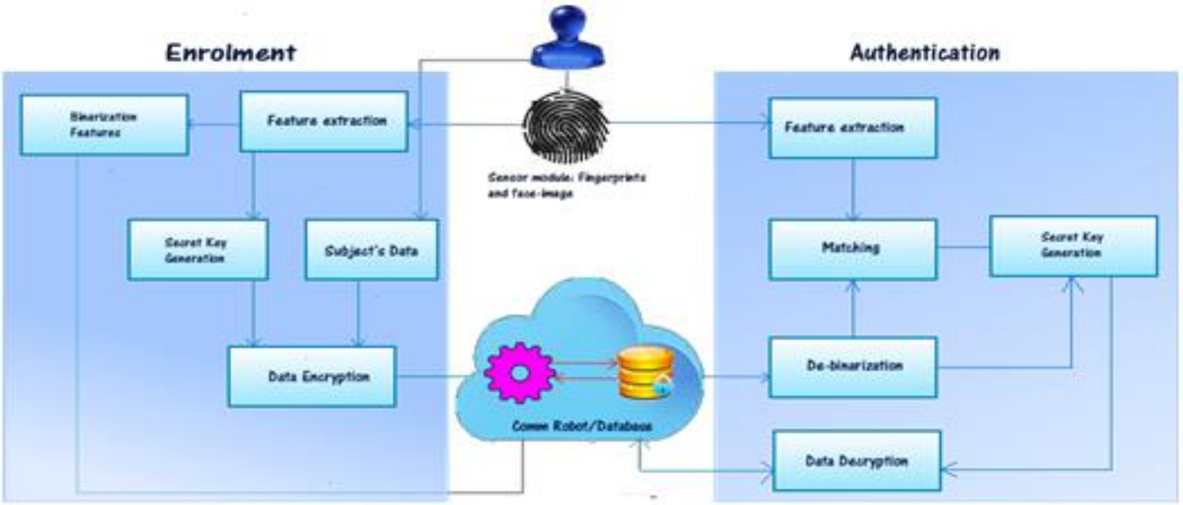
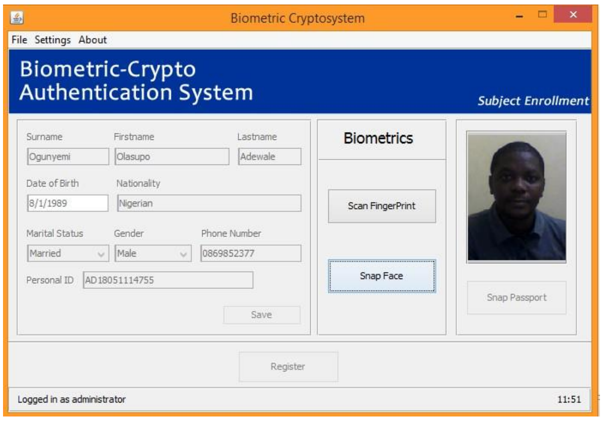


Fig. 1: Developed system architecture

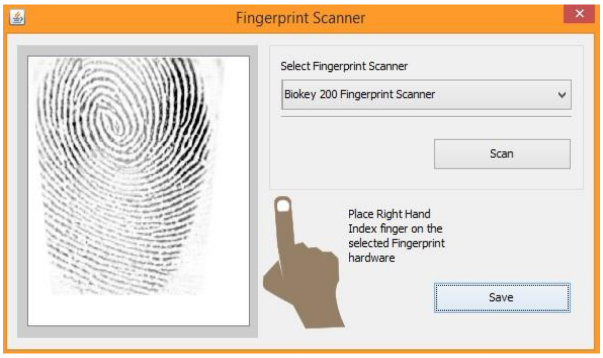
To ease enrolment process, a graphical user interface (GUI) is designed to provide a mechanism for collecting subject's details as shown in Fig. 2. During this process, a unique identification number (ID) is generated for each subject which is linked with the biometric data and is unique across all subject. This is made possible by using sequence of time concatenated with two randomly generated alphabet between A – Z. An example of an ID generated by the system is AD15202235201. Hence, an ID is a means for the subject to indicate his/her identity for authentication. The enrollment stage of the system is made up of the sensor module, feature extraction module, binarization module, and encryption module and template database as depicted in Fig. 1.



Surname: Ogunyemi
Firstname: Olasupo
Lastname: Adewale
Date of Birth: 8/1/1989
Nationality: Nigerian
Marital Status: Married
Gender: Male
Phone Number: 0869852377
Personal ID: AD18051114755

Logged in as administrator 11:51

Fig. 2: Enrolment GUI of the developed system



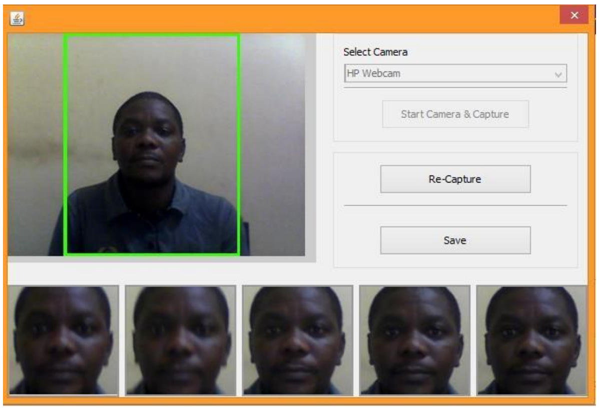
Select Fingerprint Scanner: Biokey 200 Fingerprint Scanner

Place Right Hand Index finger on the selected Fingerprint hardware

Fig. 3: Fingerprint enrollment interface of the developed system

Sensor module

At sensor module, a suitable user interface incorporating the biometric sensor or scanner was developed to measure or record the raw biometric data of users. This raw biometric data was captured and transferred to the next module for feature extraction. The fingerprint scanner uses live scan method for capturing the fingerprint image. A Live scan fingerprint is a general term for a fingerprint image directly obtained from the finger without the intermediate step of getting a stamp of an inked finger on a paper. This type of fingerprint image is based on the optical Frustrated Total Internal Reflection (FTIR) concept. When the finger is placed on one side of a glass prism, finger's ridges are in contact with the prism. The remaining part of the imaging system basically consists of a light source. The light that incidents on the prism at the glass surface touched by the ridges is randomly scattered while the light that incidents at the glass surface corresponding to valleys suffers total internal reflection. Consequently, dark portions of the image formed correspond to ridges while bright portions correspond to valleys as depicted in Fig. 3. Furthermore, the face image is captured automatically whenever a face image is detected by the system through the camera with the image been captured only when the subject is facing the camera. This is to control the quality of the image and to capture uniform images during enrollment and authentication. The face scanner was design using the AdaBoost object detection algorithm (Viola and Jones, 2001) which involves training a series of increasingly discriminating simple classifiers and then blending their outputs for face recognition. Fig. 4 shows the system face image scanner interface. It is pertinent to note also, that fingerprint scanner and the camera are connected to the computer via USB interface.



Select Camera: HP Webcam

Fig. 4: Face image scanner interface; Face images scanned, subject facing the camera

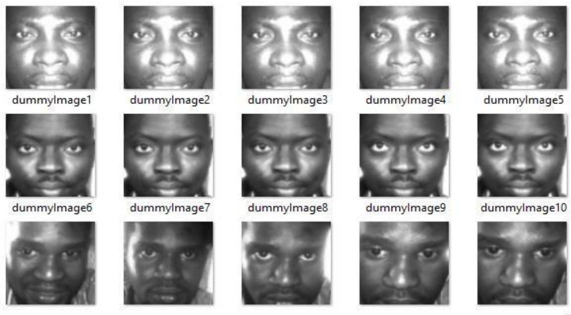


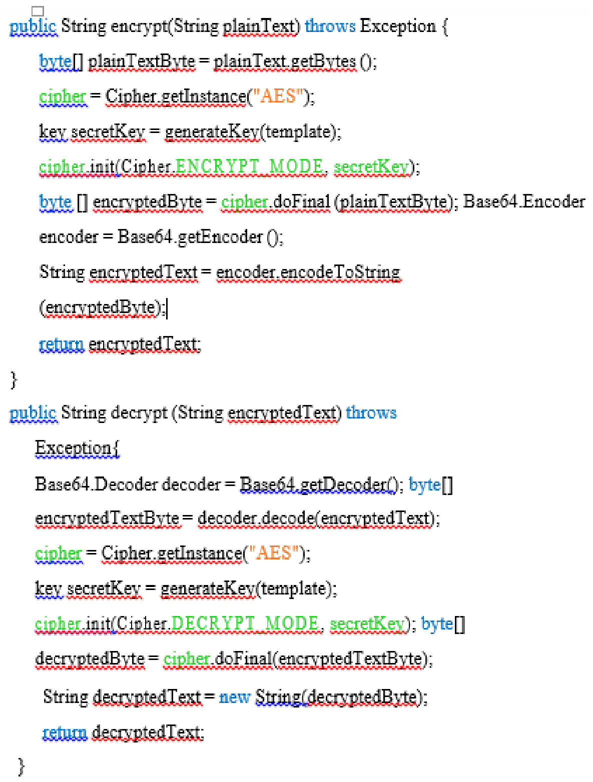
Fig. 5: Blocks of classes for fisherfaces.

Feature extraction module

At feature extraction module, the quality of the acquired biometric data from the sensor is assessed initially for further processing. For facial recognition, fisher faces (LDA) algorithm was employed for features extraction and matching because is insensitive to large variation in lighting direction and facial expression. LDA is a statistical approach for classifying samples of unknown classes based on training samples with known classes. This technique aims to maximize between-class (i.e., across users) variance and minimize within-class (i.e., within user) variance. As shown in Fig. 5 each block represents a class, there are large variances between classes, but little variance within classes. The system uses five blocks of known class samples to train against unknown samples for recognition. The system also adopt minutiae based matching algorithm for fingerprint recognition. One of the significant parts of this algorithm is the classification of fingerprints which allows minimizing significantly the number of fingerprints referenced for each authentication procedure.

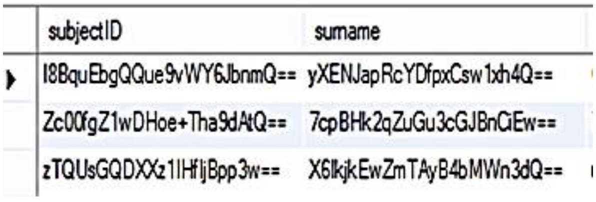
Encryption module

All entries in the database are encrypted using Advanced Encryption Standard (AES) cryptography algorithm to ensure that subject information is not saved in plain text for enhanced system security. AES algorithm works on the principle of Substitution Permutation network. The AES cipher is identified as a number of reiterations of transformation rounds that translate the input plaintext into the final output of cipher text. Using this approach, an encryption key is generated from biometric template of each subject key to protect personal data distinctively. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key. This module employs the Java Cryptography Architecture (JCA) to implement AES. Code snippet of the Security Engine designed for the system is as follows:



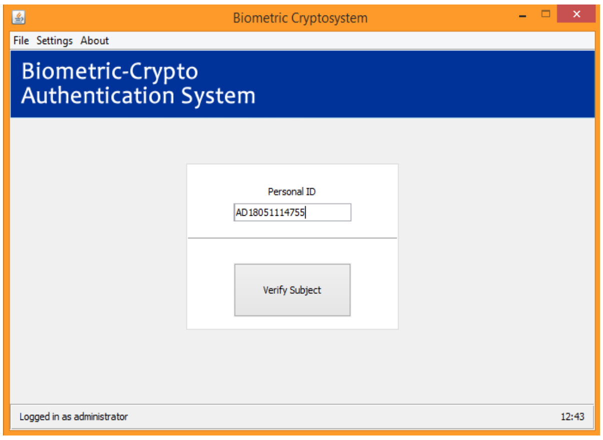
```
public String encrypt(String plainText) throws Exception {
      byte[] plainTextByte = plainText.getBytes ();
      cipher = Cipher.getInstance("AES");
      key secretKey = generateKey(template);
      cipher.init(Cipher.ENCRYPT_MODE, secretKey);
      byte [] encryptedByte = cipher.doFinal (plainTextByte); Base64.Encoder
      encoder = Base64.getEncoder ();
      String encryptedText = encoder.encodeToString
      (encryptedByte);
      return encryptedText;
}
public String decrypt (String encryptedText) throws
     Exception{
     Base64.Decoder decoder = Base64.getDecoder(); byte[]
     encryptedTextByte = decoder.decode(encryptedText);
     cipher = Cipher.getInstance("AES");
     key secretKey = generateKey(template);
     cipher.init(Cipher.DECRYPT_MODE, secretKey); byte[]
     decryptedByte = cipher.doFinal(encryptedTextByte);
      String decryptedText = new String(decryptedByte);
      return decryptedText;
 }
```

The database helper classes used the security engine to encrypt data when saving data to the database and to decrypt data when retrieving data from the data base. Fig. 6 shows encrypted data view from the database.



	subjectID	sumame
▶	I8BquEbgQQue9vWY6JbnmQ==	yXENJapRcYDfpxCsw1xh4Q==
	Zc00fgZ1wDHoe+Tha9dAtQ==	7cpBHk2qZuGu3cGJBnCiEw==
	zTQUsGQDXXz1IHfIjBpp3w==	X6lkjkEwZmTAyB4bMWn3dQ==

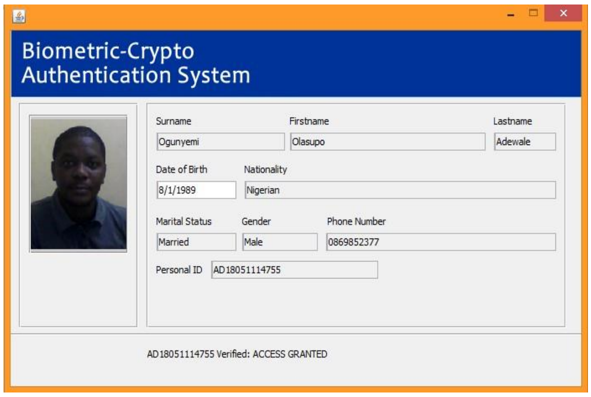
Fig. 6: Database view of encrypted data



Personal ID AD18051114755

Logged in as administrator 12:43

Fig. 7: Authentication stage interface



Surname Ogunyemi
Firstname Olasupo
Lastname Adewale
Date of Birth 8/1/1989
Nationality Nigerian
Marital Status Married
Gender Male
Phone Number 0869852377
Personal ID AD18051114755

AD18051114755 Verified: ACCESS GRANTED

Fig. 8: Authentication output interface

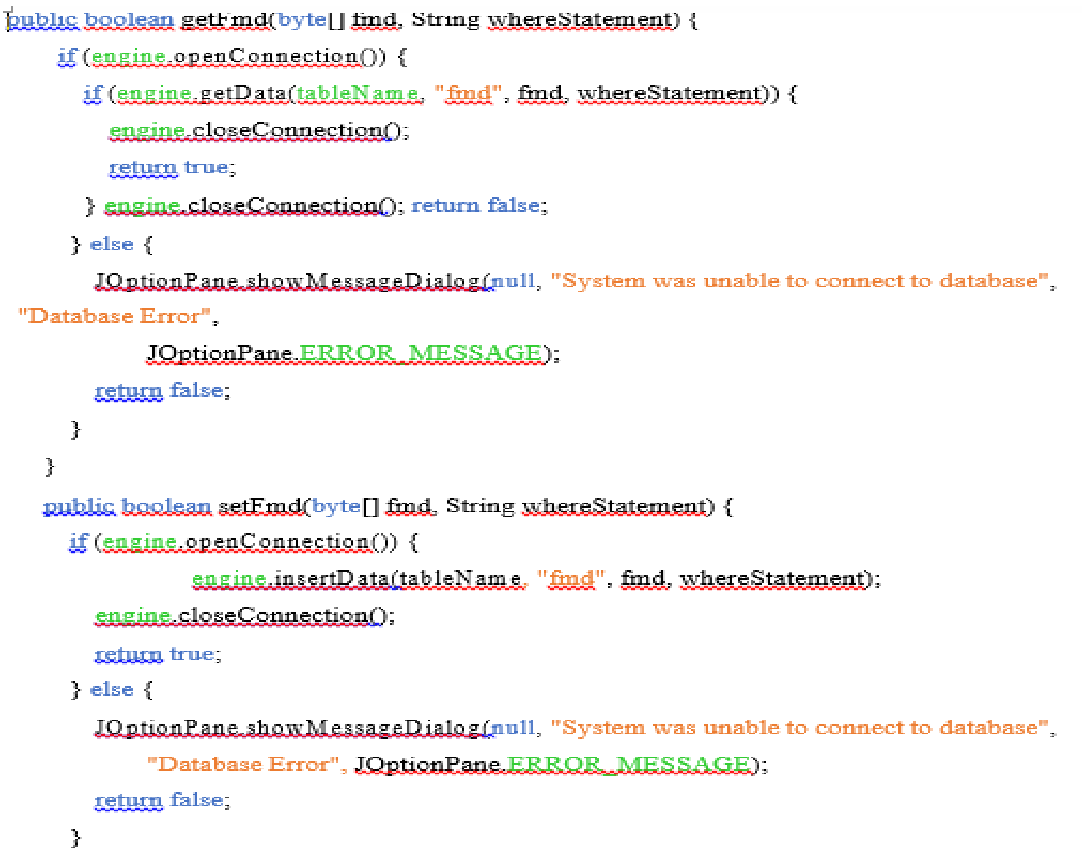
Encryption module

At the authentication stage, subject presents his/her ID as shown in Fig. 7. Thereafter, features were again extracted from face image and fingerprint acquired from the claimed authentic subject and matched with the enrolled data linked with the ID on the server. The authentication stage includes matching module that compares extracted features with stored template, and decision module which determines authentication outcome based on match score. However, the match score might be affected by the quality of the given biometric data. The matching module also compressed a decision making module in which the generated match score is used to validate the claimed identity. Comparatively, the system combines the matching score of both templates to make decision using logical AND. The matcher begins by matching the fingerprints, if the fingers matched it proceeds to matching the faces, else it denies the subject. Therefore, for a subject to be granted access, both fingerprints and face image must match the enrolled templates. Thereafter, the system uses fingerprints template to generate a key to decrypt subject and display subject information in plain text as shown in Fig. 8.

System class diagram and dependency

Object Oriented Analysis and Design (OOAD) approach was employed in the system design. This allows modeling objects by their attributes and behaviors just as human describe real-world objects. The developed system model was implemented using Java technology which support easy database connection. In addition, oracle created a standardized interface to databases from Java called Java Database.

Connectivity (JDBC), which makes it possible to connect a Java application with MySQL database. Using the Connector/J JDBC driver, the system queries the database for data. The classes modelled for the application and their dependency on each other is shown in Fig. 9. The system uses three-tier application architecture, which can be refer to as Distributed architecture**.** A business logic application ("Comm Robot") coordinates communications between the client application and the database. Comm robot runs the recognition algorithm as a service on the server. It takes request, process and makes decision before storing to the database. An object of the class SQLEngine is a main module to connect to the database. The code snippet of system connection using SQLEngine object is as follows:



```
public boolean getFmd(byte[] fmd, String whereStatement) {
      if (engine.openConnection()) {
        if (engine.getData(tableName, "fmd", fmd, whereStatement)) {
          engine.closeConnection();
          return true;
        } engine.closeConnection(); return false;
      } else {
        JOptionPane.showMessageDialog(null, "System was unable to connect to database",
  "Database Error",
              JOptionPane.ERROR_MESSAGE);
        return false;
      }
    }
    public boolean setFmd(byte[] fmd, String whereStatement) {
      if (engine.openConnection()) {
                engine.insertData(tableName, "fmd", fmd, whereStatement);
        engine.closeConnection();
        return true;
      } else {
        JOptionPane.showMessageDialog(null, "System was unable to connect to database",
              "Database Error", JOptionPane.ERROR_MESSAGE);
        return false;
      }
```

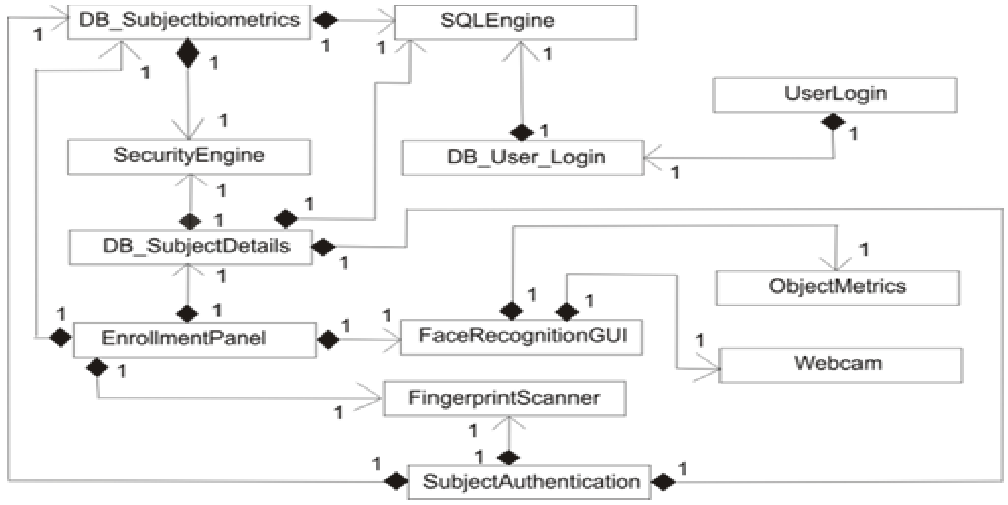


Fig. 9: UML Class dependency diagram

Performance evaluation was carried out on the developed system using false-rejection error rates and false-acceptance error rates for both stand-alone (i.e. clients and server on the same system) and network based (i.e. server on a remote computer) implementations. The error rates are described as a percentage of occurrence over all verification attempt. “Attempt” describe one round of a person using the system to verify an enrolled subject. The system allows three try per attempt. “Try” defines a single presentation of an individual’s biometric sample to the system for measurement. “False-rejection” is the rejection of subject who makes an honest attempt to be verified while “False-acceptance” is the acceptance of an imposter as subject. In our test sample, 500 subjects were enrolled by the proposed system. Individuals were trained on how to interact with the biometric devices in other to generate the best template for authentication. The study therefore assumes that all subjects are familiar with the system and that user-system interaction error were of no significant effect on the test result. It is important to note that tests were carried out using 500 genuine enrollees and 500 impostors at different threshold values.

Results and Discussion

Performance evaluation was carried out on the developed system using false-rejection error rates and false-acceptance error rates for both stand-alone (i.e. clients and server on the same system) and network based (i.e. server on a remote computer) implementations. The error rates are described as a percentage of occurrence over all verification attempt. “Attempt” describe one round of a person using the system to verify an enrolled subject. The system allows three try per attempt. “Try” defines a single presentation of an individual’s biometric sample to the system for measurement. “False-rejection” is the rejection of subject who makes an honest

attempt to be verified while “False-acceptance” is the acceptance of an imposter as subject. In our test sample, 500 subjects were enrolled by the proposed system. Individuals were trained on how to interact with the biometric devices in other to generate the best template for authentication. The study therefore assumes that all subjects are familiar with the system and that user-system interaction error were of no significant effect on the test result. It is important to note that tests were carried out using 500 genuine enrollees and 500 impostors at different threshold values. Furthermore, the performance evaluations were analyzed based on false rejection and acceptance rates. In order to evaluate false rejection rate, the test was conducted at different threshold values. Tables 1 and Table 2 showed the false rejection rate in percentage values for one-, two, and three try configuration at various threshold value for stand-alone and network based implementation, respectively. Fig. 10 depicts the graphs of false rejection rate at various threshold value for one-, two-, and three try configuration respectively. The graphs depicts that the authentication system false rejection error rate reduces as the threshold is reduced. It is also noticed that the system performance becomes more accurate on three-try configuration for both implementation. However, there is slight variation in false rejection rate as shown in the graph.

Table 1: Developed system false rejection rate for stand-alone implementation

Threshold values	False Rejection Rate (%)		
	One-try	Two-try	Three-try
100	1.00	1.00	0.01
200	3.00	1.00	0.03
300	5.00	2.00	0.05
400	8.00	3.00	0.08
500	10.00	6.00	2.00

Source: Oyetola *et al.* (2017)

Table 2: Developed system false rejection rate for Network-based implementation

Threshold values	False rejection rate (%)		
	One-try	Two-try	Three-try
100	1.05	1.50	0.02
200	3.06	1.70	0.06
300	5.08	2.20	0.09
400	8.13	3.00	1.20
500	10.12	6.00	2.20

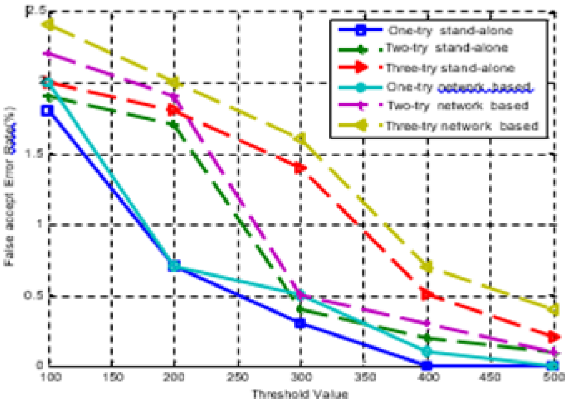


Fig. 10: False reject rate

The false acceptance test was carried out on impostors at various threshold value for one-, two- and three try configuration. Each volunteer presents ID of a known subject against his/her own biometric. The results of the test are shown in Tables 3 and 4. Graphs of the three configurations for stand-alone and network-based implementations are shown in Fig. 11. Again both implementation follows same curve pattern as show in Fig. 10.

Table 3: Developed system false acceptance rate for stand-alone implementation

Threshold values	False acceptance rate (%)		
	One-try	Two-try	Three-try
100	1.80	1.80	2.00
200	0.70	1.60	1.70
300	0.30	0.40	1.40
400	0.00	0.40	0.60
500	0.00	0.20	0.30

Source: Oyetola *et al.* (2017)

Table 4: Developed system false acceptance rate for Network-based implementation

Threshold values	False acceptance rate (%)		
	One-try	Two-try	Three-try
100	1.80	2.20	2.40
200	0.70	1.80	2.00
300	0.30	0.50	1.60
400	0.00	0.35	0.70
500	0.00	0.01	0.04

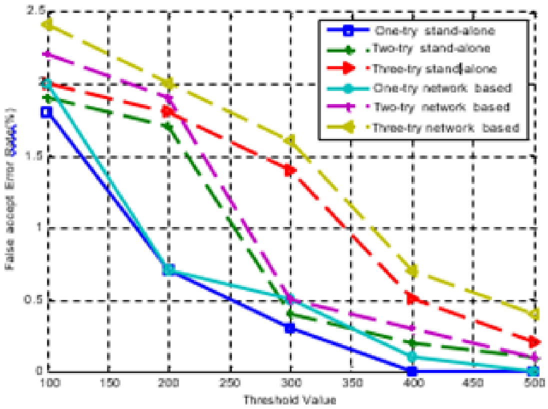


Fig. 11: False accept rate

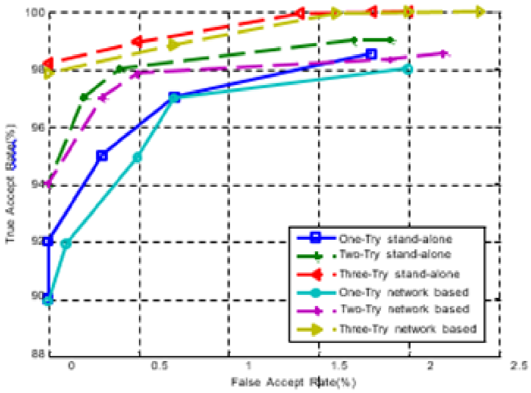


Fig. 12: Developed System ROC

ROC curve points out performance level for all possible combinations of correct verification and false acceptance rate. It is a plot of true positive (1 - FRR) vs. false positive rate (FAR) at various threshold values. The use of an ROC curve for characterizing the performance of the developed authentication system makes it relatively straightforward to compare the three operation configuration. The best configuration performance is seen at the top of the plot. As shown in Fig. 12, three-try configuration yield the best possible prediction for both stand-alone and network implementations. FAR error is 0.6% at 99% true acceptance rate for stand-alone implementation and 0.6% at 98.4% true acceptance rate for network-based implementation.

Conclusion

In this research, an authentication system that combines biometric and cryptography algorithms was developed to verify user over a computer network. Two biometric modalities were used; face image and fingerprint. The developed system employed AES encryption algorithm and database methodologies to secure data. The performance of the system was evaluated for stand-alone and network-based implementations. The system stand-alone FAR error obtained was 0.6% at 96, 98 and 99 % true acceptance rate for one-try, two-try and three-try configuration, respectively. While network-based implementation present true acceptance error of 95, 97.2 and 98.4% at 0.6% FAR for one-try, two-try and three-try configuration respectively. It is apparent in the result that as the threshold value increases, FAR reduces while FRR increases for all configurations and three-try configuration gave optimal performance at all threshold values for both implementations. The results also showed that the network overhead has no significant effect on the authentication performance of the developed system. However, the network resources incurred delay on authentication time. This can be improved by enhancing the network performance metric. Nevertheless, the developed system can be employed in securing business and personal information over a computer network.

Conflicts of Interest

No conflict of interest was declared by the authors.

References

Abuguba S, Milosavljević MM & Maček N 2015. An efficient approach to generating cryptographic keys from face and iris biometrics fused at the feature level. *IJCSNS Int. J. Comp. Sci. and Network Security*, 15(6): 6–11.

Alaswad AO, Montaser AH & Mohamad FE 2014. Vulnerabilities of biometric authentication: Threats and countermeasures. *Int. J. Infor. & Comp. Techn.*, 4(10): 947–958.

Barman S, Samanta D & Chattopadhyay S 2015. Fingerprint-based crypto-biometric system for network security. *EURASIP J. Infor. Secu.*, 1: 3. doi: 10.1186/s13635-015-0020-1.

Cryptosystem RSA, Oyelade J & Oladipupo O 2014. Implementation of secured message transmission using. *Covenant J. Infor. and Commun. Techn. (CJICT)*, 2(2): 75–88.

Falohun AS, Fenwa OD & Oke AO 2016. An access control system using bimodal biometrics. *Int. J. Appl. Infor. Sys.*, 10(5): 41–47. doi: 10.5120/ijais2016451510.

Galbally J, Fierrez-Aguilar J & Ortega-Garcia J 2007. Vulnerabilities in biometric systems: attacks and recent advances in liveness detection. *Database*, 1(3): 4.

Hadid A 2014. Face biometrics under spoofing attacks: Vulnerabilities, countermeasures, open issues, and research directions. *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, (Cmv), pp. 113–118. doi: 10.1109/CVPRW.2014.22.

Jagadeesan A, Thillaikkarasi T & Duraiswamy DK 2010. Cryptographic key generation from multiple biometric modalities: Fusing Minutiae with Iris feature. *Int. J. Comp. Applic.*, 2(6): 16–26. doi: 10.5120/673-946.

Jain AK, Ross A & Pankanti S 2006. Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Sec.*, 1(2): 125–143. doi: 10.1109/TIFS.2006.873653.

Jain AK, Ross A & Prabhakar S 2004. *An Introduction to Biometric Recognition* I, 14(1): 1–29.

Mahitthiburin S 2015. Improving Security with Two-factor Authentication Using Image Improving Security with Two-factor Authentication Using Image, (April). doi: 10.14416/j.ijast.2014.11.003.

Nandakumar K, Jain AK & Nagar A 2008. Biometric template security. *Eurasip J. Advances in Signal Processing*, 2008(January), pp. 1–20. doi: 10.1155/2008/579416.

Oyetola OK, Okubanjo AA, Osifeko MO, Sanusi OI & Abolade RO 2017. An improved authentication system using hybrid of biometrics and cryptography', in *2017 IEEE 3rd International Conference on Electro-Technology for National Devt. (NIGERCON)*. IEEE, pp. 457–463. doi: 10.1109/NIGERCON.2017.8281915.

Selvarani P & Visu P 2015. Multi-model bio-cryptographic authentication in cloud storage sharing for higher security. *Res. J. Appl. Sci., Engr. and Techn.logy*, 11(1): 95–101. doi: 10.19026/rjaset.11.1680.

Shukla S & Mishra P 2012. A Hybrid Model of Multimodal Biometrics System using Fingerprint and Face as Traits, 1: 406–410.

Viola P & Jones M 2001. Rapid object detection using a boosted cascade of simple features. *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001*, 1: pp. I-511-I-518. doi: 10.1109/CVPR.2001.990517.