Identification of a Standardized Automobile Bio-metric Security System based on Accuracy and Response time: Applicable for the Indian Automobile Market

Subhranil Ganguly, Kirubanand V.B

Abstract: ***This paper aims at the identification of a standard security system for commercial and personal vehicles installed on a remote-controlled unlocking device that promises a high accuracy without compromising on the response time. The proposed technology combines three bio-metric security systems on the basis of their performance and response times to make vehicles more secured. The paper compares the efficiencies of different bio-metric security systems based upon their mean accuracy and response times. Primary data have been collected using existing devices and technology, a detailed statistical comparison is done using computational tools like IBM SPSS 2.0 and Microsoft Excel using statistical concepts like ANOVA, Square of means, Descriptive statistics, Central tendencies, etc. The hardware required for this proposed security system is already available at reasonable cost and can be implemented in the field of automobile and a standard security system can be identified for use across all variants of vehicles universally for all the manufacturers. The performance of the bio-metric devices was measured using a 16-megapixel Sony camera IMX371 Exmor RS sensor with a pixel size of 1.0 micro-meter, mounted on a OnePlus 5T mobile phone for face recognition and a fingerprint sensor with a claimed unlock speed of 0.2 seconds mounted on the same device. Mantra MI S100 single iris scanner was used with a high-resolution sensor (CMOS) and captures images with a JPEG2000 compression format.***

Keywords: ***Automobile Security, Bio-metric ID, Accuracy, Response Time, Descriptive Statistics***

I. INTRODUCTION

Automobile industry in India is considered to be one of the largest in the world in terms of passenger-vehicle market size. The country is expected to hit its milestone of five million annual automobile production in the next five years. As per the economic trends, in the near future majority of the people will become a part of the workforce. As a result, there will be a significant rise in the number of households owning a personal car. India has been the breeding ground of small passenger vehicles and hatchbacks since ages mainly because of lack of space in the cities coupled with narrow roads. The demand for low budget cars is ever increasing.

The car manufactures tend to compromise on the security features in their cars in order to reduce the production cost. Modern cars on the other hand are equipped with smart features such as navigation, entertainment system, etc which contain personal information about the users such as entertainment preferences, location information, personal identification, etc. There should not be a trade-off between cost and security [9]. In India there is an absence of a standardized security protocol when automobiles are considered. The car manufacturers tend to put more emphasis on security systems in the high-priced cars and they have a general tendency to neglect such security measures in low-cost cars. There is an immediate need for a standard security protocol to be followed by all the car manufacturers across all the car segments [10].

II. RELATED WORKS

A. Face Recognition

Face recognition is a computerized technology that recognizes a human face by matching the facial features of the captured image with the target. This technology is used mainly in security and surveillance systems meant for securing sensitive and confidential information like banks, houses, automobiles, government properties, etc. The face recognition technology gained importance in the recent times because of its adoption by the mobile phone manufacturing companies. People gained trust on this technology as it became easily accessible for the general public via mobile phones. There are a lot of face recognition systems available currently based upon various technologies or algorithms such as Eigenfaces [1], recognition systems that employ the SIFT technology [2], there are face sensors available based on the HOG and LBP [3] technologies as well.

B. Fingerprint ID

Fingerprint identification is one of the most reliable and full-proof methods for bio-metric authorization [8]. The technology matches a captured impression of an individual's finger's minute ridges, known as dermal. For an individual, the pattern of one's finger's ridges and valleys are absolutely unique and unmodifiable. Nowadays optical fingerprint sensors are used in addition to thermal, silicon and ultrasound sensors to capture the image of one's dermal. Minutiae and pattern matching algorithms are widely used to develop fingerprint recognition systems [4]. The pattern matching algorithms

Revised Manuscript Received on July 05, 2019

Subhranil Ganguly, Christ (Deemed to be University), Bengaluru, Karnataka, India

Kirubanand VB, Christ (Deemed to be University), Bengaluru, Karnataka, India

Retrieval Number: F3573048619/19©BEIESP
DOI: 10.35940/ijitee.F3573.078919

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication

just match the sensor-captured pattern with the target pattern already saved in the device memory or in a certain database while the minutiae algorithms rely on the direction and locations of each minutiae points.

C.Iris Recognition

Iris recognition systems recognizes the uniqueness in a human eye image in order to identify an individual. There are three primary stages in an iris recognition process namely, Pre-processing, Feature Extraction and Recognition stages. The first or the pre-processing state determines the boundaries of the iris from the eye image to facilitate processing [7]. The second step comprises of processing the image data. The third or the recognition state uses the processed data to match the extracted features with the saved or the target datasets and ends with a conclusion. In the recognition stage, techniques like Hamming Distance, Learning Vector Quantization and Probabilistic Neural networks are used to match the captured image with other feature vectors in the widely available commercial systems which exhibit high efficiency [5].

III. STATISTICAL MEASURES

Analysis of Variance

Analysis of Variance is used to determine and analyse the differences between groups of samples. It provides a test (statistical) inferring whether the mean population of several groups of samples differ from each other. It is most commonly used in the analysis of experimental datasets in numerous fields. Traditional statistical terminologies are used by ANOVA, sample variance can be defined mathematically as;

$$S^2 = \frac{1}{n-1}\sum (y_i - \bar{y})^2$$

F-test

F-test is the principal comparison factor, it compares the total deviation among the groups of population samples. In one-way ANOVA statistical conclusion is drawn from the results of the F-test statistics comparisons. The F-test can be statistically defined as:

$$F = \frac{variance\ between\ tratments}{variance\ within\ treatments}$$

$$F = \frac{MS_{Treatments}}{MS_{Error}} = \frac{SS_{Treatments}/(I-1)}{SS_{Error}/(n_T - I)}$$

MS = Mean Square,
I = the number of treatments,
nT = Total cases

Standard Deviation

Standard deviation or sigma is a statistical measure that quantifies the deviation or variation of a set of values from their respective means. Standard deviation is a measure of confidence level of datasets for mathematical or statistic conclusions. In this paper standard deviation is used to measure the confidence level of accuracies of the bio-metric models. A model with low standard deviation will have a high level of accuracy and vice-versa. Standard deviation is calculated using the formula:

$$s = \sqrt{\frac{\sum_{i=1}^{N}(x_i - \bar{x})^2}{N-1}}$$

Where, {*x1,x2,x3,……xn*} = values of samples,

x̅ = mean of the samples

N = total number of observations

IV. ANALYSIS

The mean accuracy and mean response time of each of the three bio-metric security systems were calculated and compared using the above formulae and concepts. The three technologies considered are:

- Face Recognition
- Fingerprint ID
- Iris Recognition

These parameters are studied for the given technologies to identify a standard automobile security protocol that is both accurate and fast. This standard system can be made as a protocol that is to be followed by automobile manufacturers in India for enhanced safety and security in the vehicles. All the datasets were generating using devices available in the market, developed using existing technologies as given below:

Face recognition sensor - 16-megapixel Sony camera IMX371 Exmor RS sensor with a pixel size of 1.0 micro-meter.

Fingerprint sensor - Claimed unlock speed of 0.2 seconds mounted on a OnePlus 5T mobile phone device.

Iris sensor - Mantra MI S100 single iris scanner was used with a high-resolution sensor (CMOS).

1. Mean Accuracy:

The mean accuracy of all the three systems are calculated using primary data. A dataset of 100 entries are collected using different inputs from different individuals. Accuracy is measured on the basis of the robustness of the sensors in case of false and true inputs.

Based on the Means, Standard deviations and Standard Error the False Positive Rate or FPR is calculated for every sensor using the formula:

$$\frac{FP}{N} = \frac{FP}{FP+TN}$$

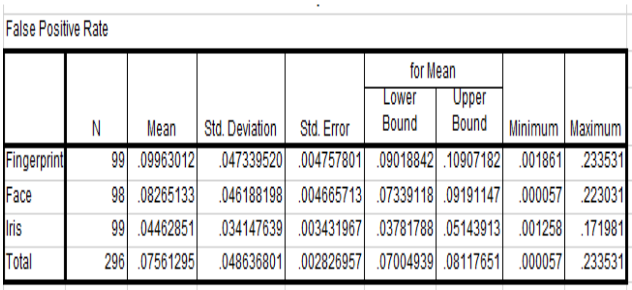
Where,

FP = total false positives

NT = total true negatives

N = total negatives.

Descriptive variables:

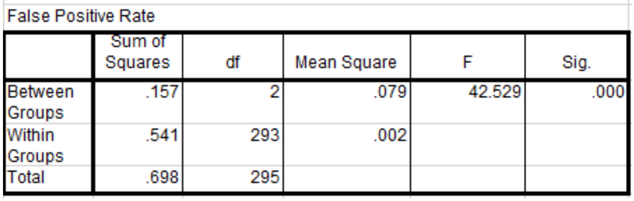


False Positive Rate

	N	Mean	Std. Deviation	Std. Error	for Mean Lower Bound	 Upper Bound	Minimum	Maximum
Fingerprint	99	.09963012	.047339520	.004757801	.09018842	.10907182	.001861	.233531
Face	98	.08265133	.046188198	.004665713	.07339118	.09191147	.000057	.223031
Iris	99	.04462851	.034147639	.003431967	.03781788	.05143913	.001258	.171981
Total	296	.07561295	.048636801	.002826957	.07004939	.08117651	.000057	.233531

Table 1

ANOVA:



False Positive Rate

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	.157	2	.079	42.529	.000
Within Groups	.541	293	.002		
Total	.698	295			

Table 2

df = Degree of freedom

Sig = Significance (p-value)
F = F-test value
Null Hypothesis (H0): All means are equal.
Alternate Hypothesis (H1): All means are unequal.

Since, p value is less than 0.05, Null Hypothesis is rejected. So, there is a significant difference between the mean accuracies in percentage.

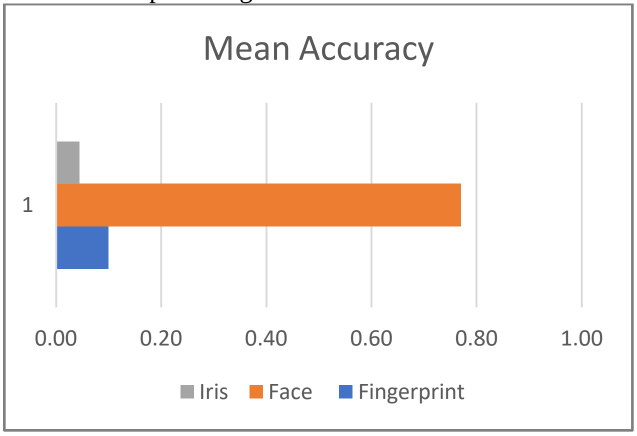
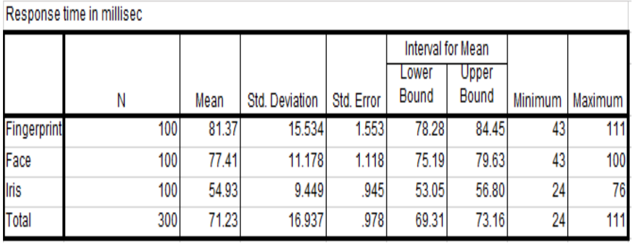


Fig. 1 Mean Accuracy

The above results are calculated using the IBM SPSS 2.0 Statistical tool along with Microsoft Excel Descriptive Statistics package.From the above results we can conclude that Face recognition can be used as a standard bio-metric device for automobile security standards based upon its accuracy. But to have an efficient security system we cannot only emphasize on accuracy as response time or speed of operation plays as important role in determining the overall acceptance of a technology. The following results are derived on running various statistical measures on the primary data collected from the above-mentioned sensors.

2. Mean Response Time

Response time is a measure of how many units of time is taken for a system to service a particular request, in this case it is defined as the amount of time required for the bio-metric system to come to a conclusion whether to authorize an individual or not when it receives a request from a user.
Mean response time of each of the system is calculated statistically using a dataset generated from primary data.
Descriptive Variables:

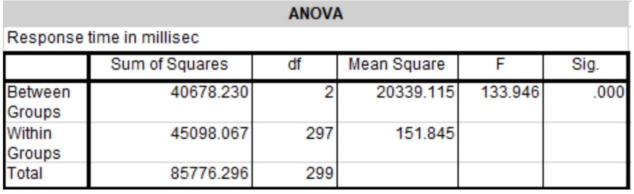


Response time in millisec

	N	Mean	Std. Deviation	Std. Error	Interval for Mean Lower Bound	 Upper Bound	Minimum	Maximum
Fingerprint	100	81.37	15.534	1.553	78.28	84.45	43	111
Face	100	77.41	11.178	1.118	75.19	79.63	43	100
Iris	100	54.93	9.449	.945	53.05	56.80	24	76
Total	300	71.23	16.937	.978	69.31	73.16	24	111

Table 3

ANOVA:



ANOVA

Response time in millisec

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	40678.230	2	20339.115	133.946	.000
Within Groups	45098.067	297	151.845		
Total	85776.296	299			

Table 4

df = Degree of freedom
Sig = Significance (p-value)
F = F-test value
Null Hypothesis (H0): All means are equal.
Alternate Hypothesis (H1): All means are unequal.
Since, p value is less than 0.05, Null Hypothesis is rejected. So, there is a significant difference between the mean response times in milliseconds.

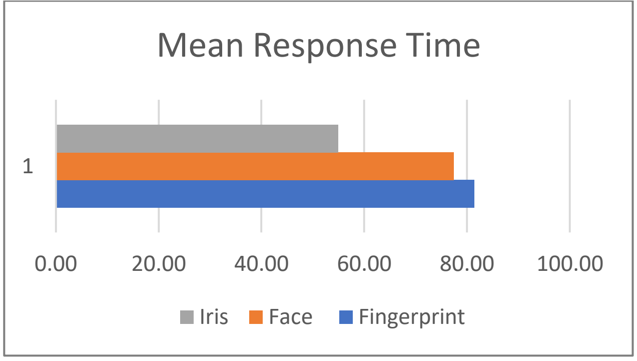


Fig. 2 Mean Response

The above results are calculated using the IBM SPSS 2.0 Statistical tool along with Microsoft Excel Descriptive Statistics package.

Retrieval Number: F3573048619/19©BEIESP
DOI: 10.35940/ijitee.F3573.078919

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication

Result Table

Technologies	Mean Accuracy (%)	Mean Response Time (msec)
Face recognition	0.78 ~ 78%	78
Fingerprint ID	0.1 ~ 10%	81
Iris recognition	0.02 ~ 2%	56

Table 5

V.CONCLUSION

A comparison of efficiencies from the result table on the three bio-metric systems show that Face recognition has the highest accuracy and Iris recognition devices have the lowest response time. So, on combining the two results we can conclude that an automobile bio-metric system having a combination of high accuracy and very low response time can be a standard protocol to be followed by every car manufacturer across all their car variants in India.

REFERENCES

1. M. Turk, A. Pentland. Eigenfaces for recognition. Journal of Cognitive Neuroscience. 1991,3(1):71-86.
2. D. G. Lowe. Distinctive image features from scale-invariant key points. International Journal of Computer Vision, 2004,60(2): 91-110.
3. N. Dalal, B. Triggs, Histograms of Oriented Gradients for Human Detection. Los Alamitos: IEEE Computer Society Press, 2005,1886-893.
4. Y. J. Wang and K. N. Plataniotis, ―An analysis of random projection for changeable and privacy-preserving biometric verification, ‖ IEEE Transactions on Systems, MAN and Cybernetics — PART B: CYBERNETICS, vol. 40, no. 5, Oct. 2010.
5. D. Lauber, "Biometrics: A Brief Overview" SANS Institute 2003.
6. https://www.mckinsey.com/industries/
7. S. S. Patil, S. Gudasalamani, N. C. Iyer and V. G. Garagad, "Tilt and scale invariant iris recognition system," *2016 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC)*, Bangalore, 2016, pp. 1-6. doi: 10.1109/ICCTAC.2016.7567342.
8. (2019). Biometric human recognition system based on ECG. Multimedia Tools and Applications. 1-18. 10.1007/s11042-019-7152-0.
9. Prasad Agrawal, Mukesh & Ram Gupta, Atma. (2019). TRAX: Smart Mobile Application to Improve the Safety and Security of Automobile Vehicles: Proceedings of ICICC 2018, Volume 1. 10.1007/978-981-13-2324-9_19.
10. Yi Chai, Nan Li and Mao Yun Quo, "Intelligent security system for automobile based on multi-agent dynamic information processing," *Fifth World Congress on Intelligent Control and Automation (IEEE Cat. No.04EX788)*, Hangzhou, China, 2004, pp. 3079-3082 Vol.4.