

# Smart Surveillance System using Deep Learning



Dayana R, Suganya M, Balaji P, Mohamed Thahir A, Arunkumar P

*Abstract-In industry and research area big data applications are consuming most of the spaces. Among some examples of big data, the video streams from CCTV cameras as equal importance with other sources like medical data, social media data. Based on the security purpose CCTV cameras are implemented in all places where security having much importance. Security can be defined in different ways like theft identification, violence detection etc. In most of the highly secured areas security plays a major role in a real time environment. This paper discusses the detecting and recognising the facial features of the persons using deep learning concepts. This paper includes deep learning concepts starts from object detection, action detection and identification. The issues recognized in existing methods are identified and summarized.*

**Keywords:** Surveillance, Security, Real time, Deep Learning, Face Detection, Face Recognition.

## I. INTRODUCTION

Now a day, securing highly Confidential matter from a third party is a challenging one. In recent times, accessing data from highly secured area had increased in number, so securing the data is essential. Most of the memory spaces of industry are occupied by the big data. The implementation of CCTV cameras in all areas due to security purpose. The use of CCTV cameras is essential, but it consumes more memory spaces to store data. Security is used for the purpose of theft identification, violence detection, unauthorized person entering, illegal activity in a region. Hence for all abnormal activity's security plays a major role so security must be implemented in the region of highly confidential. Using CCTV footage is past days methodology to find the theft

happenings and other activities, this is a tedious process and time consuming. To overcome this existing methodology, CCTV camera is used with deep learning concepts for more ease. Deep learning concepts are capable of learning data which is unstructured, and it handles large amount of data sets. Deep learning will train the data sets and gives a finite data sets as a output. Using this concept training enormous amount of data as input and gives equal accurate data sets as an output. The accuracy rate is also a desirable one. Using deep learning, facial features of data sets are recognized with the help of CCTV. By this way all the data sets that are capturing in CCTV camera will be recognized and sort out the authorized person or unauthorized person as well. The video starts to record when there is an abnormal event has been recognized. This paper will summarize the drawback of existing technology over surveillance systems.

## II. MOTIVATION

Security is essential where there is a more secured data. To secure large amount of data or highly securable data in confidential region security plays a major role. For establishing security for a data, it must be protected from an unauthorized person. The CCTV will capture the video and deep learning concepts will provide the features of facial analysis. When facial features are recognized it must be validated with authorized data sets in a database. The validated face is examined to find whether it is an authorized person or not. This concept will reduce the theft happening in real world areas and the person who attempt to enter the area in a improper manner will be notified and caught. This paper reduces the theft happening or unauthorized way of entering.

### A. Scope

The scope of this project is to minimize the theft happening in future and maximize the protection of a data in highly confidential region. This will be more essential in industry areas.

### B. Objective

1. This will minimize the theft happening.
2. The administrator will be notified at the time of theft happening.
3. The data will be protected with high security in the confidential region.
4. The administrator will be notified regarding the abnormal activity in his/her place by a means of short message service or mail system using pop3 configuration.
5. The process is fast and highly securable.
6. This will summarize the past methodology and help to serve better for future purpose.

Manuscript received on April 02, 2020.

Revised Manuscript received on April 15, 2020.

Manuscript published on May 30, 2020.

\* Correspondence Author

**Mrs. R Dayana\***, Assistant Professor, Department of Computer Science and Engineering, Jeppiaar Institute of Technology, Chennai, India. E-mail: [dayana@jeppiaarinstitute.org](mailto:dayana@jeppiaarinstitute.org)

**Mrs. M Suganya**, Assistant Professor, Department of Computer Science and Engineering, Jeppiaar Institute of Technology, Chennai, India. E-mail: [suganyam@jeppiaarinstitute.org](mailto:suganyam@jeppiaarinstitute.org)

**Balaji P**, Department of Computer Science and Engineering, Jeppiaar Institute of Technology, Chennai, India. E-mail: [balajis2479@gmail.com](mailto:balajis2479@gmail.com)

**Mohamed Thahir A**, Department of Computer Science and Engineering Jeppiaar Institute of Technology, Kanchipuram, Tamil Nadu, India. Email: [mohamedthahir.a10@gmail.com](mailto:mohamedthahir.a10@gmail.com)

**Arunkumar P**, Department of Computer Science and Engineering Jeppiaar Institute of Technology, Kanchipuram, Tamil Nadu, India. E-mail: [arunkumarp9499@gmail.com](mailto:arunkumarp9499@gmail.com)

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an [open access](https://creativecommons.org/licenses/by-nc-nd/4.0/) article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

### III. METHODOLOGY

The methodology design is based on “**Facial analysis and recognition**”. In this paper we are describing about how security is established in an area having highly confidential data’s and entering the prohibited area will be monitored without human.

The security can be established by a means of deep learning concepts. With the use of deep learning techniques, security can be established by [1] facial detection [2] facial recognition [3] intimation.

A major milestone within the development of automatic face recognition techniques was achieved by the introduction of extremely correct deep learning strategies like Deep face and Deep ID. For the primary time, face verification in free settings was achieved with accuracy surpassing human ability. This development was solely allowed for by the appearance of great improvements in hardware, like high capability GPUs. Since then, the bulk of analysis has focused on the event of deep learning-based strategies that conceive to model the human brain, via high-level abstraction achieved employing a concurrence of non-linear filters leading to feature unchangeableness. the bulk of those strategies deem more and more deep CNNs, with an emphasis on promoting scantiness and property.

### IV. RELATED WORKS

Facial recognition and verification are a region of high analysis interest because of its broad span of applications, the accessible scope for improvement in accuracy and process speed because of innovation in hardware and more and more massive and accessible databases. consequently, literature reviews are conducted sporadically to hide these changes. However, because of the large vary of face recognition ways utilized, most reviews specialize in a specific issue or set of issues, rather than addressing the complete vary of dominant ways. for instance, many recent surveys have specifically addressed a variety of methodologies that have tried to attain rotation. Other publications have reviewed face recognition techniques from numerous views. However, these surveys lack a comprehensive coverage of all presently relevant identity verification methodologies, and infrequently don't see the foremost current databases and benchmarks, like the Mega Face Challenge benchmark.

### V. DATABASE

All identity verification and detection systems need the use face datasets for coaching and testing functions. In the accuracy of CNNs is extremely captivated with large coaching datasets. For example, the development of terribly giant datasets like ImageNet, which contains over fourteen million pictures, has allowed the event of correct deep learning object detection systems. A lot of specifically, face detection and recognition datasets developed alongside benchmarks like the Mega Face Challenge[Fig 1.1]



**Fig1.1 Sample subset of mega face challenge dataset**

The Face Detection Dataset and Benchmark (FDDB) dataset and the labelled Faces within the Wild (LFW) dataset offer a way to check and rank face detection, verification and recognition systems, extremely difficult pictures in free settings. Notable and wide used datasets area unit in conjunction with info concerning their meant usage, size and the range of identities they contain. Upon analysis of the results earned by face verification and identification algorithms tested on small datasets like the LFW dataset, one is also LED to believe there remains very little scope for improvement. Once tested on sample pictures, algorithms achieving impressive results on smaller testing sets manufacture off from ideal accuracies as shown in [Fig1.2]



**Fig 1.2 Different facial action of a training sets**

The Mega Face Challenge was created in response to the saturation of tiny datasets and benchmarks, providing a large-scale public info and benchmark which needs all algorithms to be trained on the same information and tested on sample pictures, permitting honest comparison of algorithms while not the bias of personal dataset usage. However, despite the advantages bestowed by their size, each Mega Face challenge deprived by annotation problems and long tail distributions. The table1.1 shows the large collection of data sets for image processing.

**Table1.1 List of external sources contains large datasets**

Database	Website	Features
Mega face	<a href="https://cs.nyu.edu/~roweis/data.html">https://cs.nyu.edu/~roweis/data.html</a>	3,000,000 images 572,000 identities
UMass data sets	<a href="http://vis-www.cs.umass.edu/lfw/">http://vis-www.cs.umass.edu/lfw/</a>	13,233 images 3,700 identities

**VI. FACE DETECTION**

Face detection may be a basic step in biometric authentication and verification. It additionally extends to a broad vary of alternative applications together with countenance recognition, face chase for surveillance functions, digital tagging on social media platforms and shopper applications in digital technologies, like auto-focusing ability in phone cameras. This survey can examine facial detection ways as applied to biometric authentication and verification. Historically, the best obstacle faced by face detection algorithms was the power to attain high accuracy in uncontrolled conditions. Consequently, their usability applications were restricted.

However, since the face detection method, face detection settings has become commonplace. vital progress has since been created by researchers during this space thanks to the event of powerful feature extraction techniques. This review can or else target a lot of recently projected deep learning ways, that were developed in response to the restrictions and capturing salient facial info underneath at liberty conditions that embrace massive variations in resolution, illumination, pose, expression, and color. Essentially, it's the restrictions of those feature representations that have to date restricted the ability of classifiers to perform to the most effective of their ability.

Despite the increasing accuracy and speed of face detection systems, the 2 greatest challenges remain somewhat unresolved. Face detectors square measure needed to deal with giant and sophisticated variations in facial changes as shown in[Fig2.1], and effectively distinguish between faces and non-faces in unconstrained conditions. what is more, the big variation in face position and size at intervals an outsized search house presents challenges that cut back potency. This requires a trade-off between high accuracy and procedure potency. One good thing about less correct Viola Jones galvanized cascade-based face detectors over CNN strategies is their potency. so, the best demand in the current field of analysis is that the development of additional economical CNN and Principal Component Analysis (PCA) face detection techniques. part addressed this issue, achieving the present state of the art accuracy rate of 88.5% on the arduous WIDER FACE take a look at set by developing the Face Attention Network (FAN), a novel face detector designed to boost recall in cases of occlusion while not impacting on computation speed. This was achieved by exploitation associate anchor-level attention to reinforce facial features at intervals a face region, alongside random crop information augmentation to tackle occlusion and little faces.

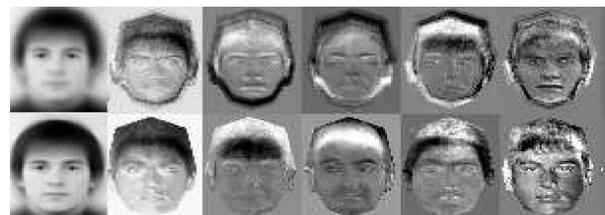


**Fig2.1 detecting facial features**

**VII. FATURE EXTRACTION**

Feature extraction sometimes happens in real time once face detection and may be thought of together of the foremost vital stages in face recognition systems, as their effectiveness relies upon the quality of the extracted options. This can be as a result of facial landmarks and fiducial points known by a given network verify however accurately options are painted. Ancient fiducial purpose locators are model based, while several recent ways are cascaded regression based mostly. Lately, key enhancements are created with the event of deep twin pathway ways, and other confidence map based mostly solutions.

Currently, the best defect gift within the realm of at liberty face alignment and fiducial purpose detection is that the lack of resolution to the matter of orienting faces no matter cause variation, and the general reliance of systems on correct face detection. The three hundred Faces within the wild info is mostly used for comparison of fiducial purpose detection ways. This face dataset is restricted, and therefore one space of improvement might embody the creation of a largescale annotated dataset containing a broad vary of at liberty facial pictures specifically designed to be used in face alignment and fiducial purpose detection applications. The facial features are extracted using PCA technique are shown in [fig3.1]



**Fig3.1feature extraction using PCA techniques**

This might improve robustness across fiducial purpose detection usually, significantly with reference to cause and expression variations, low illumination and poor quality.

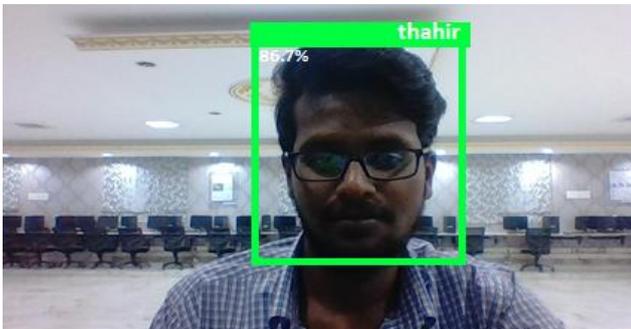
With reference to network structures, deepening neural networks might capture a lot of abstract info which can assist in detection, however it's still unclear that network layers contribute most importantly to native options relevant to fiducial purpose detection. this is often one space which can enjoy more analysis. Furthermore, the high procedure value related to localizing fiducial points remains a significant challenge in at liberty conditions.

## VIII. FACE IDENTIFICATION AND VERIFICATION

Subsequent to feature extraction, face recognition is performed. Recognition may be classified as either verification or identification. fashionable face recognition systems exploitation PCA involve deep feature extraction, and lastly, similarity comparison. A lot of specifically, verification involves comparison of matched similarity between a groundwork image and a gallery of a far-famed identity, whilst identification determines one to several similarities to work out the identity of the probe. Both these processes need sturdy feature illustration, and a discriminative classification model.

The role of the loss perform is to work out the error within the prediction. totally different loss performs can output different error values for the same prediction, and therefore verify to an outsized extent the performance of the network. Loss perform sort depends on the kind of downside, e.g. regression or classification. reduction of the error is achieved mistreatment back propagation of the error to a previous layer, whereby the weights and bias are changed. Weights are learned and changed using Associate in Nursing improvement perform, like random gradient descent, that calculates the gradient of the loss perform regarding weights, then modifies weights to cut back the gradient of the loss function. The identification of data sets are shown in [fig4.11] with accuracy value.

The sensitivity term is followed by decrease of the full error victimization the gradient descent methodology. This improves generalization and have extraction by shifting the neural activations of the hidden layers to the center high gradient space of the activation operate.



**Fig4.11** Identification of data set

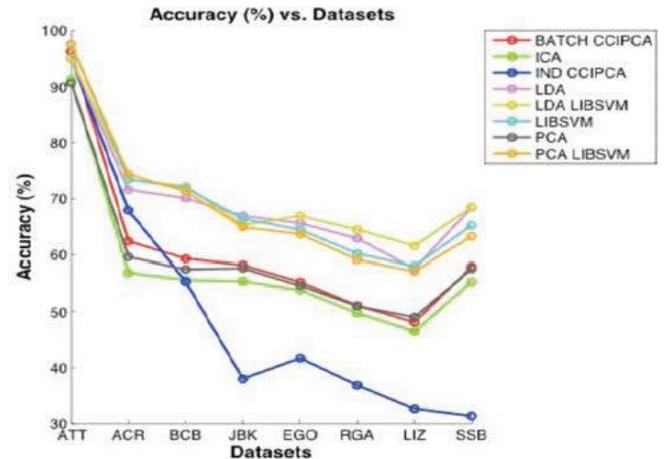
## IX. FUTURE SCOPE

In this project, we are using a smart surveillance camera to recognize the facial features of a person without his/her knowledge. This project will be more useful in industrial area and confidentiality sectors for right person to enter and access a highly secured matter.

## X. RESULT AND OUTPUT



**Fig5.1** Detection of face and recognition



**Fig 5.2** Comparison of accuracy between different datasets

## XI. CONCLUSION

This survey given an appraisal of recent face recognition methodologies, developments and challenges. It conjointly provided a comparative analysis of the obtainable databases, and connected benchmarks. It highlighted shortcomings of state of the art strategies, and evaluated responses designed to deal with these limitations, accenting outstanding problems nevertheless to be addressed. Despite drastic enhancements in accuracy of illustration thanks to the non-linearity of deep feature representations, we can with confidence conclude that there's no famous ideal facial feature that's sufficiently sturdy for face recognition in free environments. It should even be noted that solutions achieving state of the art accuracy are mostly inhibited by their dependence on sophisticated GPUs and huge databases, which means there's still adequate ought to focus analysis attention on a lot of ancient handcrafted feature representations. Refinement of pruning strategies, and step-down of training time is additionally a neighborhood requiring attention, as is specification, which might profit from increased exiguity, and selectiveness. This project is very much useful to the industries and highly confidential areas. Due to high accuracy recognition only, the authorities can be allowed into the respective centers. This will reduce the effect of unauthorized person in confidential area.

## REFERENCES

1. Y. Huang, Z. Liu, M. Jiang, X. Yu and X. Ding, "Cost-Effective Vehicle Type Recognition in Surveillance Images with Deep Active Learning and Web Data," in IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 1, pp. 79-86, Jan. 2020.
2. X. Geng, Z. Zhou and K. Smith-Miles, "Individual Stable Space: An Approach to Face Recognition Under Uncontrolled Conditions," in IEEE Transactions on Neural Networks, vol. 19, no. 8, pp. 1354-1368, Aug. 2008.
3. Y. Shan, "ADAS and Video Surveillance Analytics System Using Deep Learning Algorithms on FPGA," 2018 28th International Conference on Field Programmable Logic and Applications (FPL), Dublin, 2018, pp. 465-4650.
4. L. Kang, I. Wang, K. Chou, S. Chen and C. Chang, "Image-Based Real-Time Fire Detection using Deep Learning with Data Augmentation for Vision-Based Surveillance Applications," 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Taipei, Taiwan, 2019, pp. 1-4.
5. M. V., V. V. R. and N. A., "A Deep Learning RCNN Approach for Vehicle Recognition in Traffic Surveillance System," 2019 International Conference on Communication and Signal Processing (ICCS), Chennai, India, 2019, pp. 0157-0160.
6. J. Harikrishnan, A. Sudarsan, A. Sadashiv and R. A. S. Ajai, "Vision-Face Recognition Attendance Monitoring System for Surveillance using Deep Learning Technology and Computer Vision," 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, 2019, pp. 1-5.
7. J. Kim, Y. J. Mo, W. Lee and D. Nyang, "Dynamic Security-Level Maximization for Stabilized Parallel Deep Learning Architectures in Surveillance Applications," 2017 IEEE Symposium on Privacy-Aware Computing (PAC), Washington, DC, 2017, pp. 192-193.
8. G. Tourassi, "Deep learning enabled national cancer surveillance," 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, 2017, pp. 3982-3983.
9. K. Mughtar, F. Rahman, M. R. Munggaran, A. P. J. Dwiyanoro, R. Dharmadi and I. Nugraha, "A unified smart surveillance system incorporating adaptive foreground extraction and deep learning-based classification," 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIC), Okinawa, Japan, 2019, pp. 302-305.
10. C. Xue, P. Liu and W. Liu, "Studies on a Video Surveillance System Designed for Deep Learning," 2019 IEEE International Conference on Imaging Systems and Techniques (IST), Abu Dhabi, United Arab Emirates, 2019, pp. 1-5.
11. R. Nayak, M. M. Behera, V. Girish, U. C. Pati and S. K. Das, "Deep Learning Based Loitering Detection System Using Multi-Camera Video Surveillance Network," 2019 IEEE International Symposium on Smart Electronic Systems (iSES) (Formerly iNiS), Rourkela, India, 2019, pp. 215-220.
12. K. Mughtar, F. Rahman, M. R. Munggaran, A. P. J. Dwiyanoro, R. Dharmadi and I. Nugraha, "A unified smart surveillance system incorporating adaptive foreground extraction and deep learning-based classification," 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIC), Okinawa, Japan, 2019, pp. 302-305.



**Mrs. M Suganya** is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Jeppiaar Institute of Technology, Chennai. She has 1 year and 8 months of Teaching & 2+ years of Industrial Experience. She was awarded 6th rank in Anna University rank list among 984 candidates in her PG degree. She has published papers in Scopus Indexed Journals and also presented 10+ papers in various National and International Conferences. She has good exposure to programming skills and Cloud technologies. She has been awarded "Young Research Engineer" award for carrying out vibrant activities related to small satellites, involving students and academic institutions under the banner of UNISEC India in the areas of Nanosats, Cansats and Cubesats. Her area of Interest is Cloud Computing, in which she's doing her research work



**Balaji P** is currently pursuing his bachelor's degree in the field of Computer Science and Engineering at Jeppiaar Institute of Technology, Kanchipuram, Tamil Nadu, India. He did his schooling in Tiruvannamalai. He is particularly interested in Web Designing, App development, Mobile computing.



**Mohamed Thahir A** is currently pursuing his bachelor's degree in the field of Computer Science and Engineering at Jeppiaar Institute of Technology, Kanchipuram, Tamil Nadu, India. He did his schooling in Trichy. He is particularly interested in Web development and IoT.



**Arunkumar P** is currently pursuing his bachelor's degree in the field of Computer Science and Engineering at Jeppiaar Institute of Technology, Kanchipuram, Tamil Nadu, India. He did his schooling in Chennai. He is interested in Computer Networking and problem solving.

## AUTHORS PROFILE



**Mrs. R Dayana** is currently working as an Assistant Professor in the Department of Computer Science and Engineering at Jeppiaar Institute of Technology, Chennai. She has 7.10 years of Teaching experience. She was awarded Gold medal in her PG degree. She has handling various Computer science subjects like Compiler Design, Computer Networks, Programming in Data Structures, Object Oriented

Programming, C Programming, Mobile Computing, Adhoc Sensor Networks, Database Management Systems, Adhoc and sensor networks. She has published 6 papers in Journals and also presented 12 papers in various National and International Conferences. She is doing her research in the field of Wireless Sensor Networks and Machine learning Techniques.