iJRASET
International Journal For Research in Applied Science and Engineering Technology



# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 11 **Issue:** VII **Month of publication:** July 2023

**DOI:** https://doi.org/10.22214/ijraset.2023.54946

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue VII Jul 2023- Available at www.ijraset.com*

# Designing Intuitive and Effective Dynamic Facial Authentication: Machine Interaction with Human Factors

Saurabh Suman[1], Dr. Nagesh Salimath[2]
[1]*Ph.D Student(CSE),* [2]*Associate Professor(CSE), Madhyanchal ProfessionalUniversity, Bhopal*

***Abstract:*** ***The objective of this paper is to propose a spoof-free Face Liveness Detection system with an active approach that uses the challenge-response methodology which detects the motions and gestures of the user, thereby analyzing and recognizing a real face from a photo. With cybercrimes on the rise each day, identity thefts being one of them- especially in an unsupervised authentication system, has given rise to serious security concerns. Face liveness detection assures the user's actual presence and validates their identities. Along with that, it prevents fraudulent reproduction of face biometrics to spoof the system and thus effectively protects the rights and data of the legitimate user. A review of the many scholarly pieces of the literature revealed works of some of the existing systems that use active or passive techniques to test liveness though there is still a need for a more robust approach. Predicted results of the Human-Computer Interaction (HCI) based approach demonstrated high accuracy in detecting the liveness of the user which effectively reduced system vulnerability to face-spoof attacks. The aim is to create a system that is highly accurate, efficient, and can be integrated with existing systems.***

***Keywords: Face Liveness Detection system, face-spoof attacks, challenge-response methodology, biometric systems, Human-Computer Interaction***

## I. INTRODUCTION

The overwhelming growth of digital data in recent times has led to an increase in security concerns. People and organizations have turned to biometrics for the solution. Biometrics is a multidisciplinary field involved with the estimation and mapping of one or more intrinsic physiological or behavioral traits, e.g. fingerprints, face, voice, etc. to be used as an individualized recognition program [13]. The implementation of the face recognition system is one of the most common applications of AI and has a potentially bright future. Nonetheless, the current systems have considerable limitations. With one searching through their social accounts over the web or an oblivious capture of their picture, the malicious user can easily get hold of the victim's photos which could be used to spoof facial recognition software. These attacks majorly occur in the form of 2D or 3D i.e., static, or dynamic respectively, presentation attacks. Today, due to technological limitations, 2D attacks are more popular than 3D attacks.

Companies that heavily rely on technology for their data need much more secure systems to prevent the above-mentioned methods of fraudulent access to their data. To validate the actual existence of a person, 'liveness' detection is executed which indicates the live factors of the person authenticating the system. This prevents any kind of facial biometric manipulated reproduction thus effectively protecting the rights and data of the legitimate user. In this paper, we have proposed an approach to attain Face Liveness Detection which is predicted to have high accuracy and can be integrated with present systems with ease.

## II. LITERATURE SURVEY

In general, it does not take much effort for a human to distinguish a live face of a person from a fake one since numerous factors indicate their presence like eye movements, lip movements, facial expressions, gestures, etc. However, a machine cannot sense these clues until trained to do so. A review of some of the scholarly articles that have presented various methodologies to achieve the liveness of a person revealed some very interesting studies [4, 11].

Gang Pan et al. [5] proposed eyeblinks as an approach against photographic spoofing using a generic web camera and compares it with cascaded Adaboost and HMM. The study models various states in an undirected conditional graphical structure and observes distinguishable outcomes. It was concluded to achieve high performance as well as outperform other approaches it compared it to.

Maatta et al. [7] suggested a method based on a multi-scale local binary pattern [LBP] that extracts and analyses the micro-textures of a facial image for detecting the liveness of the person in front of the camera. As the light reflects differently from a 3D live face than a 2D photograph, micro-texture features are encoded into an enhanced feature histogram.

©IJRASET: All Rights are Reserved 

The method was found promising and gave excellent results. Similarly, Tiago et al. [18] presented a solution by using an LBP-TOP descriptor that combined time as well as space information in a single descriptor. The results when trained with a simpler classifier like LDA demonstrated great potential against face spoof attacks.

The paper by Kollreider et al. [8] put forth an idea of liveness detection focusing on lip movement. The lip was detected using facial landmarks and an SVM classifier was used to analyze the reading of the movement of the lips. A hundred videos were taken of lip movements recording digits 0 to 9. The experimental results after training on 60 and testing 40 showed and given to 10-class SVM gave 73% (0.73) as the recognition rate [6].

A technique of variable focusing was proposed by Seoyeon Kim et al. [16]. Two pictures were taken sequentially on different focuses and analysed based on the key feature of Depth of Field (DoF). Using DoF, the distance between the closest object (nose) and the farthest object (ears) in the image was calculated which distinguished a 2D fake photo from a live 3D face. Yet another interesting method of face liveness detection was put forth by Li et al. [10] which is based on the Fourier Spectra of an image. The algorithm uses albedo to analyse light reflectivity which exhibits a great difference in the frequency distribution of a fake and real image. The derived approach claims to be better than the 3D depth approach in terms of computation complexity.

## III. BASIC STRATEGY

Regardless of the modus operandi in attaining a spoof-free system, every biometric system incorporates a basic framework. The image of the subject is captured by the system's input device which is followed by the next foremost step- to detect the face. The detected face then undergoes analysis of whether the face is live or not. Accordingly, the result sorts out the fake from the real image.

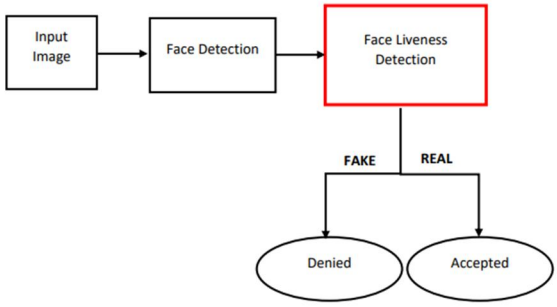



Figure 1: Basic strategy to attain Face Liveness Detection

### *A. Face Landmark Detection*

For frontal face detection, the Histogram of Oriented Gradients (HOG) proves to be a light-weighted model and computationally faster. The subsequent step is to localize key features of the face that can be extracted with the aid of the iBUG 300-W dataset which annotates and maps 68 points of facial regions [1, 2, 3]. Author Rosebrock A. (2017) [15], demonstrated accessing and visualizing various isolated facial regions such as the mouth, right eyebrow, left eyebrow, right eye, left eye, nose, and jaw via indexes in Python.



Figure 2: Sagonas C., Zafeiriou S., (n.d.). The 68-points mark-up used for annotations.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 11 Issue VII Jul 2023- Available at www.ijraset.com*

## IV. PROPOSED METHODOLOGY

There is not any more certain way of authenticating a live face than to observe the natural movement and gesture of the subject. Thus, this paper aims on approaching the problem of spoof detection by employing the challenge-response methodology. It works on the principle of Human-Computer Interaction in which the user needs to cooperate with the machine and perform simple gestures which would be detected by the system for a liveness test.

### *A. Eyeblink Detection*

The most natural movement of the eye is its blink. Eyeblink is a rapid closing and reopening of an eye. Minimum user effort is required for the same and detecting it can instantly validate the user's live presence. As mentioned in the previous section, facial landmarks detection can be used to express various key features of the face; one of them being the eye region. Soukup ova & Cech [17] derived a rather interesting equation known as EAR (Eye Aspect Ratio) in their paper. The equation computes the height and width of the eye by utilizing the distances relating to the horizontal and vertical landmarks.

A fall followed by a rise of eye aspect ratio concerning a certain threshold will be considered one blink. When an eye is open EAR mostly remains constant while it gets close to zero when the eye is closed. To prove liveness, the subject can be asked to blink the required number of times. A set counter sums up the number of blinks and if it matches with the specified number, the presence of the person is validated.

### *B. Lip Movement Detection*

Open and close of mouth can be another challenge-response approach to detect the liveness of the face. In his article, Peter Xie (2019) [20], extended the study on mouth open detection from a face recognition project. The project marked the static landmark positions of the facial regions which were then used to detect motion of the upper lip and the lower lip. A simple logical application of the positional feature analysis was the calculation of each lip height and then their relative distance when the lips were displaced.

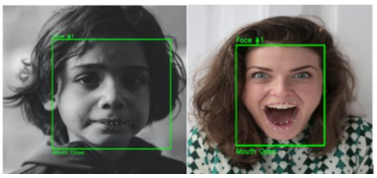


Figure 3: Mouth-close (left) and Mouth-open (right) detection

### *C. Side Profile Face Detection*

The subject can be asked to look at their right or their left. The challenge is quite simple yet a definite indication of eliminating the threat of identity spoofing. The study contributed by Voila P. and Jones M. [19] presents an efficient method of object detection known as Haar Cascade classifiers. It is a machine-learning algorithm with a rapid and high detection rate. Haar Cascade for side face is currently publicly available as a downloadable XML file.

### *D. Head Rotation Detection*

Yet another challenge to put forth is the head rotation in a specific direction which could be clockwise or anticlockwise. The execution of the same can be done by gathering the figures generated by the nose tip points of faces and plotting them within the best circle fit [9, 14]. The sequence of quadrants in the circle will determine the direction of rotation.

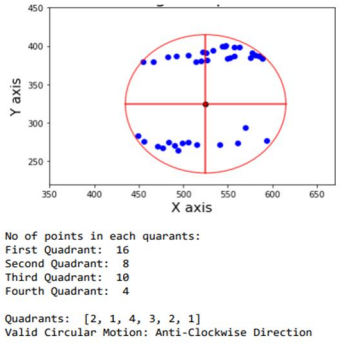



Figure 4: Analysing nose-tip points to detect Head Rotation direction

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

*E. Half Face Covered*

To further enhance the randomness and uniqueness of the liveness detection test, another action that users can be asked to perform is covering half their face with the hand, either the right or the left. There are no public datasets available for this type of gesture, hence a new curated dataset needs to be generated. This dataset would have around 7000 images each in a left-side face covered and right-side face covered, trained, and successfully tested the classified on the local machine.



Figure 5: Sample dataset of half-face cover challenge

## V. LIMITATIONS

Zhang et al. [21], in their paper on the multispectral liveness detection method, highlighted some drawbacks of a system that adopts the behavioral challenge-response technique as a means of detecting liveness. Though the challenges proposed previously in this paper are not entirely user-unfriendly, the users are required to be highly cooperative with the system. Another major limitation of the system proposed in this paper is if a 3D attack like a mask of the genuine user with eyes and mouth cut is presented, it can bypass the system.

## VI. CONCLUSION

This paper presented the development of a system with a challenge-response-based methodology to protect against face spoof attacks that generally occur in biometric systems. Some challenges that were introduced were Eyeblink, Lip Movement, Head Rotation, Side Face Profile, and Half Face Covered, along with their means of implementation in the systems' framework. Since this technique uses an active approach of Human-Computer Interaction (HCI), the predicted results demonstrated high accuracy in detecting the liveness of the user. Further, there is no demand for any auxiliary gadgets and the approach can be easily integrated with existing systems. However, user cooperation is required but the simplicity of their participation is kept minimum.

## VII. FUTURE SCOPE

The scope of the approach based on HCI is comprehensive. To increase security, some additional ideas of challenges include numerical gestures with hands, and facial expressions such as happy, sad, or angry, which can be introduced into the system. A combination of more than one liveness indicator test which analyses textural and temporal characteristics can be instilled in the system as well. Exposure of the training model to varied and expansive test data and data that involves different spoofing scenarios can increase and improve the system's performance. Furthermore, to enhance the system's capabilities, hardware input devices like light field cameras that can acquire various focusing information in the spatial domain can be integrated with the system.

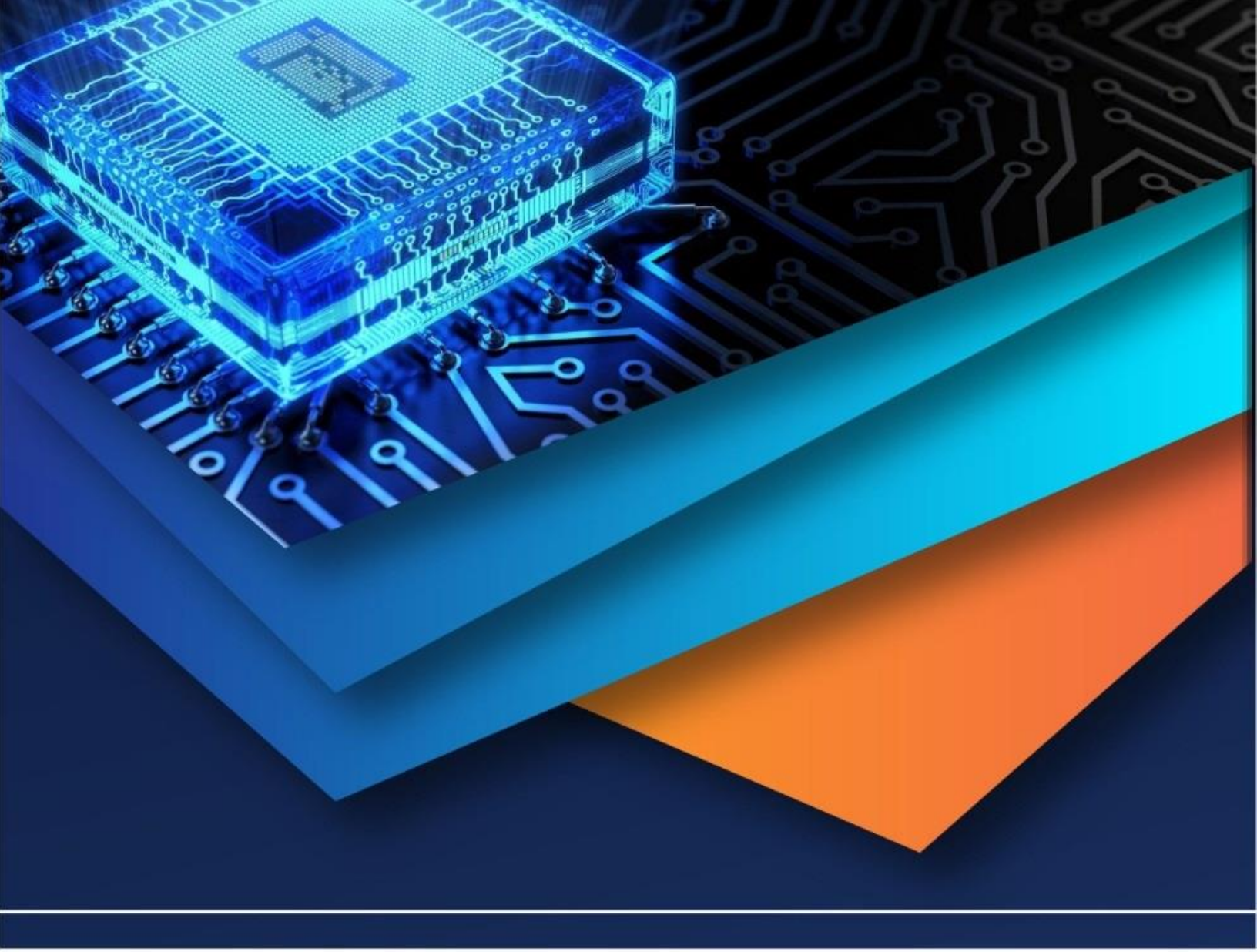
The field of biometric security systems seems to be a green area for more advanced research as there are a significant amount of disciplines to collaborate in the study with. There is still a lot of ground to cover for implanting new technologies and security solutions for digital data. A program with characteristics of automation along with its applications embedded in smart compatible devices can be considered as well. More robust countermeasures are required against video replays and 3D presentation attacks.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

## REFERENCES

[1] C. Sagonas, E. Antonakos, G, Tzimiropoulos, S. Zafeiriou, M. Pantic. 300 faces In-the-wild challenge: Database and results. Image and Vision Computing (IMAVIS), Special Issue on Facial Landmark Localisation "In-The-Wild". 2016.
[2] C. Sagonas, G. Tzimiropoulos, S. Zafeiriou, M. Pantic. 300 Faces in-the-Wild Challenge: The first facial landmark localization Challenge. Proceedings of IEEE Int'l Conf. on Computer Vision (ICCV-W), 300 Faces in-the-Wild Challenge (300-W). Sydney, Australia, December 2013.
[3] C. Sagonas, G. Tzimiropoulos, S. Zafeiriou, M. Pantic. A semi-automatic methodology for facial landmark annotation. Proceedings of IEEE Int'l Conf. Computer Vision and Pattern Recognition (CVPR-W), 5th Workshop on Analysis and Modeling of Faces and Gestures (AMFG 2013). Oregon, USA, June 2013.
[4] Chakraborty, S., and Das, D. (2014). An overview of Face Liveness Detection. Int. J. Inf. Theory 3, 11–25. doi: 10.5121/ijit.2014.3202.
[5] G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic webcamera," in Proceedings of the IEEE 11th International Conference on Computer Vision (ICCV '07), pp. 1–8, Rio de Janeiro, Brazil, October 2007.
[6] Gaurav Rajpurohit , Dr. S. R. Ganorkar, 2019, Survey on Face Liveness Detection, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) Volume 08, Issue 06 (June 2019).
[7] J. Maatta, A.Hadid, M.Pietikainen,"Face Spoofing Detection From Single pictures Using MicroTexture Analysis", Proc. Intn Joint Conference on Biometrics,2011, Washington, D.C., USA.
[8] K. Kollreider, H. Fronthaler, J. Bigun, Non-intrusive liveness detection by face images, Image and Vision Computing, Volume 27, Issue 3, 2009, Pages 233-244, ISSN 0262-8856, https://doi.org/10.1016/j.imavis.2007.05.004. (http://www.sciencedirect.com/science/article/pii/S0262885607000893).
[9] Kenichi Kanatani, Prasanna Rangarajan, Hyper least squares fitting of circles and ellipses, Computational Statistics & Data Analysis, Volume 55, Issue 6, 2011, Pages 2197-2208, ISSN 0167-9473, https://doi.org/10.1016/j.csda.2010.12.012.
[10] Li, Jiangwei & Tan, Tieniu & Jain, Anil. (2004). Live Face Detection Based on the Analysis of Fourier Spectra. Proceedings of SPIE - The International Society for Optical Engineering. 5404. 296-303. 10.1117/12.541955.
[11] M. Bagga and B. Singh, "Spoofing Detection In Face Recognition: A Review," in 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), 2016, pp. 2037–2042.
[12] O. Kahm and N. Damer, "2D face liveness detection: An overview," BIOSIG-Proceedings IEEE Int. Conf. the. Biometrics Spec. Interes. Gr. (BIOSIG), 2012, pp. 171–182.
[13] Raheem, Enas. (2019). Insight on Face Liveness Detection: A Systematic Literature Review. International Journal of Electrical and Computer Engineering.
[14] Rangarajan, Prasanna; Kanatani, Kenichi. Improved algebraic methods for circle fitting. Electron. J. Statist. 3 (2009), 1075--1082. doi:10.1214/09-EJS488. https://projecteuclid.org/euclid.ejs/1256822131.
[15] Rosebrock, A. (2017, April 10). Detect eyes, nose, lips, and jaw with dlib, OpenCV, and Python. PyImageSearch. https://www.pyimagesearch.com/2017/04/10/detect-eyes-nose-lips-jaw-dlib-opencv-python/.
[16] S. Kim, S. Yu, K. Kim, Y. Ban and S. Lee, "Face liveness detection using variable focusing," 2013 International Conference on Biometrics (ICB), Madrid, 2013, pp. 1-6, doi: 10.1109/ICB.2013.6613002.
[17] Soukupová, T., & Cech, J. (2016). Eye-Blink Detection Using Facial Landmarks.
[18] T. De Freitas Pereira, A. Anjos, J. M. De Martino, and S. Marcel, "LBP-TOP based countermeasure against face spoofing attacks," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 7728 LNCS, no. PART 1, pp. 121–132, 2013.
[19] Viola, Paul & Jones, Michael. (2001). Rapid Object Detection using a Boosted Cascade of Simple Features. IEEE Conf Comput Vis Pattern Recognit. 1. I-511. 10.1109/CVPR.2001.990517.
[20] Xie, P. (2019, Oct 8). How to Detect Mouth Open for Face Login. *towards data science*. https://towardsdatascience.com/how-to-detect-mouth-open-for-face-login-84ca834dff3b
[21] Z. Zhang, D. Yi, Z. Lei and S. Z. Li, "Face liveness detection by learning multispectral reflectance distributions," Face and Gesture 2011, Santa Barbara, CA, 2011, pp. 436-441, doi: 10.1109/FG.2011.5771438.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)