Face tracking system based on border security

Jagbeer Singh, Himanshu Partap singh, Harsh Chauhan, Govind Panday, Vikas Kumar, Sunidhi Garg
Meerut Institute of Engineering and Technology, Meerut

DOI:10.48047/ecb/2023.12.si4.733

Abstract

The main goal of the Border Security Based Face Detection System project is to lessen the illegal activities that occur at the border. Humans often engage in illegal activity that could compromise the level of security. A suggested remedy is a security system that can prevent illegal activity by detecting intruders in high-security or restricted areas. The hardware component and the software component make up this system. A camera makes up the hardware component, and face-detection and face-recognition algorithms make up the software component. When a person enters the zone, the camera takes a number of pictures, which are then sent to the software for analysis and comparison with an already-existing database of reliable individuals. If the user is not recognised, legal action against them may be taken, and if the user is recognised and permitted to cross the border, an alarm is set off.

Keywords: Haar-Cascade Classifier, Open-CV, LBPH, Criminal Identification, computer vision**.**

1. INTRODUCTION

The main objective is to identify the correct identity of person by the use of face detection method if their identity is matched with the database then they allow to cross by the border. In a way of doing this we can increase the security aspect of the border [1]. Also through Face Detection Method we will reduce pen and paper work as it is done digitally and this will increase the security level which will reduce the illegal activities and will help the officers in recognising the person easily and also doing the Criminal Identification [2][3].

Face recognition is the task of identifying an already detected object as a known or unknown face. Often the problem of face recognition is confused with the problem of face detection. Face Recognition on the other hand is to decide if the "face" is someone known, or unknown, using for this purpose a database of faces in order to validate this input face. Face recognition is a software application adaptesad to identify individuals via tracking and detecting. The main intention of this paper is to recognize the faces of people. This approach can be executed practically in crowded areas like Borders, airports, railway stations,

universities and malls for security. The main target of this paper is to enhance the recognition rate and accuracy [4] [5].

After the event of 9/11, developing security systems has become more concerned importance to provide safety to the citizens, particularly in crowded areas like airports, railway stations, in borders, organizations where detection and recognition is imperative. To identify the individuals, Surveillance camera with face recognition system can be provided. Face recognition system has the dexterity to mitigate the danger and ultimately ward off any future assault from happening. There are countless applications for this Face recognition system over the world. It has also elevated in applications like Facebook, Instagram and in many social media platforms [2]. It will suggest the user to tag the person who has been detected in images [6][7].

2. TECHNOLOGY USED

2.1 Haar-Cascade Classifier

Cascade is a machine learning object detection algorithm used to identify objects in an image or video and based on the concept of features proposed by Paul Viola and Michael Jones in their paper "Rapid Object Detection using a Boosted Cascade of Simple Features".It is a machine learning based approach where a cascade function is trained from a lot of positive and negative images. It is then used to detect objects in other images [8][9].The cascade classifier consists of a collection of stages, where each stage is an ensemble of weak learners. The weak learners are simple classifiers called decision stumps. Each stage is trained using a technique called boosting. Boosting provides the ability totrain a highly accurate classifier by taking a weighted average of the decisions made by the weak learners [10][11].

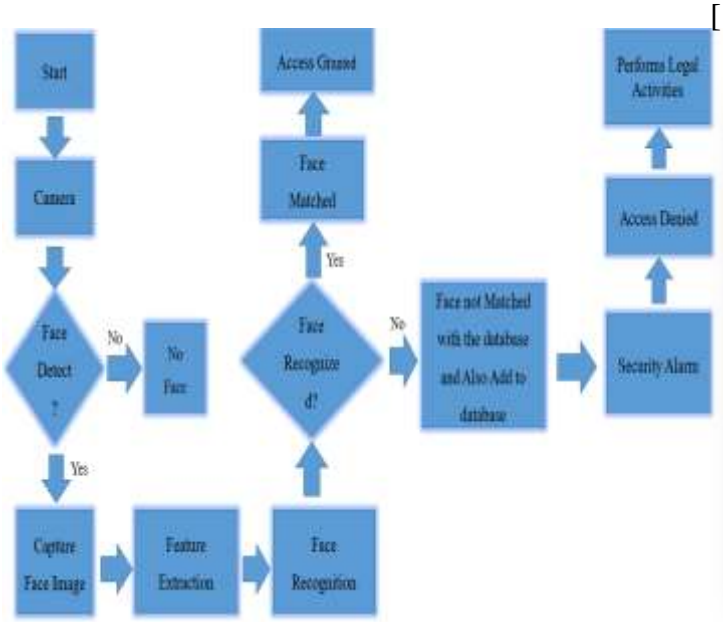


Figure 1.1 Flowchart of On Border Security System

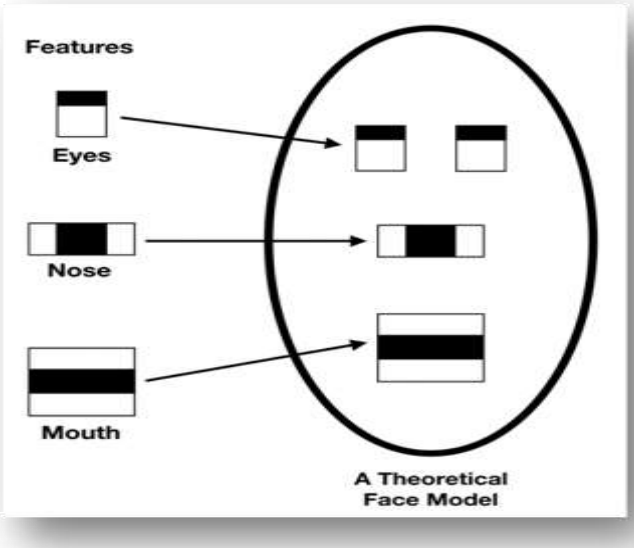


Figure 2.1 Haar- Cascade Features

2.2 LBPH

The Local Binary Pattern Histogram (LBPH) algorithm is a simple solution on face recognition problem, which can recognize both front face and side face. To solve this problem, aModified LBPH algorithm based on pixel neighbourhood grey median (MLBPH) is proposed [12][13] The first computational step of the LBPH is to create an intermediate image that describes the original image in a better way, by highlighting the facial characteristics. To do so the algorithm uses a concept of a sliding window, based on the parameters radius and neighbours [14][15].

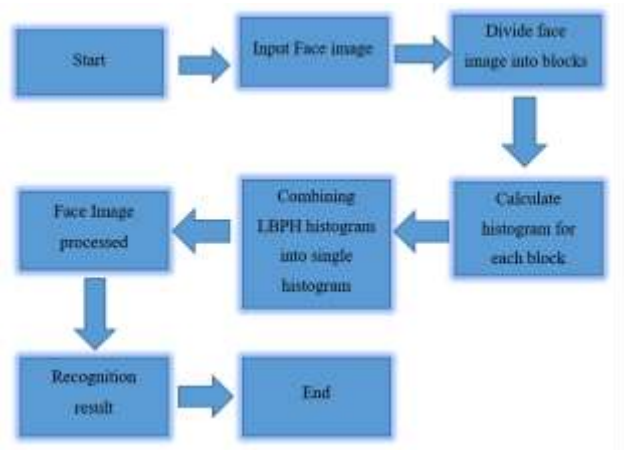


Figure 2.2 LBPH model for On Border Security System

2.3 Open-CV

Open CV is a Python library which is designed to solve computer vision problems. Open CV supports a wide variety of programming languages such as C++, Python, and Java etc. Support for multiple platforms including Windows, Linux, and Mac OS. Open CV Python is nothing but a wrapper class for the original C++ library to be used with Python. Using this, all of the Open CV array structures gets converted to/from Num Py arrays. This makes it easier to integrate it with other libraries which use Num Py. For example, libraries such as SciPy and Matplotlib. Next up on this Open CV Python Tutorial blog, let us look at some of the basic operations that we can perform with Open CV [5] [16][17].

3. LITERATURE REVIEW

Facial Recognition Using Haar-Cascade Classifier for Criminal Identification [4]: The presented system will get implemented using Open CV. The recognition rate attained by this process is 90%-98%. There will be deviation in the result on account of the distance, camera resolution and lightning. Advanced processors can be put to use to reduce the processing time [18][19][20].

A Literature Survey in Face Recognition Techniques [2]: Face recognition is a highly challenging task in the domain of image analysis and computer vision that has received an immense deal of attention over the last few decades because of its many applications in vast domains. Few classical face recognition techniques are cited in this paper. In some face database, the methods of SVM and HMM can produce better face recognition results, but they use more complex algorithms [21][22].

A Research Survey on Face Recognition Techniques [3]: Face detection is a challenging problem in the field of image processing and computer vision. Because of lots of application in

different fields the face recognition has received great attention. In this paper different face recognition algorithms are mentioned with their advantages and disadvantages. You can use any of them as per your requirement and application. You can also work over to improve the efficiency of the discussed algorithms and improve the performance [23][24].

4. METHODOLOGY

4.1 Dataset Collection

When benchmarking an algorithm it is recommendable to use a standard test data set to be able to directly compare the results. While there are many databases in use currently, the choice of an appropriate database to be used should be made based on the task given (aging, expressions, lighting etc.) [3]. Another way is to choose the data set specific tothe property to be tested (e.g. how algorithm behaves when given images with lighting changesor images with different facial expressions), so we took some sample of photos about 250 using Haar-Cascade Classifier method using Open-CV by webcam in different environment [25][26].

Figure 4.1 Image samples for dataset using Haar-Cascade in Open-CV

Figure 4.2 Image samples for dataset using Haar-Cascade in Open-CV

4.2 Training

In the training module the dataset images can be trained using the various training algorithms in on border Security based Face Detection System the Haar Cascade Training Algorithm is used to train the model which contain the various sample of imagesinto an accurate angle and size using Open-CV which comes with detector as well as Trainer. Its Features are shown in the figure 2.1. [27][28].

4.3 Recognition

For the recognition we use the LBPH algorithm in which the sample of images which are collected in database can be matched in real time if face can be matched then the door unlock and the following person is allowed to cross the border. The flowchart of LBPH is shown in the figure 2.2 [29].

When the system is attached to the video surveillance camera the recognition system searches the field of view of a video camera for

faces. A multi-scale algorithm is used to search for faces in low resolution. Once a face is detected, the system determines the head's position, size and pose. A face needs to be turned at least 35 degrees toward the camera for the system to register it [30]. The image of the head is scaled and rotated so that it can be registered and mapped into an appropriate size and pose [1]. Normalization is performed regardless of the head's location and distance from the camera [31].

The system translates the facial data into a unique code. This coding process allows for easier comparison of the newly acquired facial data to stored facial data. The newly acquired facial data is compared to the stored data is compared to the stored data and (ideally) linked to at least one stored facial representation [5].

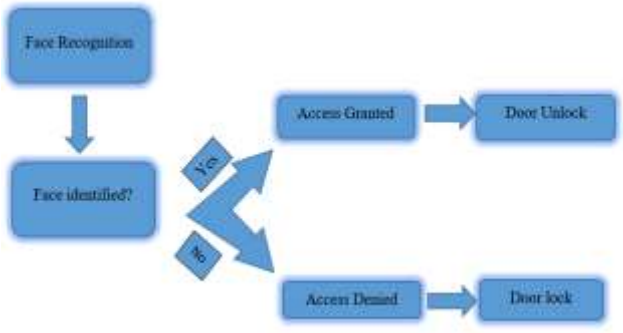


Figure 4.2 Flowchart of Security based face recognition.

5. Reference Basis Set Evaluation

The reference face descriptors are obtained by projecting the gallery and probe images into the reference basis set; therefore, the selection of reference faces of the reference basis set plays an important role, and affects the overall system performance. In order to evaluate the reference basis set, we adopt the method in but from a different perspective. In an image alignment method is proposed using sparse and low-rank decomposition. The low-rank decomposition learns the common component of a set of images with variations in illumination, expression, pose, etc. The calculated sparse error component indicates the specificity of that image in the image set. In our application, we examine the diversity of the reference faces. Specifically, for each pose or specific expression in the reference basis set, a matrix D whose columns represent images of all reference faces is constructed. The goal is to determine the diversity of D and how effective it is as the basis function matrix. The optimization follows the formulation.

$$\min \|A\|_? + \lambda\|E\|_1 \text{ s.t. } \quad D \circ \tau = A + E,$$

A,E,τ where A is the aligned version of D, $\|A\|_?$ takes the nuclear norm of A, E is the error matrix, λ is a positive weighting parameter, and $\|E\|_1$ corresponds to the 1-norm of E. τ is a set of transformations specified by,

$$D \circ \tau = [I_1 \circ \tau_1,...,I_n \circ \tau_n],$$

where Ii ∘ τi represents applying transformation τi to image Ii. If the images in D are similar, the sparse error E would be small since the common component will be dominating. On the other hand, if the images in D are very dissimilar, the error E would be larger. In the reference basis set, dissimilar images are preferred to define a more definitive basis set. Figure shows the averaged mean squared error of E over multiple experimental

runs as the size of the reference basis set increases. The black line is a polynomial trendline of order 2 fitted to the mean squared values.

The peak of the MSE is observed with 400 reference faces in the reference basis set which contains images from FEI and Multi-PIE Thus, from the 500 individuals in the second reference basis set only 400 are chosen for the experiments.

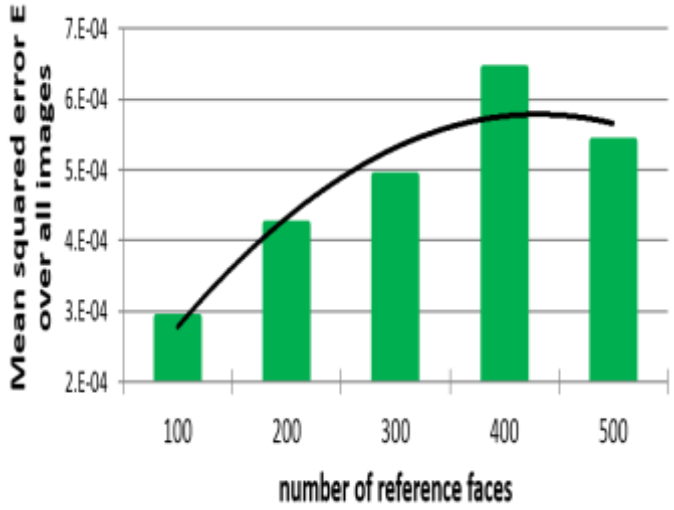
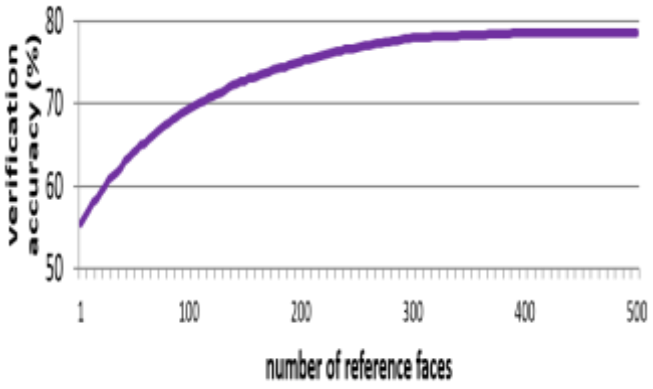


Fig. 7. Mean squared error vs. reference basis set size. The black line is a polynomial trendline of order 2 fitted to the mean squared values.

A similar evaluation is performed for the first reference basis set, and based on the results 250 individuals are chosen.

Figure 8 illustrates how the number of reference faces affects the verification accuracy on the Face Pix database [45]. Four Patch LBP (FPLBP) [30] is the feature used in this experiment. As the number of reference faces increases over 400, the plot flattens around 78%. Note that the number of reference faces (*N*) determines the dimensionality of the reference face descriptors.



Verification accuracy on FacePix [45] with increasing number of reference faces.

6. Comparison with Other Methods

We compare the proposed method with several state-of-theart algorithms on multiple databases.

• Comparison on LFW database [19]: We followed the default 10-fold verification protocol on the LFW database to provide a fair comparison. Table III shows the average classification accuracies of the proposed RFG approach and other methods including a commercial recognition system.

With simple LBP feature used and without face alignment, our method achieves an average classification accuracy of 0.9284 with a standard deviation of 0.0027, which is very competitive.

To examine the performance in detail, we further compare RFG recognition with associate-predict (AP) method likelihood-predict (LP) model cosine similarity metric.

Classification accuracy on LFW[19] using protocol of ”UNRESTRICTED, LABELED OUTSIDE DATA RESULTS”

Method	Accuracy
Attribute classifiers [22]	0.8525 ± 0.0060
Multiple LE + comp [47]	0.8445 ± 0.0046
Associate-Predict [23]	0.9057 ± 0.0056
Combined Joint Bayesian [48]	0.9242 ± 0.0108
POOF-HOG [49]	0.9280 ± 0.0047
Tom-vs-Pete [31]	0.9310 ± 0.0135
face.com [50]	0.9130 ± 0.0030
RFG (this paper)	0.9284 ± 0.0027

We compare the proposed method with several state-of-theart algorithms on multiple databases.

• Comparison on LFW database We followed the default 10-fold verification protocol on the LFW database to provide a fair comparison. Table III shows the average classification accuracies of the proposed RFG approach and other methods including a commercial recognition system. With simple LBP feature used and without face alignment, our method achieves an average classification accuracy of 0.9284 with a standard deviation of 0.0027, which is very competitive.

To examine the performance in detail, we further compare RFG recognition with associate-predict (AP) method [23], likelihood-predict (LP) model [23], cosine similarity metric

Classification accuracy on LFW[19] using protocol of “UNRESTRICTED, LABELED OUTSIDE DATA RESULTS”

Method	Accuracy
Attribute classifiers [22]	0.8525 ± 0.0060
Multiple LE + comp [47]	0.8445 ± 0.0046
Associate-Predict [23]	0.9057 ± 0.0056
Combined Joint Bayesian [48]	0.9242 ± 0.0108
POOF-HOG [49]	0.9280 ± 0.0047
Tom-vs-Pete [31]	0.9310 ± 0.0135
face.com [50]	0.9130 ± 0.0030
RFG (this paper)	0.9284 ± 0.0027

7. RESULT AND DISCUSSION

The output proposed in this paper by the recognition of accuracy is 82% but this model is refined in the future to improve the security level more effectively and even at the time of forming the dataset, each person will get designated using an id number. While recognition, when the test person image matches with the dataset then a message will get send like an unauthorized person symbolizes criminal or thief through internet of things, if the test person image does not get matched with the dataset then no message will get send symbolizes a normal human being.

Figure 5.1Final output screen with Accuracy

8. CONCLUSION

After deep evaluation, the computational models used in this project were selected, and the positive testing outcomes show that the researcher's decisions were sound. The accuracy of automatic face recognition was not higher than 90% in the system with manual face detection. Therefore, it can be concluded that the accuracy is at least 90% and never less than 80%, indicating that the accuracy is entirely dependent on environmental factors. At the moment, all researchers are working on this real-time project, focusing primarily on accuracy and efficiency, but in the future, accuracy may be greater than 90%, and a large number of sample images may be successfully used to train the suggested in order to increase its efficiency and accuracy as well at the security aspect on border.

9. FUTURE SCOPE

A. Face detection and recognition is a very effective technology that can help law enforcers recognize criminals.

B. This technology can be further developed to be used in other avenues such as ATMs, accessing confidential files, or other sensitive materials.

10. REFERENCES

1. Krishna Prasad Bhattarai, VishnuPrasad Gautama ,Kazuhiko Sato "Authentic Gate Entry System by Using LBPH for Smart Home Security System" International Conference on Networking and Network Applications (NaNA), 2018.
2. M.Tamilselvia, Dr. S.Karthikeyan,"A Literature Survey in Face Recognition Techniques International Journal of Pure and Applied Mathematics" Volume 118 December 27, 2017.
3. Riddhi Patel, Shruti B. Y agnik, "A Research Survey on Face Recognition Techniques" International Journal of Computer Trends and Technology (IJCTT) – volume 5 number 4 –Nov 2013.
4. Senthamizh Selvi.R, D.Sivakumar, Sandhya.J.S, Siva Sowmiya.S, Ramya.S, Kamara Suba Raja.S "Face Recognition Using Haar - Cascade Classifier for Criminal Identification" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7, Issue-6S5, April 2019.
5. S L Suma, Sarika Raga, "Real Time Face Recognition of Human Faces by using LBPH and Viola Jones Algorithm." International Journal of Scientific Research in Computer Science and Engineering, Vol.6, Issue.5, pp.01-03, Oct. 2018.
6. *M. Günther, D. Haufe and R.P. Würtz*. Face recognition with disparity corrected Gabor phase differences**.** In Artificial neural networks and machine learning, volume 7552 of Lecture Notes in Computer Science, pages 411-418. 9/2012.
7. Madeena Sultana and Marina L. Gavrilova, "Face recognition using multiple content-based image features for biometric security applications" International Journal of Biometrics, Volume 6, pp. 417- 418, 2014.

8. Riddhi Patel, Shruti B. Yagnik, "A Research Survey on Face Recognition Techniques" International Journal of Computer Trends and Technology (IJCTT) – volume 5, pp. 191-193, Nov 2013.
9. Jean-François Connolly, Eric Granger, Robert Sabourin, "An adaptive classification system for videobased face recognition" Information Sciences, Volume 192,pp 50-54, 1 June 2012.
10. Y. Peng, A. Ganesh, J. Wright, W. Xu, and Y. Ma, "RASL: Robust alignment by sparse and low-rank decomposition for linearly correlated images," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 11, pp. 2233–2246, Nov. 2012.
11. Mohseni, S., Yang, F., Pentyala, S., Du, M., Liu, Y., Lupfer, N., ... & Ragan, E. (2021, May). Machine learning explanations to prevent overtrust in fake news detection. In Proceedings of the International AAAI Conference on Web and Social Media (Vol. 15, pp. 421-431).
12. Narayan, Vipul, et al. "Enhance-Net: An Approach to Boost the Performance of Deep Learning Model Based on Real-Time Medical Images." Journal of Sensors 2023 (2023).
13. Babu, S. Z., et al. "Abridgement of Business Data Drilling with the Natural Selection and Recasting Breakthrough: Drill Data With GA." Authors Profile Tarun Danti Dey is doing Bachelor in LAW from Chittagong Independent University, Bangladesh. Her research discipline is business intelligence, LAW, and Computational thinking. She has done 3 (2020).
14. NARAYAN, VIPUL, A. K. Daniel, and Pooja Chaturvedi. "FGWOA: An Efficient Heuristic for Cluster Head Selection in WSN using Fuzzy based Grey Wolf Optimization Algorithm." (2022).
15. Faiz, Mohammad, et al. "IMPROVED HOMOMORPHIC ENCRYPTION FOR SECURITY IN CLOUD USING PARTICLE SWARM OPTIMIZATION." Journal of Pharmaceutical Negative Results (2022): 4761-4771.
16. Narayan, Vipul, A. K. Daniel, and Pooja Chaturvedi. "E-FEERP: Enhanced Fuzzy based Energy Efficient Routing Protocol for Wireless Sensor Network." Wireless Personal Communications (2023): 1-28.
17. Tyagi, Lalit Kumar, et al. "Energy Efficient Routing Protocol Using Next Cluster Head Selection Process In Two-Level Hierarchy For Wireless Sensor Network." Journal of Pharmaceutical Negative Results (2023): 665-676.
18. Paricherla, Mutyalaiah, et al. "Towards Development of Machine Learning Framework for Enhancing Security in Internet of Things." Security and Communication Networks 2022 (2022).
19. Sawhney, Rahul, et al. "A comparative assessment of artificial intelligence models used for early prediction and evaluation of chronic kidney disease." Decision Analytics Journal 6 (2023): 100169.
20. Srivastava, Swapnita, et al. "An Ensemble Learning Approach For Chronic Kidney Disease Classification." Journal of Pharmaceutical Negative Results (2022): 2401-2409.
21. Mall, Pawan Kumar, et al. "FuzzyNet-Based Modelling Smart Traffic System in Smart Cities Using Deep Learning Models." Handbook of Research on Data-Driven Mathematical Modeling in Smart Cities. IGI Global, 2023. 76-95.
22. Mall, Pawan Kumar, et al. "Early Warning Signs Of Parkinson's Disease Prediction Using Machine Learning Technique." Journal of Pharmaceutical Negative Results (2022): 4784-4792.
23. Pramanik, Sabyasachi, et al. "A novel approach using steganography and cryptography in business intelligence." Integration Challenges for Analytics, Business Intelligence, and Data Mining. IGI Global, 2021. 192-217.
24. Narayan, Vipul, et al. "Deep Learning Approaches for Human Gait Recognition: A Review." 2023 International Conference on Artificial Intelligence and Smart Communication (AISC). IEEE, 2023.
25. Narayan, Vipul, et al. "FuzzyNet: Medical Image Classification based on GLCM Texture Feature." 2023

International Conference on Artificial Intelligence and Smart Communication (AISC). IEEE, 2023

26. Mahadani, Asim Kumar, et al. "Indel-K2P: a modified Kimura 2 Parameters (K2P) model to incorporate insertion and deletion (Indel) information in phylogenetic analysis." Cyber-Physical Systems 8.1 (2022): 32-44.
27. Singh, Mahesh Kumar, et al. "Classification and Comparison of Web Recommendation Systems used in Online Business." 2020 International Conference on Computation, Automation and Knowledge Management (ICCAKM). IEEE, 2020.
28. Awasthi, Shashank, Naresh Kumar, and Pramod Kumar Srivastava. "A study of epidemic approach for worm propagation in wireless sensor network." Intelligent Computing in Engineering: Select Proceedings of RICE 2019. Springer Singapore, 2020.
29. Srivastava, Arun Pratap, et al. "Stability analysis of SIDR model for worm propagation in wireless sensor network." Indian J. Sci. Technol 9.31 (2016): 1-5.
30. Ojha, Rudra Pratap, et al. "Global stability of dynamic model for worm propagation in wireless sensor network." Proceeding of International Conference on Intelligent Communication, Control and Devices: ICICCD 2016. Springer Singapore, 2017.
31. Shashank, Awasthi, et al. "Stability analysis of SITR model and non linear dynamics in wireless sensor network." Indian Journal of Science and Technology 9.28 (2016)