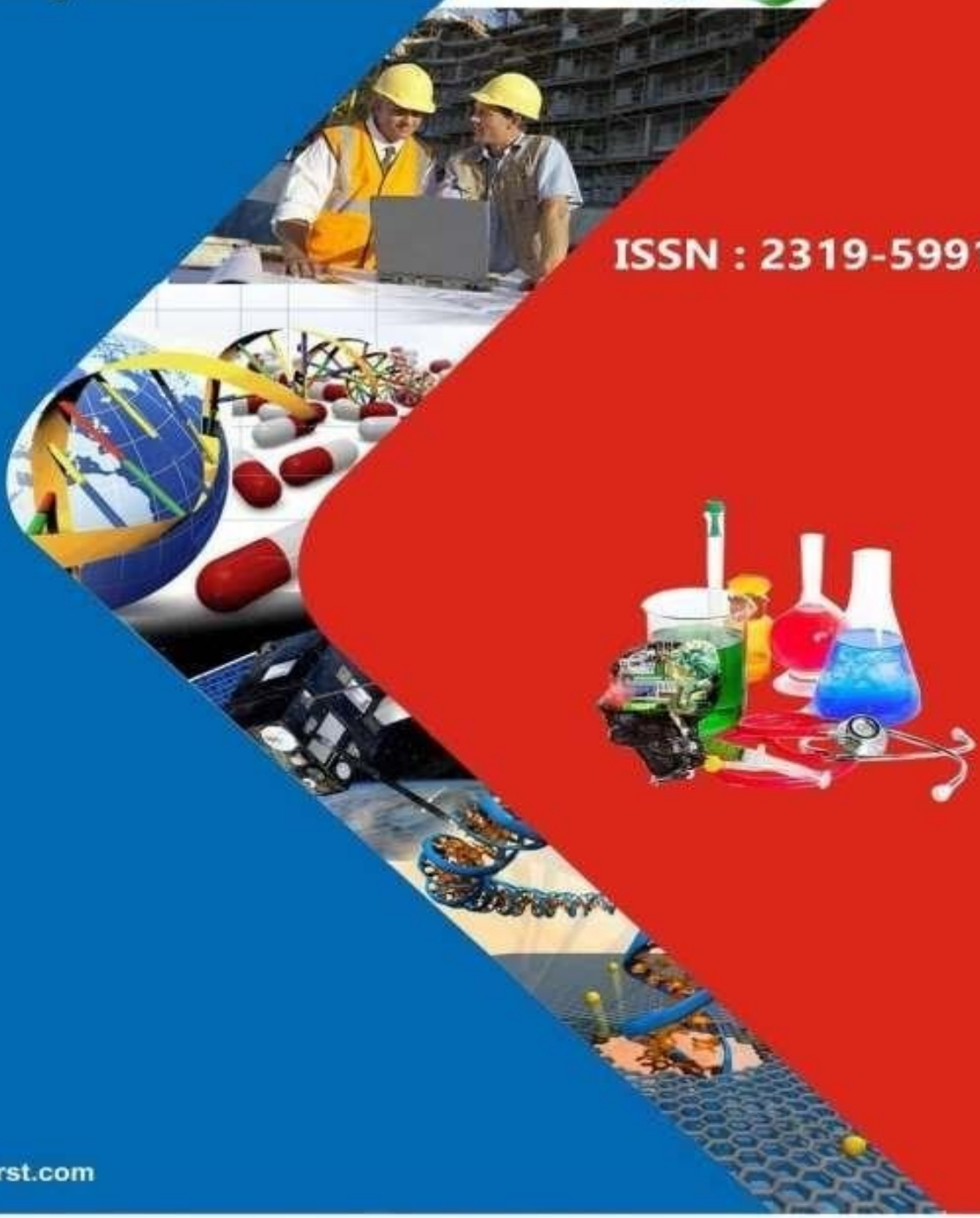
# International Journal of Engineering Research and Science & Technology

IJERST

ISSN : 2319-5991



www.ijerst.com

Email: editor@ijerst.com or editor.ijerst@gmail.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

# Signature Forgery Detection

**SK. Naga Rehmathunnisa[1], Gampala Sailaja[2], G. Sowjanya[3], L.Naga Cherishma[4]**

[1] Associate Professor, Dept. of Computer Science & Engineering, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada-521108

[2,3,4,] Students, Dept. of Computer Science & Engineering, Vijaya Institute of Technology for Women, Enikepadu, Vijayawada-521108

Email id: shaikrehmathunnisa@gmail.com[1] , gampalasailaja26@gmail.com [2], godavarthisowjanya6@gmail.com[3], nagacherishmalanka@gmail.com[4]

**Abstract:**

Every individual has their own signature, which is primarily used for peraonal identification and Verification of vital papers or legal transactions. Even today, in many commercial instances, such as check payment, register office the signature verification process is still relied on a single known sample being reviewed by a human. The probability that the two signatures made by the same person is very less. So, forgery detection becomes a huge task. The signatures that undergoing verification is not only difficult but also time consuming, especially when they are signed offline and no information about the procedure is available. To prevent the possibility of theft or fraud, a system that can distinguish between real and faked signature is required. Before recognizing the signature is forged or not certain stages of pre-processing must be done for the images (signature) are acquired from the data set since it is in raw form. The proposed work is based on off-line signature verification using deep learning model incorporating Convolution Neural Network (CNN) and novel method for extracting local features. This method can be used in various organizations where the number of individuals is confined so the model can train those before detecting any forged signatures in the future

Keywords: Convolution Neural Network (CNN), Forgery Detection, off-line signature

## Introduction

In an era where digital transactions and document authentication are integral parts of our daily lives, the vulnerability of signatures to forgery poses a significant threat to the security and trust worthiness of these processes. The Signature Forgery Detection project emerges as a pivotal response to this challenge, seeking to revolutionize signature verification through the application of cutting-edge technologies.

This project recognizes the escalating risks associated with signature forgery and aims to provide a sophisticated solution that goes beyond traditional methods. By harnessing the power of artificial intelligence, machine learning, and advanced image processing techniques, the Signature Forgery Detection system endeavours to elevate the standards of signature authentication. The project addresses the multifaceted nature of signature forgery, taking into account the evolving sophistication of fraudulent techniques. It seeks to create a comprehensive and adaptive system capable of not only identifying common forgery patterns but also learning and adapting to new, emerging threats over time. By offering a robust and dynamic approach to signature verification, the project aims to instill confidence in various sectors, including banking, legal, and administrative domains, where the integrity of signatures is of paramount importance. The endeavour is not merely a technological advancement but a strategic move towards fortifying the foundation of trust in digital transactions and document authentication processes.In essence, the Signature Forgery Detection project represents a leap forward in the ongoing battle against cyber threats, contributing to the broader narrative of bolstering security measures in an increasingly interconnected and digitally dependent world.

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

**Objective**

The primary objective of this project is to create a reliable and automated system for detecting forged signatures, providing a valuable tool for businesses, financial institutions, and legal entities. The Signature Forgery Detection project encompasses a set of comprehensive and strategic objectives, each designed to address specific challenges in the existing system and contribute to the development of a robust and adaptive signature authentication solution.

## LITERATURE REVIEW

Signature forgery Is a pervasive issue with profound implications across various domains, including finance, legal documentation, and security. The ability to detect forged signatures is of paramount importance to ensure the integrity of transactions, legal agreements, and personal identification. In recent years, the advancement of computational techniques, particularly in the realms of image processing and machine learning, has provided new avenues for enhancing the accuracy and efficiency of signature forgery detection. **G. Lourenco and R. Santos (2009):** This paper provides an overview of offline signature verification and identification techniques, including various methods and challenges. **V. Ramachandran (2011):** The authors review different approaches to signature verification, covering both online and offline methods. **R. Singh and M. Kumar (2015):** The authors review the literature on signature verification, discussing signature acquisition, feature extraction, and classification techniques. **M. Z. Rashid etal. (2021)** This review focuses on online handwritten signature verification, discussing different techniques and challenges associated with online signatures. Signature forgery detection has been a subject of extensive research, with numerous studies contributing to the development of robust and accurate methods for authenticating hand written signatures.

## EXISTING SYSTEM

Currently, many organizations rely on manual inspection and subjective judgment to identify forged signatures. This method is time-consuming, prone to errors, and lacks the efficiency required to keep up with the increasing sophistication of forgery techniques. The existing system falls short in providing a comprehensive and reliable solution to the rising threat of signature fraud.

## SYSTEM DESIGN AND ANALYSIS

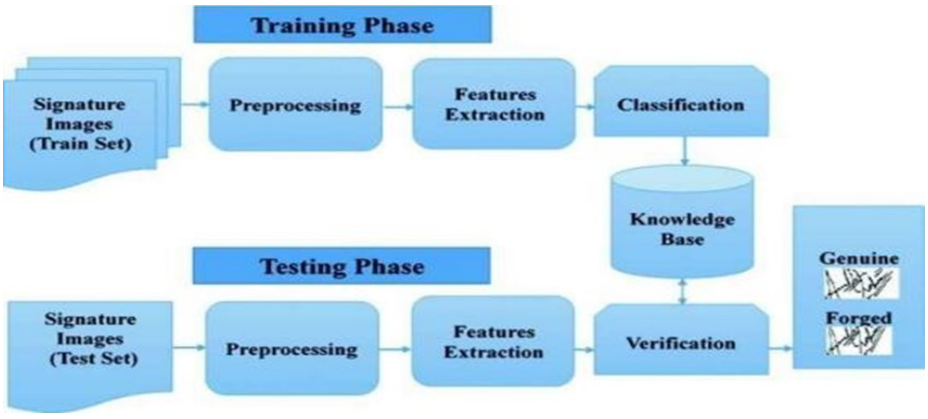



**Figure: Architecture**

**Use Case Diagram**

A use case diagram in the Unified Modeling Language (UML) is a type of behavioural diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases.

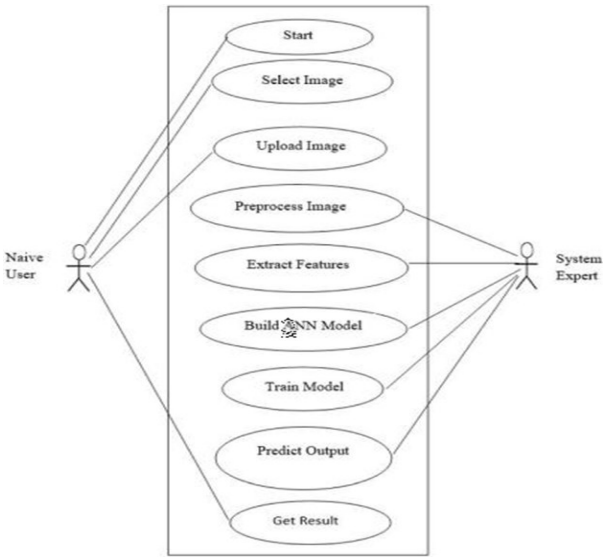



**Figure:** Use-Case Diagram

**Data Flow Diagram**

The DFD is also called as bubble chart. It is a simple graphical format that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system. DFD show the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow Data flow diagrams represent systems by use of a sparse number of symbols. Systems processes are symbolized by circles, entities external to the system which interact with the system are represented by rectangles, and data stores are denoted by an open-ended rectangle.

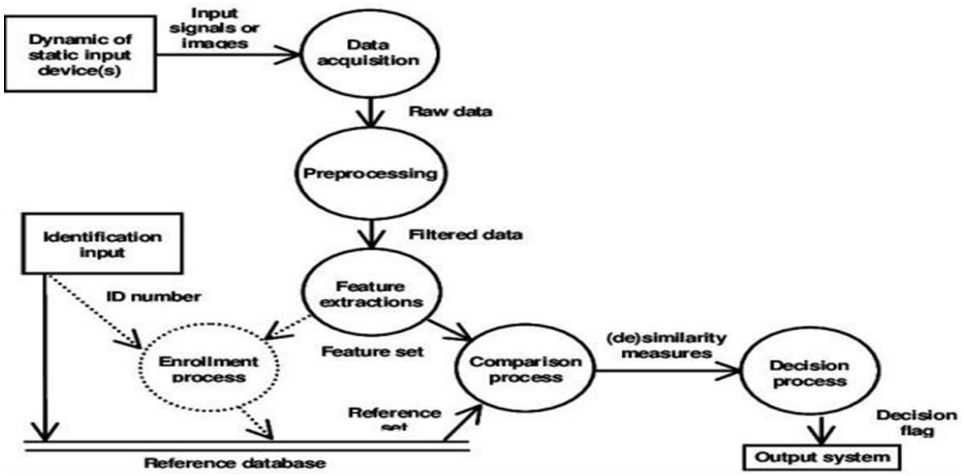



**Figure: Data Flow Diagram**

**CLASS DIAGRAM**

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

In software engineering, a class diagram in the Unified Modeling Language (UML) is a type of static structure diagram that describes the structure of a system by showing the system's classes, their attributes, operations (or methods), and the relationships among objects. The class diagram is the main building block of object-oriented modeling. It is used for general conceptual modeling of the structure of the application, and for detailed modeling, translating the models into programming code. Class diagrams can also be used for data modeling. The classes in a class diagram represent both the main elements, interactions in the application, and the classes to be programmed.

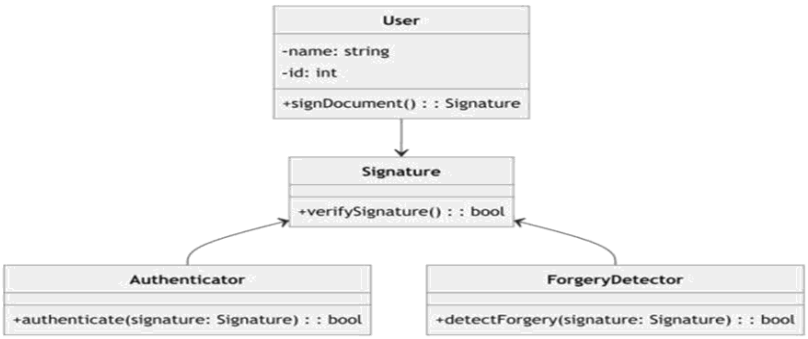



**Figure:** Class Diagram

**DATASET:**

These datasets contain signatures of 12 different persons. They have 5 copies of each real and forged signatures. Sometimes signatures made by same person may vary hence we are using 5 copies of each person's signatures

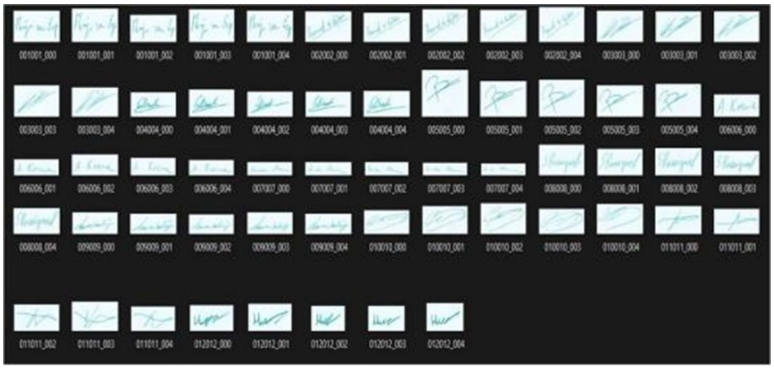


**Figure:** Sample dataset

A forged dataset is one that has been intentionally manipulated or created with false information, usually with the intent to deceive or mislead. This can involve fabricating data points, altering existing data, or generating entirely fictional data. Forged datasets are often used maliciously for various purposes such as academic fraud, spreading misinformation, or training biased machine learning models. On the other hand, a real dataset contains authentic and accurate information collected from observations, experiments, surveys, or other legitimate sources. Real datasets are essential for conducting meaningful analysis, research, and decision-making in various fields, including science, business, and government.

**CNN ALGORITHM**

CNN, or Convolutional Neural Network, is a type of deep neural network designed for tasks involving visual data, such as image recognition, object detection, and image classification. The architecture of

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

CNNs is inspired by the visual processing that occurs in the human brain. The convolutional neural network (CNN) algorithm is a deep learning model tailored for analysing structured data like images.

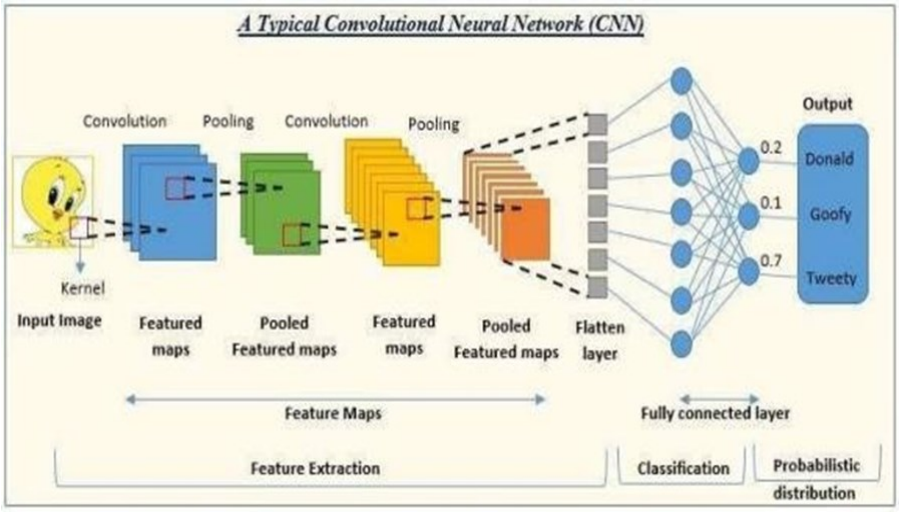
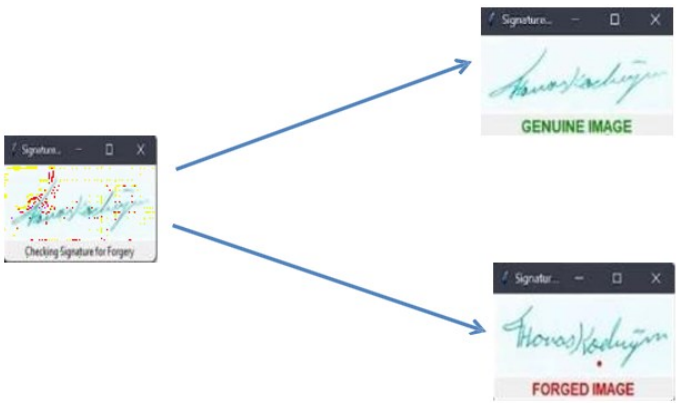



Figure: CNN Architecture

## OUTCOMES OF THE PROPOSED SYSTEM

Unit testing is usually conducted as part of a combined code and unit test phase of the software life cycle, although h it is not uncommon for coding and unit testing to be Conducted as two distinct phases test strategy and approach. Field testing will be performed manually, and functional tests will be written in detail. Software integration testing is the incremental integration testing of two or more integrates of software components on a single platform to produce failures caused by interfaced effects. The task of the integration test is to check that components or software applications e.g: components in a software system or one step up software application sat The company level interact without error.




Deep learning and machine learning are considered the breakthroughs that have happened in this century. It helps in achieving better accuracy and efficiency among the models by extending the depth and complexity of the existing network layers. The major important point to be noted is in finding the genuine datasets which are used to train the algorithms so that high output is obtained. Dr Santosh Kumar Bharti (2020) proposed the use of machine learning algorithms for digital signature forgery. The paper uses the CNN method along with the SURF algorithm & Harris corner detection algorithm. It proves that using machine and deep learning algorithms can be used for getting higher accuracy and precision and thus ensure them getting the results. Here the associated accuracy hits near 85%. During

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

signature forgery detection it has an accuracy of 85-89% while during signature detection it has 90-94%. Lu'lu'il Ayunin Fakhiroh (2021) talks about a methodology for finding the accuracy of offline signatures based on mobile devices. This paper propped a new approach based on CNN in mobiles. It trains two different networks separately to test the same dataset. It provides the highest accuracy for training with 99.33%. During testing, this has provided a 100% accuracy rate with a loss value of 0.032. But the drawback that was found was it had a loss value during verification cases greater than the normal cases. Another drawback that was present was the testing is more optimal and more suitable for mobile applications.

## CONCLUSION

The primary goal of this project is to create a signature verification system that can accurately distinguish between genuine and forged signatures. Automation is a key focus of this project. The system is designed to process large volumes of documents efficiently, reducing the need for manual signature verification. We have developed this system to eradicate some of the problems of existing system and to improve the accuracy of results. As achieving a high level of accuracy in signature forgery detection is critical to the project's success. The system will be trained on a diverse data set of genuine and forged signatures to ensure its reliability. Manually written signatures are collected and some unique features are extracted to create knowledge base for each and every individual. This project will provide an effective solution for signature forgery detection, enhancing security and trust in various sectors reliant on document authentication. It will also open up opportunities for further research into improving the robustness and efficiency of signature verification systems. Convolutional neural networks (CNNs) have emerged as powerful tools for image- related tasks, demonstrating remarkable performance in tasks such as image classification, object detection, and semantic segmentation. Through their hierarchical architecture and ability to learn complex patterns from raw data, CNNs have revolutionized fields like computer vision and machine learning, enabling advancements in areas ranging from medical imaging to autonomous vehicles. The extensive research and development in CNNs have led to the creation of sophisticated models capable of achieving state-of-the-art results on various benchmark datasets.

## FUTURESCOPE

The project can progress further and can be improved by the following methods to improve the accuracy of signature forgery detection:

- It can be improved further by improving the data set quantity and quality to train the model.
- The training model can be trained in multiple epochs to produce more accurate results
- It can use more types of algorithms when training the model while including features extracted in different scenarios.
- It can be used in combination with online signature authentication methods to produce a higher accuracy of signature forgery detection if it involves crucial signatures of important dignitaries.

References:

1. Offline Signature Verification and Recognition:An Overview "by Yefeng Zheng(2016).
2. Offline Signature Verification Using Writer- Independent Feature Learning "by PalakJain (2017)
3. Offline Signature Verification and Identification Using Convolutional Neural Network"by M.A. Hakak, etal. (2018)

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com

Vol. 21, Issue 1, 2025

4. "Deep Representations for Iris,Face,and Fingerprint Spoofing Detection"by U. Uludag,etal. (2018)