

Open Access

Advances in Applied Science Research

Review Article

Face Recognition and Machine Learning

Sameer Sadiq Sofi^{*}, Chandikaditya Kumawat, Rafi Ahmad Khan

Department of Mechanical Engineering, University of Kashmir, Srinagar, Jammu andKashmir, India

ABSTRACT

Face recognition has become an important area of research from the last decade as there is much need of security for data as well as physical assets of almost every organization. Today is the age of data and with increasing voluminous amounts of data day by day, there is need of some sophisticated system to manage this vast data. Moreover, these organizations need some robust system to secure as well as manage these data resources so that only authorized users can access them. Face recognition system can be used on a large scale to meet this demand especially by using some techniques of machine learning. ML techniques promise of producing accurate estimates. In this paper, we are explaining various machine learning techniques and also explain working of machine learning model in context of face recognition.

Keywords: FRS; Machine learning; Supervised; Un supervised; AI; Expert system

INTRODUCTION

Many organizations and industrial sectors have been using machine learning from the last two decades and new smart applications are being developed using this process and is on rise. Today machine learning is affecting almost every field such as education, finance, health, banking, military and many more. Machine Learning (ML) is used in the context to learn from the data. It is being utilized by enabling machines to handle data more efficiently and in a proper way. When humans cannot quickly interpret or extract information after viewing data, then ML is applied [1]. ML is used to design and develop programs that learn and improve continuously as applied to new data. As the datasets are increasing in size, ML is also getting its scope wider. Research is on to enable machines to learn themselves [2,3].

LITERATURE REVIEW

In this section, we will discuss ML and its theories and continue with more popular and useful neural network techniques.

Machine Learning

Learning is the process of modifying and improving skill or a program based on past experience, automatically without any external human assistance. It is cognitive process through which knowledge or a skill is acquired. Artificial Intelligence (AI) played a great role in evolving machine learning by applying its computational learning theory while studying pattern recognition in images. Machine learning is a subset of artificial intelligence that helps machines to perform very crucial tasks and important applications by making data driven decisions without need of explicitly programming them. In this procedure, a model is constructed from example

Received:	25-May-2022	Manuscript No:	AASRFC-22-13652
Editor assigned:	27-May-2022	PreQC No:	AASRFC-22-13652
Reviewed:	10-June-2022	QC No:	AASRFC-22-13652
Revised:	10-October-2022	Manuscript No:	AASRFC-22-13652
Published:	17-October-2022	DOI:	10.36648/0976-8610.13.11.98

Corresponding author Sameer Sadiq Sofi, Department of Mechanical Engineering, University of Kashmir, Srinagar, Jammu and Kashmir, India; E-mail: sofi.sam4@gmail.com

Citation Sofi SS, Kumawat C, Khan RA (2022) Face Recognition and Machine Learning. Adv Appl Sci Res. 13:98.

Copyright © 2022 Sofi SS, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

inputs to perform data driven choices or predictions without following static program instructions. The model improves over time as it experiences on exposing to new data. With the help of Machine Learning deficiencies of manual knowledge acquisition techniques can be overcome by automating the learning process. We can broadly classify machine learning into two groups or methods: a) inductive and b) deductive. Deductive learning use existing knowledge and facts. It then creates new knowledge from old facts. Inductive learning generalizes and extracts new rules and patterns from big datasets rather than operating the existing knowledge.

Evolution of ML

Since machine learning is a sub filed of artificial intelligence, its history dates back to the 1950's which were cognitive science days. In that era, birth of many general techniques took place and at that time bioscience was more popular and development of perceptron was a landmark, which was modeled after neurons [4]. Later on work on neural networks began. The period of 1970's was featured as more practical programs and algorithms were developed and this achievement of designing algorithms was characterized with usage of symbolic techniques [5]. Many useful discoveries belonging to that period included 'learning of knowledge acquisition bottleneck', Buchanan and Mitchell's Meta-Dendral, and results of diagnosing soyabean. In 1980's, 'version spaces' was developed after increased analysis and evaluation of various Learning techniques [6], and much achievement was creation of decision tree algorithm. Probably Approximately Correct (PAC) learning was defined by Valiant in 1984 and the back propagation algorithm removed many limitations of perceptron [7]. Different learning techniques such as explanation based learning, case based learning and speedup learning were deeply analysed and became popular. Significant progress was on rise in decision tree and rule learning at the end of this period. During 1990's organizational data was made available and compared with algorithms. Meanwhile data mining emerged and this made it possible to compare various statistical records. Multi relational learning and Kernal methods were designed and analysed. Reinforced learning, bayesian learning, automatic bias selection, adaptive software agents, voting, bagging, boosting, inductive logic programming and applications to robotics became popular.

2000 and onwards: This period showed interaction between computational learning theory, symbolic machine learning statistics, pattern recognition and neural networks. Various new applications for ML techniques such as knowledge discovery in databases; robot control; language processing and combinatorial optimization were on rise. Also support vector machines, statistical relational learning and ensembles were touching new heights. Learning ensembles, learning complex stochastic models, scaling up Supervised Learning Algorithms (SLA) were developed to improve accuracy.

Categories of Machine Learning

Machine learning can be broadly categorized into four sub classes: These sub classes have their own respective objectives and techniques which make them capable to implement different types of learning and mechanisms.

- Supervised learning.
- Un-supervised learning.
- Semi-supervised learning.
- Reinforcement learning.

Supervised Learning

It is that type of Machine Learning in which after giving new data, a pre defined set of 'training examples' enable its ability to reach an accurate conclusion. In Supervised Learning, 'labels' are used for data and given as examples. After that a suitable learning algorithm is applied to these 'example label' pairs one by one and after predicting the label for each example by the algorithm, feedback is received and thus it depicts whether the right choice is predicted or not. With time, the algorithm will learn to approximate the exact nature of the relationship between labels and examples. After some time, when the algorithm attains full training, it then becomes capable to identify and observe a new example and predicts a better label for it. In supervised machine learning algorithms, there is need of external assistance and the input dataset is divided into training and testing dataset. The training dataset needs to be predicted as the algorithms of this kind have variable output and then dataset is classified. In the same way, mostly all algorithms learn some kind of patterns from the training dataset and then they put on them to the test dataset for classification or prediction [8]. The classification problem is one of the standard making of supervised learning, here the learner is requisite to learn, in other words, to approximate the behaviour of a function that connects a vector into one of several classes by looking at several input/ output examples of the function [9]. Here knowledge is induced from already known observations.

Decision tree: It is a predictive modelling technique in the field of machine learning and statistics which can be used to model the underlying data patterns. It is also an example of a classification algorithm. Classification algorithms are utilized in solving problems ranging from credit card theft detection to diagnosing patients with heart defects by recognizing distinctive patterns in a dataset and classifying activity based on that retrieved information [10].

Support Vector Machines (SVMs): It works on the principle of 'margin calculation'. Basically margins are drawn between the classes *via* some non-linear mapping 'input vectors' into a high dimensional feature space. The maximum separation between decision classes is given by maximum margin hyper plane and in this way classification errors are minimized. The closest training examples to the maximum margin hyper plane are termed as the 'support vectors'.

Neural networks: An artificial neural network can be constructed for a specific application, such as data classification or pattern recognition, through a learning process. These networks can be utilized with their ability to derive meaning from complicated or imprecise data and thus are able to extract patterns as well as detect trends that otherwise are too complex to be noticed by either humans or other computer methods. Hence, ANNs can be used as classifiers for various security applications and other crucial tasks.

Rough set: Rough set theory has been employed in discovering knowledge in experimental databases and datasets [11,12]. In this technique an upper and a lower approximation of a set are carried out. According to Obersteiner and Wilk, the 'rough sets theory' is measured on the assumption that some information is associated with every object of the considered universe (data, knowledge), expressed in the form of some attributes that is used for description of the object under consideration [13].

Un-supervised Learning

Page 3

Here labels are not used, instead the learning algorithm receives a lot of data and after using the tools it understands the properties of the data. From that point the algorithm is able to group, cluster, and organize the data in such a way that a human or some other intelligent algorithm can come and make sense of the newly organized data. In this way the model becomes able to learn through observations, it then finds structures in the data. When the model is given a dataset, clusters are created by automatically finding the relationships and patterns in the dataset. Unsupervised learning can mostly be used for clustering and feature reduction and as it is data driven and no usage of labels is performed, the outcomes are controlled by the data and the way it is formatted.

Principal component analysis: PCA is used to reduce dimensions between the data to make the computations faster and easier. Working of PCA can be understood by taking example of 2D data. When we plot data in a graph, it will take up two axes. When we apply PCA on that data; the data then will be 1D.

Self-Organizing Maps (SOM): SOM network is an unsupervised network and is mainly used as a clustering technique when no training data are available. The principle of clustering algorithm is that the degree of data pattern similarity within a cluster is maximized, while the similarity which these patterns have with the patterns belonging to different/other clusters is minimized. SOM technique has recently been used for the visualization and analysis of symbolic and text data [14].

Adaptive Resonance Theory (ART): Stephen Grossberg and Gail Carpenter introduced the Adaptive Resonance Theory (ART) for human cognitive information processing [15]. This

theory has led to development of neural models that are used for pattern recognition and unsupervised learning. Learning of stable recognition categories have been made possible by these models. A variety of cognitive and brain data models are being explained with the help of ART systems.

Clustering: In clustering, unlike classification the groups are not predefined. Here, the grouping is performed by finding similarities between data. A similarity metric is defined for the concerned data. A nested set of clusters is created in hierarchical clustering where the number of clusters is not known beforehand.

Semi-supervised

Semi supervised learning: Here strength of both supervised and unsupervised learning is combined. When unlabeled data is already present, effective results are produced and getting the labeled data is a difficult process. There are various categories of semi supervised learning algorithms which combine both labelled and unlabeled examples to generate an appropriate function or classifier.

Reinforcement Learning

In this type of learning decisions are made based on what to do, how to map situations to actions so as to maximize a numerical reward signal. Prior knowledge is not available to learner about which actions to take. Reinforcement learning is applicable to limited to a small set of real world situations, until it's been given a situation. It is the responsibility of the learner who needs to discover which actions yield the most reward by trying them. Reinforcement learning has two most important distinguishing features 'trial and error search' and 'delayed reward' and these are the its two most.

Q-learning: It is a type of reinforcement learning that does not solely depend on model. Q-learning uses the information observed to approximate the optimal function from where the optimal policy can be constructed. In the initial stages the learning rate is high and it gradually decreases so the learner needs to perform each state action infinitely. The Q-learning has requirements that the sum of the learning rates goes to infinity and that the sum of the squares of the learning rates is finite.

How does Machine Learning Work?

A training data set is used to create a model to train machine learning algorithm. This model is then used by ML algorithm to make a prediction as it encounters new data. After that the model is gradually tested and evaluated for accuracy and if there acceptable accuracy then the ML algorithm is deployed otherwise the model is trained further to attain accuracy with an augmented training data set again and again (Figures 1 and 2).

A Typical Machine Learning Process



Figure 1: Machine Learning Process (MLP).

Elaborating Each Step

Page 4



Figure 2: Elaborating each step of machine learning.

A machine learning system has three major building blocks:

The model, the parameters, and the learner

- Model is used for making predictions.
- The parameters are the factors that the model considers to make predictions.
- The learner's job is to make adjustments in the parameters and the model to align the predictions with the actual results.

Here we will explain each step of a machine learning system through a 'known' and unknown face example to understand how machine learning works. A machine learning model predicts whether a face is known or unknown. The parameters selected are the facial features like presence of eyes, nose, cheekbones, lips etc. of the human face. The first step is:

Gathering Data

The quantity and quality of the data dictate how accurate the model is. The outcome of this step is generally a representation of what will be used for training. We can also use pre collected data in this step. In this case, the data we collect will be feature vectors containing human face parameters.

Face encoding (feature vector)	Match (%)	known or unknown
170	30-55	Unknown
212	60-90	Known
220	65-95	Known

This will yield a table of 'face encoding', 'match %', and whether it is known or unknown. This will be our training data.

Table 1: Indicating feature vector and match percentage versus classification of face.

Preparing Data

- Spat/wrangle input data and further prepare it for training.
- Wrangled data needs to be clean with removing duplicates, correct errors, deal with missing values, normalization, and data type conversions, etc.
- After that we need to randomize data to erase the effects of the particular order in which we collected or otherwise prepared our data.
- Then data is visualized to help to detect relevant relationships between variables or class imbalances, or in other words perform other exploratory analysis.
- Lastly data is split into training and evaluation sets.

In this step, we load our data into a suitable place and prepare it for use in our machine learning training. The data is first put all together, and then the order of data is randomized. In our aim to classify face, we make a

determination of what a face is, independent of what face came before or after it. Here we do any pertinent visualization of our data, to help to see if there are any relevant relationships between different variables you can take advantage of, as well as show you if there are any data imbalances. For example, if we collected way more data points about known than unknown, the model we train will be biased toward guessing that virtually everything that it sees is known, since it would be right most of the time. However, in the real world, the model may see known and unknown an equal match, which would mean that guessing "known" would be wrong half the time. Also we split the data in two parts, the first part, used in training our model, will be the majority of the dataset. The 2nd part will be used for evaluating our trained model's performance. Same data that the model was trained on for evaluation cannot be used, since it could then just memorize the "questions". Sometimes the collected data needs other forms of adjusting and manipulation. Processes like de duping, normalization, error correction, etc., these would all happen at the data preparation step.

Choosing a Model

As different algorithms exist and are for different tasks, we need to choose the right one. Researchers and data scientists have created different models over the years and some are very well suited for image data, others for sequences like text, or music, some for numerical data, and others for text based data. In our case, since we only have 2 features, known/ unknown and match %, we can use a small linear model, which is a fairly simple to do our job.

Train the Model

- To train the model, is to answer a question or make a prediction correctly as often as possible.
- Considering the linear regression example: Algorithm here needs to learn values for m (or W) and b (x is input, y is output).
- So each iteration of the process is a training step.

In this step, we will use our data to incrementally improve our model's ability to predict whether a given face is known or unknown. This is performed on a much smaller scale with our faces images. In particular, the formula for a straight line is' $y=m \times x+b'$, where x is the input, m is the slope of that line, b is the y-intercept, and y is the value of the line at the position x. These values that we have available to us for adjusting, or 'training', are m and b. There is no other way to affect the position of the line as the only other variables are x, our input, and y, our output. In machine learning, there can be many m's since there may be many features. The collection of these m values is usually formed into a matrix, that we will denote W, for the "weights" matrix. Likewise for b, we arrange them together and call that the biases. In training process initializing some random values for W and b are involved and attempt is made to predict the output with those values. As it can be imagined, the model does pretty poorly. But by comparing our model's predictions with the output that it should produce and adjusting the values in W and b such that, we will have more correct predictions (Figure 3).



Figure 3: The values in W and b such that, we will have more correct predictions.

This process is then repeated and each iteration or cycle of updating the weights and biases is termed as one 'training step'. In case of our dataset when we first start the training, it's like we drew a random line through the data. Then with each step of the training progresses, the line moves step by step closer to an ideal separation of the known and unknown.

Error Measurement

After training the model on a defined training set, it needs to be checked for any discrepancies or errors. To do this task, we use a fresh set of data to accomplish it. The result of this test would be one of these four outcomes

- **True positive:** This outcome occurs when the model predicts the condition when it is present.
- **True negative:** When the model does not predict a condition when it is absent, this result occurs.
- False positive: The model predicts 'such a condition when it is absent'.
- **False negative:** The outcome is False Negative when the model does not predict a condition when it is present.

Keeping the above outcomes in view, the sum of FP and FN is the total error in the model.

Noise Management

Page 6

- Further, the hypothesis then created will have a lot more errors because of the presence of the noise. Noise is defined as unwanted anomalies that disguise the underlying relationship in the data set and weakens the learning process. This noise may occur due to a lot of below reasons:
- If dataset for training is large.
- When errors are already in input data.
- When data labelling has errors.
- Unobservable attributes that are not considered in the training set due to lack of data and might affect the classification process.

To approach a machine learning problem here that is the known/unknown and match percentage for instance and for the sake of simplicity, we have considered only two parameters. But in reality, we may have to consider hundreds of parameters and a broad set of learning data to solve a machine learning problem. To keep the hypothesis as simple as possible, we can accept a certain degree of training error due to noise.

Evaluate the Model

- We use some metric or combination of metrics to measure objective performance of the model.
- The model is tested against previously unseen data.
- In the real world, this unseen data is meant to be somewhat representative of model performance but it still helps tune the model as opposed to test data, which does not.
- Good train/eval split? 80/20, 70/30, or similar, this is depending on domain, data availability, dataset particulars, etc.

As our training is complete, now we should see how the model is any good, this is done using evaluation. This is where that dataset that we set aside earlier comes into play. Evaluation allows us to test our model against data that has never been used for training and this metric enables us to see, 'how the model might perform against data that it has not yet seen'. We do this to make the model a representative of how it might perform in the real world. A good rule of thumb I' can be used for a 'training evaluation split' somewhere on the order of 80/20 or 70/30 of which much depends on the size of the original source dataset. Perhaps you don't need as big of a fraction for the evaluation dataset, if there is a lot of data.

Testing and Generalization

An algorithm or hypothesis might be possible to fit well to a training set and might fail when applied to another set of data outside of the training set, and then only data is the way to judge this, *i.e.*, testing. Further, generalisation refers to how well the model predicts outcomes for a new set of data; therefore, it is essential to figure out if the algorithm is fit for new data. As we fit a hypothesis algorithm for maximum possible simplicity, it might have less error for the training

data, but might have more significant error while processing new data; we call this as 'under fitting'. But if the hypothesis is too complicated to accommodate the best fit to the training result, it might not generalize well; this is the case of 'over fitting'. In either case, the results are fed back to train the model further.

Parameter Tuning

- Parameter tuning refers to hyper parameter tuning, which tune model parameters for improved performance.
- Simple model hyper parameters may include following sub processes: What is the number of training steps, learning rate, initialization values and distribution?

After evaluation is done, we might want to see if we can further improve our training in any way. This can be done by tuning our parameters. There were a few parameters we implicitly assumed when we did our training, and now we can go back and test those assumptions and try other values. To understand this, we can explain as how many times we run through the training dataset during training. This means that we can "show" the model our full dataset multiple times, rather than just once. This can sometimes lead to higher accuracies (Figure 4).



Figure 4: An experimental process of Face Recognition and Machine Learning.

Another parameter is "learning rate". This refers to how far we shift the line during each step, based on the information from the previous training step. These values all play a role in how accurate our model can become, and how long the training takes. For more complex models, initial conditions can play a significant role in determining the outcome of training. Differences can be seen depending on whether a model starts off training with values initialized to zeroes versus some distribution of values, which leads to the question of which distribution to use. We typically refer these parameters as "hyper parameters". The raining or adjustment of these hyper parameters remains a bit of an art, and is more of an experimental process that heavily depends on the specifics of your dataset, model, and training process.

Make Predictions

Page 7

The class labels that were withheld from the model till this point can further be used to test the model as test set, a better a better approximation of how the model will perform in the real world can be traced. Machine learning is using data to answer these questions. So Prediction, or inference, can be termed as the step where we get to answer some questions. At this point of time and all this work, the value of machine learning is realized. In this approach we can finally use our model to predict whether a given face is known or unknown, given its feature vector and match percentage.

DISCUSSION

Machine Learning Applications

Machine learning has achieved much progress in tackling real world applications. The following achievements present the utilization and applications of different types of machine learning's:

Advertisement popularity: Advertisements are made more effective with the help of supervised learning by providing clicking ability more attractive. Also with a learning algorithm, match between advertisement and placement on a website is made more effective.

Spam classification: A modern email spam filter is managed with the help of supervised algorithm. With the usage of labels indicating spam, not spam, this system learns how to pre emotively filter out malicious emails so the user is saved from dangers and other hacking staff.

Recommender systems: In youtube or netflix, different video recommendation systems are often kept in the unsupervised domain. Different parameters of videos such as their duration, their genre etc, watch history of different users, watching similar videos and their relationship in the data prompt us such a suggestion.

Buying habits: Buying and selling habits of online users are contained in a database somewhere and that data is being bought and sold actively at this time. An unsupervised algorithm is applied to group customers into similar purchasing segments. This way companies market to these grouped segments and can even resemble recommender systems.

Grouping user logs: Unsupervised learning can be used to group user logs and issues and with this learning feature companies can design and use identifying central themes to issues their customers face and rectify issues, through improving a product or designing an FAQ to handle common issues. An issue with a product or submitting a bug report often fed to an unsupervised learning algorithm to cluster it with other similar issues.

Video games: Various online games are mostly played by using reinforcement learning. Alpha zero and alpha go are google's reinforcement learning application which are learned to play the game go. Another example is 'our mario' game.

Gaming sector has increasing bright future in learning through Reinforcement Learning.

Industrial simulation: Many robotic applications like 'think assembly lines' for industrial simulation can learn to complete their tasks without having to hardcode their processes. With IS, severe failures in industries can be saved and tasks can be cost effective.

Resource management: Reinforcement learning can be used to perform navigation of complex environment and it can handle the necessity to balance certain requirements. For instance, google's data centers applied reinforcement learning to balance the need to satisfy our power requirements and also efficiently and effectively cutting major costs. In bio surveillance, machine learning is applied to detect and track major disease outbreaks. For example, the RODS project involves real time collection of admissions reports to emergency rooms across western Pennsylvania, and the use of machine learning software to learn the profile of typical admissions so that it can detect anomalous patterns of symptoms and their geographical distribution over cost effective lines and intend of major accuracy.

CONCLUSION

This study discussed various techniques of machine learning that have played a major role in improving the process of face recognition. But still we face various challenges in this field and it needs much more to be done as the loopholes are evident in many aspects. There is a need to improve upon those challenges and come up with a more robust system of face recognition and this is possible through proper and efficient use of intelligent machine learning techniques especially neural networks. Now research is in progress and new techniques are being devised for extracting rules from neural networks, and combining neural networks with other intelligent techniques like genetic algorithms, fuzzy logic and expert systems to arrive at appropriate conclusions and solutions. In most cases, neural networks perform well than the traditional classification techniques with which they are compared. Deep learning, due to its vast features and high learning capacity, has tremendous scope in future and it can help humans in achieving real success in securing their valuable assets and overcome large scale destructions caused by natural calamities by getting valuable information in advance. Such technology can help in making day to day life comfortable and secured in this fast and smart world.

REFERENCES

- Richert W, Coelho LP (2013) Building Machine Learning Systems with Python. Packt Publishing, Birmingham, UK. 1-290.
- 2. Welling M (2010) A First Encounter with Machine Learning. 1-93.
- M Bowles (2019) Machine Learning in Python: Essential Techniques for Predictive Analytics. 2nd Ed. Wiley Publishers, New York, United States. 1-368.

4. Rosenblatt F (1957) The Perceptron: A Probabilistic Model for Information Storage and Organization in the Brain. Psychol Rev. 65(6):386-408.

Page 8

- 5. Mitchell TR (1982) Motivation: New directions for theory and research. Acad Manage Rev. 7(1):80-88.
- Kotsiantis S (2007) Supervised Machine Learning: A Review of Classification Techniques. Informatica. 249-268.
- 7. Chan PK, Stolfo SJ (1999) Toward Scalable Learning with Non-uniform Class and Cost Distributed data mining in credit card fraud detection. IEEE Intell Syst.14(6):67-74.
- Pawlak Z (1985) Rough sets. Int J Comp Sci. 11(1): 341-356.
- 9. Skowron A (1990) The rough sets theory and evidence theory. Fundam Inform. 13(3):245-262.
- Obersteiner M, Wilk S(1999) Determinants of Long term Economic Development: An Empirical Cross country Study Involving Rough Sets Theory and Rule Induction. Vienna: Institute for Advanced Studies.

- Grossberg S (1976) Adaptive pattern classification and universal recoding, I: Parallel development and coding of neural feature detectors and II: Feedback, expectation, olfaction, and illusions. Biol Cybern. 23(4):187-202.
- 12. Zhu GX (2009) Introduction to Semi Supervised Learning. Synthesis Lectures on Artificial Intelligence and Machine Learning. Morgan and clay pool publishers. Madison, USA. 1-130.
- Sutton SR, Barto AG (1998) Reinforcement Learning: An Introduction. Massachusetts: MIT Press, London, England. 1-352.
- 14. Sutton RS (1992) Introduction: The Challenge of Reinforcement Learning. Mach Learn. 173(1):225-227.
- 15. Mansour ED, Yishay E (2003) Learning Rates for Q-learning. Mach Learn Res. 5:1-25.