ISSN 2347 - 3983

Volume 7, No. 12 December 2019

International Journal of Emerging Trends in Engineering Research

Available Online at http://www.warse.org/IJETER/static/pdf/file/ijeter147122019.pdf

https://doi.org/10.30534/ijeter/2019/147122019

System of Individual Multidimensional Biometric Authentication

Barkovska Olesia[1], Movsesian Iana[2], Yeromina Nataliia[3], Liashenko Oleksii[4], Tkachenko Danyil[5]

[1,2,3,4,5]Kharkiv National University of Radio Electronics, Ukraine, Kharkiv, 61166,
Nauki ave., 14, d_ec@nure.ua

ABSTRACT

The article is devoted to solving the problem of multidimensional biometric authentication on the base of combination of several biometric indicators - fingerprints, facial geometry and voice. The indicators applied in the proposed system are the most accessible source of biometric credentials as well as provides for the compliance to such requirements to identification and authentication systems as noninvasive data acquisition for the analysis, relative inexpensiveness and compactness / portability of the system under development. The proposed approach implemented in the hardware and software suite described in the work has an advantage over the existing unifactorial biometric authentication approaches by such indicators as FRR and FAR and is also easy in use. The result of the proposed individual multidimensional biometric authentication system is the increase in overall reliability compared to the separate use of the current methods as well as a relatively small increase in the system response delivery time (from data input in the system to namely identification).

Key words: biometric technologies, authentication, indicators, fingerprints, facial geometry, human voice, false acceptance rate, false rejection rate, multidimensional, microcomputer.

1. INTRODUCTION

The market volume of biometric systems, which utilize biometric identification along with authentication, experiences sustainable growth and development. The examples may be security systems at government bodies, banking institutions, private companies as well as airports, railway stations and subway, the functioning of which is based on processing biometric data for making various decisions (Figure 1). In access authority systems, which are used to gain access to the secured area, the application of biometric data enables to improve the level of security of the secured area as well as provide for the ease of gaining access to the secured area. In perimeter rove systems, which are used for security service personnel identification during the perimeter rove along the designated route at the scheduled time, the application of biometric data enables to improve discipline. In work time logging systems, which are used for confirmation of the time spent on the territory, the application of biometrics enables to enhance the personnel work time logging data reliability at the enterprise as well as improve discipline. In video recognition surveillance systems, which are used to identify individuals in public places on the basis of a certain database, application of biometrics enables to calculate the amount of people in public places as well as gives the possibility to identify criminal elements, reduces the threat of public disorders and terrorist acts.

The described systems use the methods of individual biometric verification and identification, which are based on the unique human biological characteristics (HBC) [1, 2], which can be classified into two big subgroups – statistical (fingerprints, facial geometry, palm geometry, palm vein pattern, eye retina, DNA), and dynamic (signature, voice, tenue, typing speed and strength, handwriting, cardiac rhythm) (Figure 2) [3].

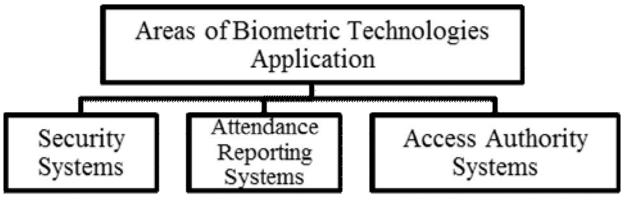
Areas of Biometric Technologies Application
Security Systems
Attendance Reporting Systems
Access Authority Systems

Figure 1: Areas of Biometric Technologies Application

The main requirements to the MBA systems are:

– authenticity (generalizes factors, which show the degree of simplicity of deceiving the biometric identifier (tolerance to fraudulent alteration), how tolerant the system performance is in various external environments such as change of indoor lighting or temperature, tolerance to the environment);

– result generation speed;

– noninvasive data acquisition for the analysis (the degree of complexity of biometric sensor application).

The supplementary requirements may include:

– relative inexpensiveness;
– system versatility;
– compactness / portability.

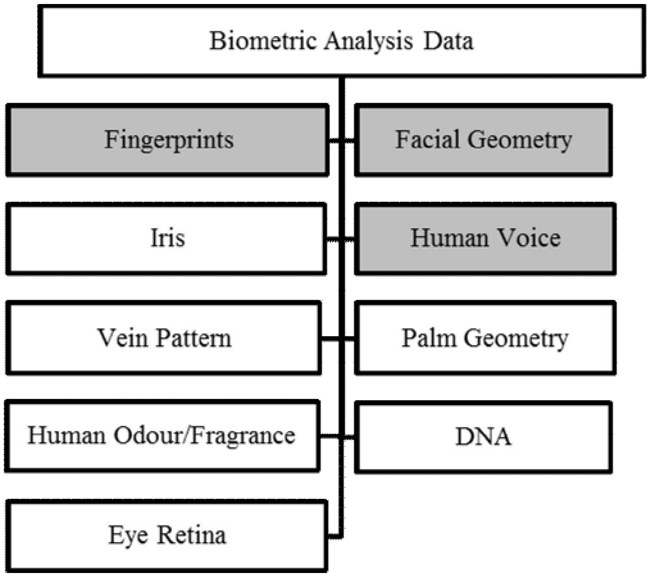

Figure 2: Used HBCs

In order to evaluate HBC-based authentication methods the requirement of biometric system performance validity, which refers to type 1 errors (FRR - False Rejection Rate – target dropout – shows access denial probability for authorized users – the system denies access for authorized users) and type 2 errors (FAR - False Acceptance Rate – false alert – shows false biometric characteristics coincidence probability for two individuals – the system takes one person for another by mistake) (Table 1) are used along with the requirement for authentication data acquisition.

Subjective attributes for the selection of factors for biometric authentication system formation may include the following characteristics:
- fingerprint identification method is characterized by the low cost of fingerprint scanning devices, simple fingerprint scanning procedure. The shortcomings of the given method include the fact that papillary picture lines are easily damaged by minor scratches, cuts, and impact of chemical reagents;
- facial geometry identification method is characterized by the possibility to record undercover videos of faces in public places; the use of inexpensive equipment is possible (however, the possibility to recognize faces at big distances from the camera is only provided by expensive analogs). The drawbacks of the given method include severe requirements to lighting; impact of external interference – presence of glasses, beards, hairstyle change, head rotation, frequent change of mimics – reduce the accuracy of authentication; low integrity in twins authentication;
- voice identification method is characterized by the ease of authentication data retrieval and low cost of sensors. However, the drawback is the indicator (voice) variability over extended periods of time (e.g., change of voice during catarrhal diseases); inability to identify numb people.

The analyses [4, 5, 6, 7] demonstrated that the systems, which use only one biometric indicator (e.g., facial geometry), do not provide for the high certainty of identification.

Table 1: Given HBC-Based Authentication Methods Evaluation

Biometric Indicator	Authenticity		Ease of Application
	FRR	FAR	
Facial Geometry	Around 6%	Around 0,1%	High
Fingerprints	Around 1%	Around 0,00002%	Medium
Voice	Around 3%	Around 0,1%	High
Iris	Around 0,2%	Around 0,0001%	Medium
Vein Pattern	Around 0,01%	Around 0,00008%	High

In cases when high certainty of identification is necessary, a combination of several biometric indicators is applied – individual multidimensional biometric authentication (MBA). An example of the given systems application is individuals behavioural analysis [8].

1.1 Research task rationale

Certainty of human identification is the crucial requirement to identification systems, which cannot be achieved by means of unifactor authentication, which is proved in [7]. Temporary damage or unavailability for scanning of certain biometric indicators can also be the reason for the switch to cross or hybrid biometric authentication systems in MBA systems enabling to generate the identifier and authenticate identity of the authorized user via integrating the individual's identification results against more than one indicator, which grounds the relevancy of the proposed MBA method, which is based on the conformance analysis of the static suite of indicators such as fingerprints, facial geometry, voice of the individual to be authenticated, provided by the user for the purpose of their verification. The indicators applied in the proposed system are the most accessible source of biometric credentials as well as provides for the compliance to such requirements to identification and authentication systems as noninvasive data acquisition for the analysis, relative inexpensiveness and compactness / portability of the system under development.

1.2 Aims and tasks of the work

The aim of the work is the development of multidimensional biometric authentication system. In order to achieve the set aims the following tasks must be accomplished:
- analysis of the basic methods for system multidimensional biometric authentication construction;

- comparative analysis of the existing multidimensional biometric authentication systems;
- development of individual multidimensional biometric authentication system;
- analysis of the obtained multidimensional biometric authentication results.

2. TASK FULFILLMENT

The multidimensional biometric authentication system proposed in the work is based on identification of the compliance of the static suite of three biometric indicators (fingerprints, facial geometry, voice) provided by the user with the available suite in the system database, for its verification. Combination of three biometric indicators enables to compensate for the drawbacks of some indicators with the advantages of other indicators and vice versa as well as enables to improve the certainty of identification. The abstract representation of the system is provided in Figure 3.

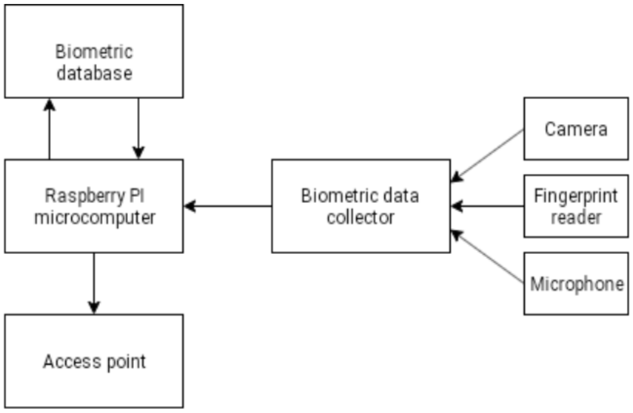

Figure 3: Abstract MBA System Representation

Biometric data obtained from a fingerprint scanner, a portable video camera and a microphone embedded in the camera are provided in order to gain access.

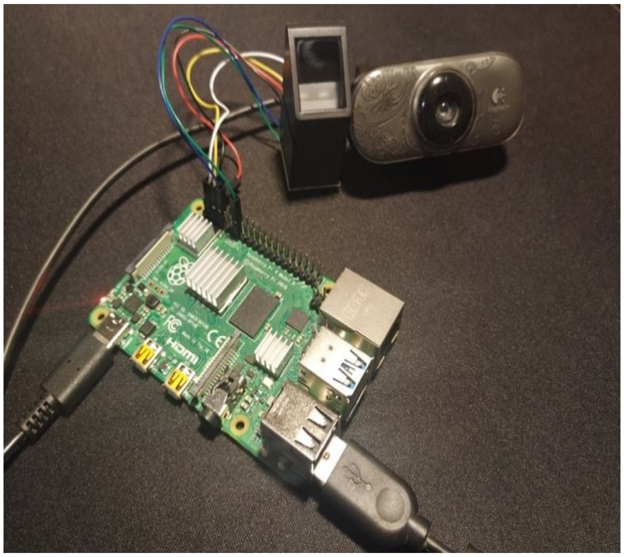

Figure 4: The Proposed MBA System Testing

At the test and operation phases, the proposed system has the form presented in Figure 4.

The proposed designed system is completely autonomous with the ability в battery supply on condition of supply in 5B 3A.
Network connection when in operation is not necessary because the database resides in the device. The software and the database are updated by means of connecting the workstation.

The designed MBA system has a small size: the system may be embedded in a 70x50x20mm case if a specialized camera module, a small-sized fingerprint scanner and a microphone are connected.

Due to the fact that the data obtained from sensors have a different nature – bidimensional grayscale face image and finger papillary picture as well as voice pattern, the algorithms plied in the preliminary and proper processing operations may vary.

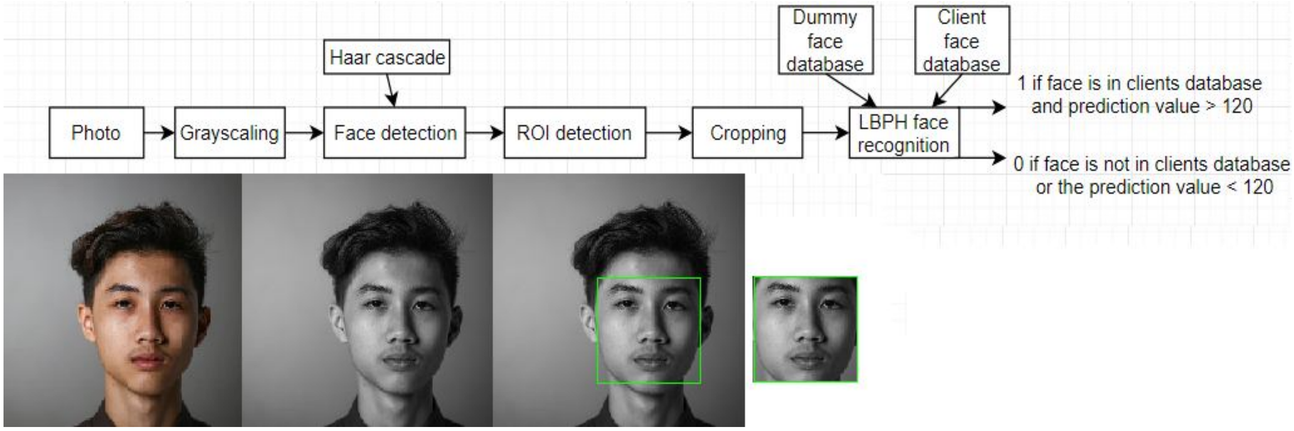
Dummy face database
Client face database
Haar cascade
1 if face is in clients database and prediction value > 120
Photo
Grayscaling
Face detection
ROI detection
Cropping
LBPH face recognition
0 if face is not in clients database or the prediction value < 120

Figure 5: Algorithm Applied in Photo-Fit Photographic Identification

Decision making concerning the bidimensional grayscale face image input in the MBA system is performed in compliance with the algorithm presented in Figure 5.

Among the existing face comparison methods, the following methods were regarded: LBPH, Fisherfaces and Eigenfaces. The LBPH method proved to be the most resilient (the algorithm is adaptable to various image sizes without any additional preprocessing stages), the least resource-consuming and the fastest. This method is also quite flexible, e.g. learning on the basis of this method does not require ROI face cropping, however, this is used, primarily, for reducing the size of the file for storing in a database and for obtaining a more uniform histogram.

LBPH is the method of image data retrieval by means of LBP (logical binary patterns) operation applied to the matrix built on the basis of the obtained image, and after the operation we have a new image consisting fully of binary data, and, by further dividing the resulting image into segments, histograms are built, which characterize the given image (Figure 6-7).

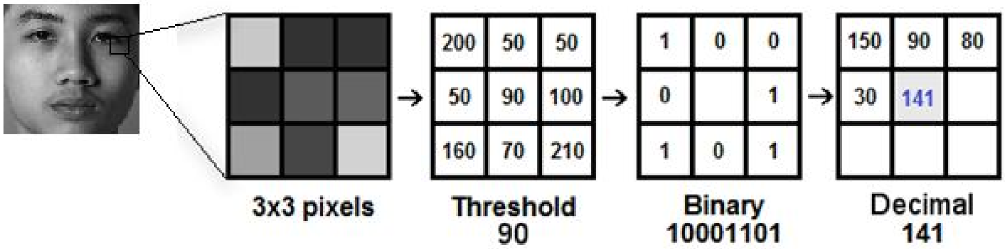

Figure 6: Application of LBP Operation to Image

An LBP operation refers to retrieving a binary matrix from a decimal one. Firstly, a reference matrix element is selected, the values of which are further compared with other elements around it with the radius and number of neighboring elements being variable and selected by the user, in the given example the number of such elements being 8, and after the operation a new value for the element is obtained. Methods of its obtaining may vary but the results will not differ dramatically, in the given example, we obtained the values of “1000 1101” = 141 after an LBP operation.

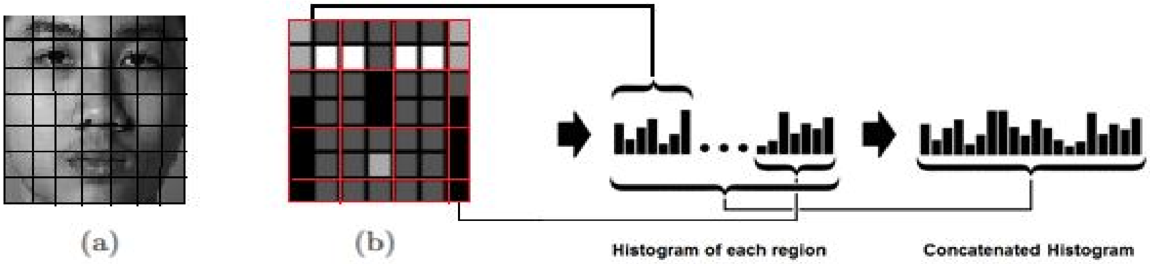

Figure 7: Results of Application of LBP Operation to Image and Obtaining a Histogram

Decision making based on bidimensional grayscale finger cristae cutis image input in the MBA system, is performed in compliance with the algorithm presented in Figure 8.

The minutiae points comparison algorithm, which consists in finding unique points, e.g. cutoffs, single short lines or branching, in the image is applied in the work. The given algorithm demands less labour input and is characterized by simplicity of implementation described in [9-10].

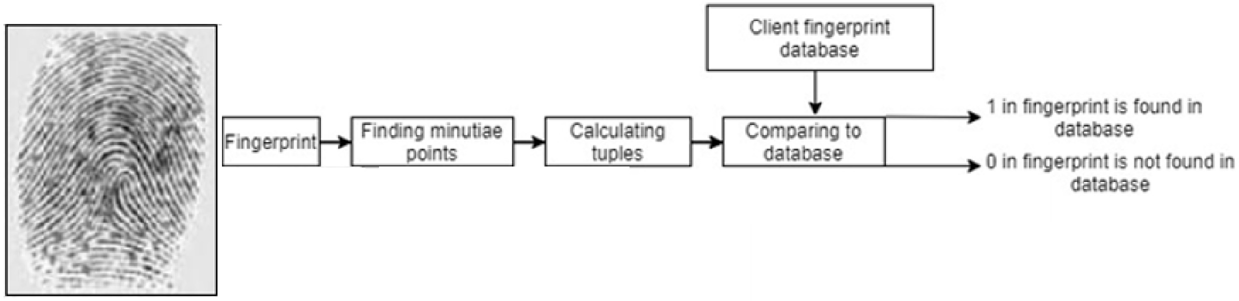
Client fingerprint database
Fingerprint
Finding minutiae points
Calculating tuples
Comparing to database
1 in fingerprint is found in database
0 in fingerprint is not found in database

Figure 8: Algorithm Applied in Photo-Fit Cristae Cutis Identification

Decision making based on the voice pattern input in the system is performed in compliance with the algorithm presented in Figure 9.

For the purpose of voice pattern identification, the algorithm described in [11] was used.

The algorithm refers to the following sequence of steps:
– Voice activity detection (VAD).
– Real key word delivery intervals detection based on long-term spectral divergence (LTSD).
– Sonic features retrieval for further application of Gaussian mixture models (GMM) for voice pattern (voice fingerprint)creation based on Mel Frequency Cepstral Coefficients (MFCCs).

With the purpose of developing a free and shared system, publicly available CMU Sphinx interface was used, which provides for detection of the words pronounces by the user as well as enables to shed the necessity of network connection, which makes the MITM attack almost impossible.

3. ANALYSIS OF RESEACRH FINDINGS

AT&T public database consisting of 40 people with 10 photographs for each person was used as the learning sample for face detection.

Photos of two people from the AT&T face base (with 10 photographs of each person) as well as photographs of three random people who agreed for the test (with 10 photographs of each person) were taken as a test set. These three people gave their consent for providing their fingerprints and key word delivery records for the purpose of their identification by fingerprints and voice.

In the design process, it was decided to take fingerprints as the basic detection method because it has the lowest type 2 error in comparison with the other applied biometric authentication methods. After scanning the fingerprint, user record is determined for future data reading for the purpose of comparison. It was also taken into account that certain users may be numb, therefore, a special mark was made in the user record.

After the successful authentication by fingerprint, the camera and the microphone are activated and key words are pronounced into the loudspeaker, 2 words in one delivery by the user. The success of the remaining two stages, we prove certainty that this is the system user and not any person who somehow successfully passed the first stage of authentication.

Analysis of the findings given in the table proves that the proposed algorithms of unifactorial Biometric authentication produce a high identification error but they have smaller response delivery time. However, with certainty of identification being the basic requirement to MBA systems, the proposed approach implemented in the hardware and software suite described in the work has an advantage over the existing unifactorial biometric authentication approaches by such indicators as FRR and FAR and is also easy in use (Table 2).

Table 2: Results of the Designed Individual Multidimensional Biometric Authentication System Performance

Biometric Indicator	Accuracy		Processing Time	Ease of Applicatio n
	FRR	FAR	ms	
Facial Geometry	~ 6%	~ 0,1%	~750 ms	High
Fingerprin t	~ 1%	~ 0,00002 %	~400 ms	Medium
Voice pattern	~ 3%	~ 0,1%	~1500м ms	High
MBA System	~ 1%	~ 0,00001 %	~2600 ms	Medium

The result of the proposed individual multidimensional biometric authentication system is the increase in overall reliability compared to the separate use of the current methods as well as a relatively small increase in the system response delivery time (from data input in the system to namely identification).

4. CONCLUSION

The paper analyzes the methods of biometric identification, considers the existing systems of multidimensional biometric identification. A multidimensional biometric authentication system has also been developed, which is completely autonomous and has small dimensions. Biometric data obtained from a fingerprint scanner, a portable video camera and a microphone built into the camera, which have a different nature - a two-dimensional grayscale image of the face and papillary finger pattern, as well as a voice print, is fed to the system input. The result of the proposed individual multidimensional biometric authentication system is the 2 times average increase in overall reliability compared to the separate use of the current methods as well as a relatively small increase (1500ms average) in the system response delivery time (from data input in the system to namely identification).

REFERENCES

[1]. Wen-Shiung Chen, Kun-Huei Chih. **Personal Authentication Technique with Human Iris Recognition using Wavelet Transform and Coding**, *International Journal of Emerging Technologies in Engineering Research (IJETER)* ,Volume 6, Issue 6, pp.18-28, June (2018).

[2] Li, P. and Zhang, R. **“The evolution of biometrics”**, *In Proceedings of the IEEE International Conference on Anti-Counterfeiting Security and Identification in Communication*, Chengdu, China, PP. 253–256, 2010. https://doi.org/10.1109/ICASID.2010.5551405

[3] O.Barkovska, N. Axak, D. Rosinskiy, S. Liashenko “**Application of mydriasis identification methods in parental control systems**”. *Proceeding of 9th International IEEE Conference “DEpendable Systems, SERvices and Technologies” (DESSERT’2018).* – Kyiv, Ukraine, PP. 459-463, 2018. https://doi.org/10.1109/DESSERT.2018.8409177

[4] A.K. Jain et al., **50 years of biometric research: Accomplishments, challenges, and opportunities,** Pattern Recognition Letters, PP. 80-105, 2016. https://doi.org/10.1016/j.patrec.2015.12.013

[5]. Lanitis A., **“A survey of the effects of aging on biometric identity verification”,** *Int. J. Biom*, 2, 1, 34-52, 2009. https://doi.org/10.1504/IJBM.2010.030415

[6] Rohan Chandra Pradhan, Saumya Rai , Smit M Shah, Brinda. Biometric Security System Using Arduino forVehicles, International Journal of Emerging Technologies in Engineering Research (IJETER), Volume 6, Issue 10, pp. 24-27, October (2018)..

[7] Ross A., Jain A.K. **Biometrics, Overview. In: Li S.Z., Jain A.K. (eds) Encyclopedia of Biometrics.** Springer, Boston, MA, 2015 available at https://doi.org/10.1007/978-1-4899-7488-4_182

[8] I.Ruban, V.Martovytskyi, A.Kovalenko, N.Lukova-Chuiko **“Identification in informative systems on the basis of users’ behaviour”.** *Proceeding of 8th International Conference on Advanced Optoelectronics and Lasers (CAOL*2019).* – Sozopol, Bulgaria. – September 06-08, PP. 574-577, 2019.

[9] A. Chandrasekaran and B. Thuraisingham**, "Fingerprint Matching Algorithm Based on Tree Comparison using Ratios of Relational Distances,"** *The Second International Conference on Availability, Reliability and Security (ARES'07)*, Vienna, PP. 273-280, 2007.

[10] Ajimol C, Dr.R.Kavitha Jaba Malar. **Biometric Fingerprint Spoof Identification Using Neural Networks,** *International Journal of Emerging Technologies in Engineering Research (IJETER)*, Volume 7, Issue 5, pp. 6-8, May (2019).

[11] J. K. Hundal and S. T. Hamde, **"Some feature extraction techniques for voice based authentication system,"** 2017 *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, Chennai, PP. 419-421, 2017. https://doi.org/10.1109/ICPCSI.2017.8392328