IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

**International Journal of Digital Application & Contemporary Research**
**Website: www.ijdacr.com (Volume 6, Issue 8, March 2018)**

# Analysis of Multimodal of Biometric System

[1]Rahul C Bakshe
[1]PhD Scholar, SRK University, Bhopal
Email- [1]rahulbakshe@gmail.com

*Abstract*— **A biometric authentication system uses the physiological characteristics (such as fingerprints, face, hand features, iris) and / or behavioural characteristics (such as voice, signature, walking, and writing) of an individual to identify their identity. There are many biometric methods of identifying individuals, the most used is through the fingerprint. This is why the purpose of the present titling work is to analyze the vulnerabilities of fingerprint based biometric recognition systems, since there are different attack techniques that allow access by means of the falsification of fingerprints. For this, a Systematic Review was developed using the IEEE, Science Direct and Google Scholar databases, finding, under certain criteria of inclusion and exclusion, scientific articles as well as of the work done, since, based on the protocol of Barbara Kitchenham, studies were obtained showing that There are ways to attack the different levels of processing of identification and verification of fingerprints, which will address software attack algorithms such as Hill - Climbing and Side - Channel which consist of the generation of pattern patterns for fingerprints Random fingerprints that are iteratively modified to achieve a desired similarity with respect to a real footprint in order to be accepted by a verification system.**

*Keywords*— **Fingerprint, Hill Climbing, Side Channel, Multimodal, Unimodal.**

## I. INTRODUCTION

In the current context, the security of information systems has become a very important area of research; in particular, designing a Reliable, efficient and robust identification system is a priority task.

The identification of the individual has become essential to ensure the safety of systems and organizations, Faced with this growing demand, several methods of biometric recognition have been proposed, speaker recognition, facial recognition, fingerprint, recognition of the iris, retina, shape of the hand.These methods have reached their limits, in terms of performance. For example, Face recognition or voice recognition are very well accepted by users but the rate of good facial identification is at best of the order of 85% [1], which makes them too unsatisfactory for real applications.

Other methods are more reliable such as recognition of the retina or the iris, they are expensive and in general, poorly accepted by the general public. Moreover, the systems that rely on a single biometric modality are vulnerable to attack. For the moment, no biometric indicator is reliable at 100% according to [2]. What created a need to the fusion of biometric indicators multimodal all the arguments cited before plus the results of the various works [3] [4] [5] [6] showed the performance of Multimodal Biometric Systems compared to Unimodal systems is a strong reason that led us to work on this subject (Adding a modality to a biometric system is adding a new source of information [7]).

Biometrics has its origins in anthropometric recognition processes1, the oldest being fingerprint analysis. The imprint of the thumb was already used as a signature during commercial exchanges in Babylon in ancient times and in China in the 7th century. For several years, significant efforts have been made in the area of biometrics research. This is explained by the presence of a global context in which security needs are becoming increasingly important and where the economic stakes are enormous. Biometric applications are numerous and allow to bring a higher level of security regarding access (secure buildings, airports, casinos, etc.).

The first question we need to answer is: what is biometrics? The word biometrics refers in a very broad sense to the quantitative study of living things, but in our more specific context of recognition and identification of individuals, there are two main definitions that complement each other [8]:

- Biometrics is the science that uses mathematics to study biological variations within a given group;
- Any automatically measurable, robust and distinctive physical characteristic or personal trait that can be used to identify an individual or to verify the identity that an individual asserts.

### *A. Biometric characteristics*

Biometric characteristics [9] can not be easily stolen, falsified, or shared. Thus, they are more reliable and secure for person recognition than traditional methods based on knowledge or possession. However, these physical and behavioural characteristics must satisfy several constraints for a high reliability of the biometric systems. Indeed, the objectives of biometric recognition are the ease of use by a recognition without card or PIN, the increased security which is translated by the difficulty to circumvent the access control as well as the greater performance with regard to the precision and the speed of treatments. Thus, each physiological and / or behavioural characteristic can be used as a biometry to recognize a person as long as it meets these requirements:

- universal (exist in all individuals),
- unique (to differentiate one individual from another),
- Permanent (allow evolution over time),
- Recordable (collect the characteristics of an individual with his agreement),
- Measurable (allow future comparison).

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

**International Journal of Digital Application & Contemporary Research**
**Website: www.ijdacr.com (Volume 6, Issue 8, March 2018)**

However, in a practical biometric system, there are a number of parameters that need to be considered, including:

- User acceptance that reflects the extent of concerns and objections that the use of a given biometric technology tends to generate. In some countries, facial recognition is poorly accepted; in other countries, fingerprint recognition has criminal overtones. The measure of acceptance remains highly subjective and varies from person to person and from country to country, depending on the data protection regime in force, the cultural context and the users' personal expectations.
- The bypass, which reflects how easy it is to cheat the system by fraudulent methods.
- The permanence or stability that is defined by the constancy of a biometric characteristic during normal development and aging of a person. In principle, the more stable a feature is, the less need to update personal characteristics or re-register the person.

A practical biometric system must have an acceptable accuracy and a reasonable recognition rate of resources required, harmless to users, accepted by the population, and robust enough against fraudulent methods. Many biometric modalities are used in various applications (see Figure 1). Each biometric modality has its strengths and weaknesses and the choice usually depends on the application to be processed. No biometric modality actually meets the requirements of all applications.

The comparison between the different biometries makes it possible to choose a technology according to the constraints related to the application. Indeed, each biometric feature (or modality) has its strengths and weaknesses, and matching a specific biometric system to an application depends on the operational mode of the application and the biometric characteristics chosen.

*B. Modes of Operation of A Biometric System*

Biometric systems can provide three modes of operation, namely, enrollment, authentication (or verification) and identification. In the following, the figures will illustrate the example of a biometric system using the fingerprint as modality [10].

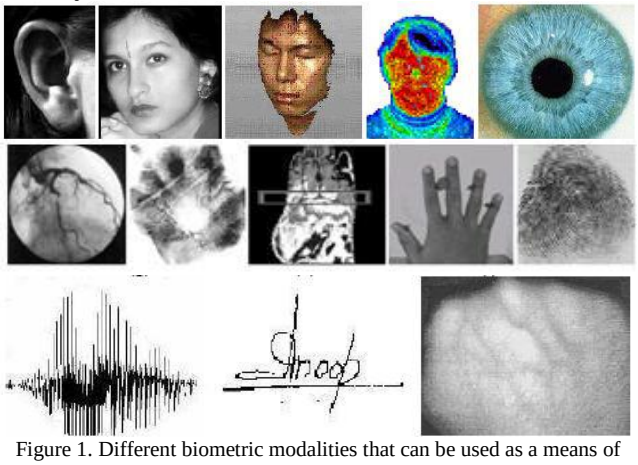

Figure 1. Different biometric modalities that can be used as a means of identification

*Enlistment mode:* This is the first phase of any biometric system, which is the stage in which a user is registered in the system for the first time and where one or more biometric modalities are captured and recorded in a database. This recording may be accompanied by the addition of biographical information in the database.

*Authentication mode:* The user asserts his identity and the system checks whether this statement is valid or not.

*Identification mode:* The user does not explicitly disclose his identity (see Figure 1). However, the implicit assertion made by the user is that she is one of the people already enlisted by the system. Thus, the biometric sample of the individual is compared with the models of all persons in the database. This is called 1: N correspondence. The output of the biometric system consists of the identity of the person whose model has the highest degree of similarity with the biometric sample presented as input. Typically, if the greatest similarity between the sample and all models is below a fixed minimum security threshold, the person is rejected, which implies that the user was not one of the people enlisted by the system. Otherwise, the person is accepted.

*C. Biometric techniques*

Biometric techniques [11] are currently used for security applications. Each has advantages and disadvantages, the choice of a technique is according to the application. Figure 1 shows some biometric techniques. Biometric terms can be classified into three categories:

- The methods that are based on the analysis of biological traces (odour, blood, DNA, etc.)
- Morphological modalities that use a part of the human body such as fingerprint, iris, etc.
- Behavioural modalities use a personal behavioural trait, such as signature, gait, etc.

Morphological modalities are the most used in relation to behavioural modalities. This is due to their stability over time and the difficulty of falsifying these modalities. Moreover, the behavioural modalities are generally affected by the moral state of the individuals.

Biometric techniques are divided into two groups according to the cooperation or not of the individual:

1. *Intrusive Techniques:* These techniques require physical contact with the individual to identify them, such as fingerprints, retina, laughing or the shape of the hand. Their use is generally badly accepted [12].
2. *Non-intrusive Techniques:* These techniques do not require the cooperation of the individual in question their application can be done remotely using sensors that do not require direct contact with the user (face, gait, etc.) [13].

*D. Measuring the Performance of a Biometric System*

First of all, in order to understand how to determine the performance of a biometric system, we need to clearly define three main criteria:

1. The first criterion is called the False Reject Rate (FRR). This rate represents the percentage of people who are supposed to be recognized but who are rejected by the system;

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

**International Journal of Digital Application & Contemporary Research**
**Website: www.ijdacr.com (Volume 6, Issue 8, March 2018)**

2. The second criterion is the False Accept Rate (FAR). This rate represents the percentage of people who are expected to be unrecognized but who are still accepted by the system;
3. The third criterion is known as the Equal Error Rate (EER). This rate is calculated from the first two criteria and constitutes a point of measurement of current performance. This point corresponds to the place where FRR = FAR, that is to say the best compromise between false rejections and false acceptances.

These two comparisons make it possible to choose an appropriate technology according to the constraints related to the requested application. For example, we note that the iris and the fingerprint are the most discriminating modalities. This is useful for large-scale identification systems requiring a high level of security.

TABLE I. SHOWS THE OVERALL RESULT OF THIS COMPARISON

| Technique | Advantages | Disadvantages |
|---|---|---|
| Digital fingerprint | Inexpensive ; Medium ergonomics; Ease of use ; Small size of the reader; Most tested; Fast treatment. | Optimum quality of measuring devices (Reliability); Average acceptability; Possibility of attacks. |
| Geometry of the hand | Very ergonomic; Good acceptability. | Bulky system; Expensive; Possible disturbance by injuries. |
| Face | Inexpensive; Compact; Good acceptability. | Identical twins; Psychology; Vulnerability to attacks. |
| Retina | Reliability, Durability. | Expensive; Low acceptability. |
| Iris | Reliability; Durability. | Expensive; Low acceptability; Acquisition constraints. |
| Voice | Ease. | Vulnerability to attacks. |
| Signature | Ergonomics. | Psychology; Depends on the reliability of the signature. |
| Keyboard strike | Ergonomics. | Physical and psychic state. |

Among the performance indices used to judge the effectiveness of a modality, the FAR and FRR rates (previously described) are used (Table 2) [14].

TABLE II.
COMPARISON OF THE 4 MAJOR BIOMETRIC MODALITIES
\

| Biometric Modality | FAR (%) | FRR (%) |
|---|---|---|
| **Iris** | 0.00129 | 0.583 |
| **Digital print** | 0.01 | 2.54 |
| **Geometry of the hand** | 0.05 | 7.29 |
| **Face** | 1 | 10 |

The physical and behavioural characteristics used by current biometric modalities are not always 100% reliable. For example, fingerprint recognition is far from perfect and accurate. It can be attacked by a thin layer of silicone reproducing geometry and fingerprints. Similarly, users who do not have fairly good fingerprints may not be correctly identified. In addition, the quality of fingerprints can be degraded over time, especially for people with manual activities. The recognition of the geometry of the hand also suffers from the same types of disadvantages as in the case of fingerprint recognition, especially among people of the same family and more particularly in twins. For facial recognition biometric systems, voice, or iris, many problems related to attacks are known (e.g. acquisition conditions, recorded voice attack, static or dynamic photography attack, etc.) [15].

## II. Applications of Biometrics

Authentication through biometrics is used in all areas requiring controlled access such as banking applications, highly secure locations such as government offices, parliament, army, security service, etc. As for recognition, it is often used by the police and immigration services at airports, as well as in the search for criminal databases. It is also found in civilian applications where the authentication of credit cards, driver's licenses and passports is becoming more common.

With the advent of the internet and its popularization and with the development of the various services and especially with the emergence of electronic commerce (E-commerce), all the suppliers of products and services are making considerable efforts to secure against all possible fraudulent intrusions.

Here is a non-exhaustive list of applications that can use biometrics to control access:

- Physical access control to the premises: Computer room, sensitive site (research service, nuclear site, military bases etc.).
- Logical access control to information systems: Launch of the operating system, access to the computer network, e-commerce, transaction (financial for banks, data between companies), and all software using a password.
- Communication equipment: Internet access terminals, mobile phones.

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

**International Journal of Digital Application & Contemporary Research**
**Website: www.ijdacr.com (Volume 6, Issue 8, March 2018)**

- Various Machines & Equipment: Safe with electronic lock, ATM machine, club membership check, loyalty card, time management and control, car (anti-start), etc.

## III. LIMITATIONS OF UNIMODAL BIOMETRIC SYSTEMS

The successful installation of biometric systems in various civil applications does not imply that biometrics is a fully resolved problem. It is clear that there are many possibilities for improvement in biometrics. Researchers are not only addressing the problems of reducing error rates, but they are trying to look at other ways to improve the profitability of biometric systems. Biometric systems that operate using any feature alone (single-mode biometric systems) have the following limitations [16]:

Noise on the captured data: Captured data may be noisy or damaged. A fingerprint with a scar or a cold-modified voice (cold) are examples of noisy data. They could also be the result of a faulty or poorly maintained sensor (for example: accumulation of dirt on the fingerprint sensor). The noisy data may be incorrectly compared with the database models [17] resulting in incorrect user rejection.

## IV. MULTIMODALITY

Multimodality [18] is the use of several biometric systems. The combination of several systems aims to reduce the limitations seen previously. Indeed, the use of several systems is primarily intended to improve recognition performance. By increasing the amount of discriminant information of each person, it is desired to increase the recognition power of the system. Moreover, the fact of using several biometric modalities reduces the risk of impossibility of registration as well as the robustness to fraud.

### A. *The different multi-possibilities:*

Multimodal biometric systems reduce the constraints of single-mode biometric systems by combining several systems. Five types of multimodal systems can be differentiated according to the systems they combine; we call them [19]:

1. Multi-sensors: when they combine several sensors to acquire the same modality, for example an optical sensor and a capacitive sensor for the acquisition of the fingerprint.
2. Multi-instances: when they associate several instances of the same biometry, for example the acquisition of several face images with changes of pose, expression or illumination.
3. Multi-algorithms: when several algorithms process the same acquired image, this multiplicity of algorithms can intervene in the extraction module by considering several sets of characteristics and / or in the comparison module by using several comparison algorithms.
4. Multi-samples: when they combine several different samples of the same modality, for example two fingerprints of different fingers or both irises. In this case, the data are processed by the same algorithm but require different references to the record, unlike multi-instance systems that require only one reference.
5. Multi-Biometrics: when considering several different biometrics, for example face and fingerprint.

A multimodal system can of course combine these different types of associations, for example the use of the face and the impression but using several fingers.

All these types of systems can overcome different problems and each have their advantages and disadvantages. The first four systems combine information from one and the same modality, which does not address the problem of the non-universality of certain biometrics and the resistance to fraud, unlike "multimodal biometrics" systems [20].

In fact, systems combining several pieces of information from the same biometry make it possible to improve recognition performance by reducing the effect of intra-class variability. But they do not allow to deal effectively with all the problems of unimodal systems. For this reason, multi-biomechanical systems have received a lot of attention from researchers.

## V. PERFORMANCE EVALUATION

To implement an automatic recognition system, mechanisms are needed to evaluate the goodness and capacity of the system. Quantifying the error that the system produces will help to its developer to improve it and compare it with others already implemented.

A recognition system captures a biometric feature, extracts its characteristics and forms a model which compares with another or others to evaluate whether or not they belong to the same person. In this way, biometric features of different people are required to be very different and that models generated from the biometric feature from the same person are very similar. However, there are factors that decrease inter-class variation and that increase variation intra-class, leading to errors in recognition. For example, a user who interacts with the sensor in a different way or that experiences behavioural or physiological changes can make the system generate very different models from the same biometric feature, increasing intra-class variation.

Our goal is to offer a multimodal biometric system while respecting several constraints of comfort [28] and reliability (Increase the rate of recognition, inexpensive calculation, robustness). In this context, the merger allows fill the lack of information that results from the use of a single modality.

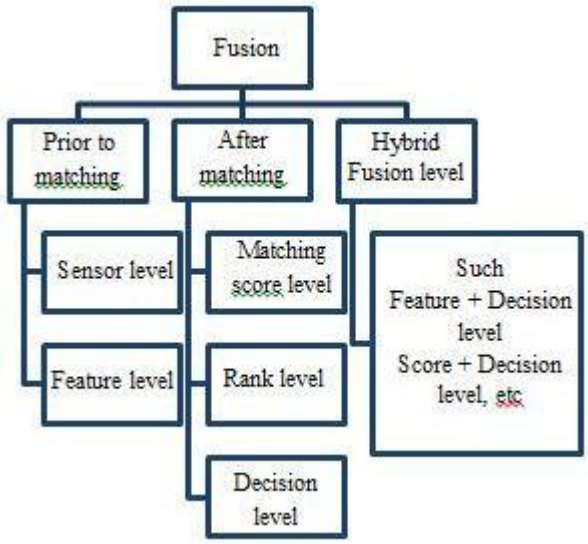


Figure 2. Categories of different fusion levels

IJDACR
ISSN: 2319-4863

IJDACR
International Journal Of Digital Application & Contemporary Research

**International Journal of Digital Application & Contemporary Research**
**Website: www.ijdacr.com (Volume 6, Issue 8, March 2018)**

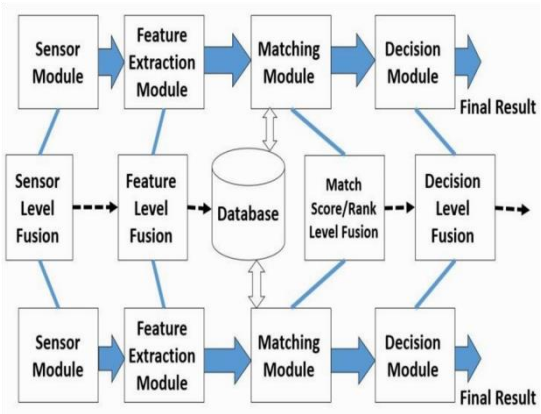


Figure 3. Prior to Matching and after matching fusion levels

In this article we propose an adaptive system of recognition of individuals by the fusion of three biometric modalities: fingerprint, face, geometry of the hand. Let's treat each modality separately with two types of classifiers: the neural classifier MLP and SVMs, and then compare the results.

In the following sections, we will detail the steps of pre-processing and classification for each modality, and then we will present the experimental results and discuss our prospects for work.

TABLE III.
EXAMPLES OF PREVIOUS RESEARCH BASED DIFFERENT FUSION IN DIFFERENT LEVELS

| Year | Modalities fused | Authors | Fusion Level | Fusion Approach | Performance in percentage |
|---|---|---|---|---|---|
| **2004** | Fingerprint + Face | Kalyan, et al.[24] | Score + Decision | Sum Rule and Likelihoods | 58.33% improvement with correlation 0.9 and (sum rule, PSO)=(0.0324,0.0135) % |
| **2011** | Face + Palm print | Linin Shen [25] | Feature+ Decision | FPCODE | Feature level fusion : 91.52 % Decision level fusion : 91.63% |
| **2013** | Face + Ear | S.M.S. Islam[26] | Feature + Score | L3DF, Iterative closet point | FAR = 0.001 % Recognition: 96.8 % Verification: 97.1 % |
| **2014** | Face + Fingerprint + Iris | A. Annis Fathima et al. [27] | Score + Dynamic decision | Weighted average Fusion and K-NN | Recognition Rate = 78.55% (Iris + Face) = 85 % |

## VI. CONCLUSIONS

The ability and security in methods of identifying people have become in a key need in the interconnected society in which we live. Faced with this need, automatic biometric recognition systems have been replacing, every time faster since the last decades, to traditional identification systems (based on Identification cards or keys). The use of the palmar fingerprint as a biometric feature presents certain advantages (universality, high social acceptance, ease of use, etc.) compared to others traits; which are very useful in certain applications, such as the controls of access. In this project the design and implementation of a biometric system of recognition based on images of palm prints.

This study allowed us to validate the feasibility of a biometric system multimodal by merging three biometric modalities the fingerprint, the geometry of the hand, the face. The treatments developed respect the constraints low computational cost with both SVM and MLP classifiers (table 2 and table 3) Using these programs is all about selecting a good family of core functions and to adjust the parameters of these functions. The obtained results by an SVM classifier are better by comparing with an MLP classifier, but it is faster in computation time the merger confirms that the systems multimodal are more efficient unimodal. As prospects the use of the Biometric multimodal database [28] made up of 130 different ones within the Getbiomet project, as well as test other fusion methods

Biometrics is an expanding field with a growing body of research that aims to achieve an effective, reliable and timely way of identifying people. The two proposed biometric modalities are the iris and the fingerprint.

In this paper, we presented the process of identifying individuals by multimodal biometrics. Our main goal is to implement a multimodal biometric system for the identification of individuals where information from both biometric scores (iris and fingerprint) are combined.

In order to achieve this goal, our work has been carried out in several stages presented throughout this document:

After introducing the general concepts in biometrics, we have detailed the different levels and techniques of possible mergers in a multimodal biometric system, presented a state of the art in recognition of the iris and in recognition of the fingerprint.

At the end of this work, we have seen that: The quality of a unimodal identification system depends on several parameters (the capture environment, the behavioural variability according to individuals, etc.) which hinder the proper functioning of the latter. However, we can make the performance of the biometric system reliable by simultaneously using several different modalities.

The multimodal recognition process improves the performance of single-mode systems. Indeed, the tests that we carried out showed the interest of the fusion at the level of the scores.

The performance of the score fusion system can be degraded by the weakness of one of the unimodal systems. In general, to increase the performance of the system it is necessary to merge modalities with similar performances.

The integration of the data at the level of the correspondence scores by the weighted sum method gives the best result and makes it possible to significantly improve the performance of the multimodal system.

It would also be interesting to study other fingerprint recognition and iris recognition and combination techniques using other multilevel information classification and fusion methods.

IJDACR
International Journal Of Digital Application & Contemporary Research

**International Journal of Digital Application & Contemporary Research**
**Website: www.ijdacr.com (Volume 6, Issue 8, March 2018)**

REFERENCES:

[1] Ding, C., Choi, J., Tao, D. and Davis, L.S., 2016. Multi-directional multi-level dual-cross patterns for robust face recognition. *IEEE transactions on pattern analysis and machine intelligence*, *38*(3), pp.518-531

[2] Allyn, M.A., Intel Corp, 2018. *Authenticity-assured data gathering apparatus and method*. U.S. Patent 9,881,184.

[3] Zhang, H., Patel, V.M. and Chellappa, R., 2015, September. Multitask multivariate common sparse representations for robust multimodal biometrics recognition. In *Image Processing (ICIP), 2015 IEEE International Conference on* (pp. 202-206). IEEE.

[4] Shekhar, S., Patel, V.M., Nasrabadi, N.M. and Chellappa, R., 2014. Joint sparse representation for robust multimodal biometrics recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *36*(1), pp.113-126.

[5] Dhouib, M. and Masmoudi, S., 2016. Advanced Multimodal Fusion for Biometric Recognition System based on Performance Comparison of SVM and ANN Techniques. *International Journal of Computer Applications*, *148*(11).

[6] Lumini, A. and Nanni, L., 2017. Overview of the combination of biometric matchers. *Information Fusion*, *33*, pp.71-85.

[7] Ghayoumi, M., 2015, June. A review of multimodal biometric systems: Fusion methods and their applications. In *Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on* (pp. 131-136). IEEE.

[8] Li, S.Z. and Jain, A., 2015. *Encyclopedia of biometrics*. Springer Publishing Company, Incorporated.

[9] Song, X., Langenbucher, A., Gatzioufas, Z., Seitz, B. and El-Husseiny, M., 2014. Effect of biometric characteristics on the change of biomechanical properties of the human cornea due to cataract surgery. *BioMed research international*, *2014*.

[10] Ghayoumi, M., 2015, June. A review of multimodal biometric systems: Fusion methods and their applications. In *Computer and Information Science (ICIS), 2015 IEEE/ACIS 14th International Conference on* (pp. 131-136). IEEE.

[11] Saini, R. and Rana, N., 2014. Comparison of various biometric methods. *International Journal of Advances in Science and Technology*, *2*(1), pp.24-30.

[12] Cheng, K.P., Chang, E.Y. and Wang, Y.F., Proximex Corp, 2015. *Adaptive multi-modal integrated biometric identification detection and surveillance systems*. U.S. Patent 8,976,237.

[13] Vasiete, E., Chen, Y., Char, I., Yeh, T., Patel, V., Davis, L. and Chellappa, R., 2014, September. Toward a non-intrusive, physio-behavioral biometric for smartphones. In *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services* (pp. 501-506). ACM.

[14] M. Monwar, "*A Multimodal Biometric System Based on Rank Level Fusion,*" PhD, Department of Computer Science University of Calgary, ALBERTA 2012.

[15] S. A. S. DzatiAthiarRamli, AiniHussain, "*A Multibiometric Speaker Authentication System with SVM Audio Reliability Indicator*," International Journal of Computer Science & Information Technologies (IAENG), vol. 36, no. 4, pp. 313-321, 2008.

[16] S. K. Grewal, "*A Composite Approach for Biometric Template Security*," International Journal and Conference Service Center (IJCSC), vol. 5, no. 1, pp. 170-176, 2014.

[17] I. A. Saleh and L. M. Alzoubiady, "*Decision Level Fusion of Iris and Signature Biometrics for Personal Identification using Ant Colony Optimization*," International Journal of Engineering and Innovative Technology (IJEIT), vol. 3, no. 11, pp. 35-42, 2014.

[18] A. Naghate, M. Sahu, P. Bhange, S. Lonkar, P. Wankhede, and Y. Bute, *"Implementation of Multibiometric System Using Iris and Thumb Recognition,"* International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 3, no. 3, pp. 932 – 940, 2014.

[19] C. Lupu and V. Lupu, "Multimodal Biometrics for Access Control in An Intelligent Car," presented at the Computational Intelligence and Intelligent Informatics, 2007. ISCIII'07. International Symposium on, Agadir, 2007. pp. 261-267.

[20] A. C. Panda, *"Parallel Algorithms for Iris Biometrics," M.Sc., Department of Computer Science and Engineering"*, National Institute of Technology Rourkela, Odisha, India, 2011.

[21] K. Veeramachaneni, L. Osadciw, A. Ross, and N. Srinivas, *"DecisionLevel Fusion Strategies for Correlated Biometric Classifiers,"* presented at the Computer Vision and Pattern Recognition Workshops, 2008. CVPRW'08. IEEE Computer Society Conference on, Anchorage, AK 2008. pp. 1-6.

[22] L. Shen, L. Bai, and Z. Ji, *"FPCODE: An Efficient Approach for MultiModal Biometrics,"* International Journal of Pattern Recognition and Artificial Intelligence, vol. 25, no. 02, pp. 273-286, 2011.

[23] S. M. Islam, R. Davies, M. Bennamoun, R. A. Owens, and A. S. Mian, *"Multibiometric Human Recognition Using 3D Ear and Face Features,"* Pattern Recognition, vol. 46, no. 3, pp. 613-627, 2013.

[24] W. Almayyan, *"Performance Analysis of Multimodal Biometric Fusion,"* PhD, Faculty of Technology, De Montfort University, England, United Kingdom, 2012.

[25] A. A. Fathima, S. Vasuhi, N. N. Babu, V. Vaidehi, and T. M. Treesa,*"Fusion Framework for Multimodal Biometric Person Authentication System,"* IAENG International Journal of Computer Science, vol. 41, no. 1, pp. 1-14, 2014.

[26] J. Galbally, S. Marcel, and J. Fierrez, *"Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition,"* IEEE Transactions on Image Processing, , vol. 23, no. 2, pp. 710-724, 2014.

[27] V. SIREESHA and K. SANDHYARANI, *"Multimodal Biometric System Using Iris-Fingerprint: An Overview,"* International Journal of Engineering Sciences Research-IJESR, vol. 02, no. Special Issue 01, pp. 1342-1349, 2013.

[28] A. A. Albahdal and T. E. Boult, *"Problems and Promises of Using the Cloud and Biometrics,"* presented at the 11th International Conference on Information Technology: New Generations (ITNG) 2014, 2014. pp. 293300.