Chapter 10
Privacy Preservation of Image Data With Machine Learning

Chhaya Suryabhan Dule
Dayananda Sagar University, India

Rajasekharaiah K. M.
AMC College of Engineering, Visvesvaraya Technological University, India

ABSTRACT

The methods used to predict, categorize, and recognize complex data like pictures, audio, and texts have been popular in machine learning. These methods are the basis for future AI-driven internet providers because of unparalleled precision in deep learning methodologies. Commercial firms gather large-scale user data and perform machine learning technique. The massive information necessary for machine learning raises privacy problems. The user's personal and extremely sensitive data such as photographs and voice records are gathered and retained forever by these commercial firms and users can not limit the intents of these sensitive information. In addition, centrally stored data is susceptible to legal and extrajudicial monitoring. Many data owners use profound extensive learning by security and confidentiality. This chapter contains a practical approach that allows several parties to learn a precise model of complex systems for a specific purpose without disclosing their data sets. It provides an interesting element in utility and privacy.

DOI: 10.4018/978-1-7998-9430-8.ch010

INTRODUCTION

Privacy Preserving Machine Learning for Image Data

Machine learning (ML) is an intelligence branch that consistently uses algorithms to synthesize the links between knowledge and information (Pannu & Student, 2008). For illustration, ML systems on automated speech processing may be developed to translate acoustic information into the conceptual system, which consists of a collection of words in a series of spoken data. An Internet search, ad insertion, credit assessment, financial sector prognosis, DNA sequence analytics, comportment analyses, intelligent coupons, medication research, weather prediction, huge data assessment, and many more apps are already standard in machine training. ML will decisively develop a variety of user-centred technologies. The advancement of machine learning means that fundamental linkages are characterized in wide-ranging information so that big data analysis, behaviour pattern identification, and information development solve issues. In order to represent changes in operational behaviour, machine learning methods may also be trained to categories the changing conditions of a procedure. As security features influence innovative concepts and capabilities, machine learning techniques may recognize interruptions, re-design the latest systems, and educate them to adjust and co-develop new information (Mulla, 2013; Sharma, 2017).

Supervised Learning

Supervised learning (Figure 1) is a set of learning approaches that uncover links between independent characteristics and a chosen dependency characteristic (the label). Learning supervised utilizes a training dataset to create predictive models by using input data and output values. A database can be used to forecast the output values. The effectiveness of supervised learning models depends on how large and varying the training data is so that new datasets can be more generic and more predictive. The majority of induction algorithms come within the area of supervised learning (Kshirsagar et al., 2016b).

Unsupervised Learning

Unsupervised learning includes techniques of learning which group instances lacking a particular property. In general, this method includes learning organized data patterns by eliminating pure unstructured noise. Algorithms for clustering and reduction of dimensionality are typically uncontrolled (Singh & Mishra, 2021).