Detection of Fraudulent Degree Certificates using Histogram Features and AI Techniques

Sarala M[1*], Muralidhara B L[2], Suresh R[3]

[1]Department of Computer Science(PG), Jyoti Nivas College, Bangalore, India
Email: sarala@jyotinivas.org
[2]Department of Computer Science and Applications, Bangalore University, Bangalore, India
Email: murali@bub.ernet.in
[3]Department of Statistics, Bangalore University, Bangalore, India
E-mail: sureshr@bub.ernet.in

ABSTRACT

Artificial Intelligence (AI) techniques support detecting fake regions in high-dimensional datasets such as images and videos through fake detection methods. The scope of educational credential forgery is required for authenticating it for admission, and recruitment. In this study, we detected forged educational credentials using machine learning (ML) algorithms such as Support Vector Machine (SVM), NaïveBayes, Logistic Regression, K-Nearest Neighbours (KNN), Random Forest, and Decision Tree. We have collected the primary dataset of degree certificates, and extracted the features using the histogram features (HF): skewness, mean, kurtosis, standard deviation, and entropy from preprocessed certificate images, as structured data is essential for ML models. Further, we conducted a detailed empirical evaluation by fine-tuning the hyperparameters of each model to improve classification performance. Among the algorithms tested, Random Forest attained a good accuracy of 99.4%, surpassing the other methods in detecting fraudulent degree certificates.

Keywords: classification, degree certificate, fraudulent detection, histogram features

1. Introduction

Educational institutions and industries need authentication certificates from students and job seekers to know the genuineness of the degree. The creation of fake credentials is a social issue around the globe, and it has existed since the advancement of software technology. The manual authentication process consumes human resources and time. To report this problem, our research study focuses on identifying fraudulent degrees using ML algorithms, which have wide applications in healthcare, spam detection and outlier detection, like machinery fault detection.

Generally, image forgery detection falls under two approaches: Active approach, focused on digital signature, and digital watermarks; passive approach includes copy-move: moving image region from one location to another, splicing: combining two or more image regions to create a new image; and resampling techniques create the template or image as it was previously. Supervised algorithms trained with labelled datasets. Unsupervised methods group the features using a clustering algorithm on unlabeled datasets. Our approach falls under the passive and resampling techniques and follows the supervised algorithms. Histogram features(HF) are highly used in medical image analysis, and ML algorithms used in disease diagnosis. It was chosen owing to their proven effectiveness in image-based forgery detection. In this study, we have extracted the features of credentials using HF, and used supervised ML algorithms to detect counterfeit degree certificates, and they were classified as either ‘genuine’ or ‘fake’, using supervised algorithms. This is a novel study in the detection of forged credential ls.

© The Author(s) 2026
P. Bagchi et al. (eds.), *Proceedings of the International Conference on Information Systems Design And Intelligent Applications (ICISDA 2026)*, Advances in Intelligent Systems Research 215,
https://doi.org/10.2991/978-94-6239-821-4_8

2. Literature Review

Machine Learning(ML) algorithms are used in classification tasks such as recognition of images, patterns, diagnosing diseases into normal and abnormal; time series analysis such as weather prediction, rainfall prediction, and stock market analysis; and fraud detection such as credit card fraud in banking, and machinery fault detection. We found a few research works on forged credentials detection. Hence, we focused on fake image detection, fake currency detection, and the extraction of histogram features. Further, we reviewed the literature emphasizing binary classification in healthcare and plant domains, time series analysis, and network anomaly detection.

Fraud detection is categorized into two types: anomaly detection and misuse detection. Anomaly can be detected using supervised, unsupervised, semi-supervised, and data reduction approaches and algorithms. It widely used in telecommunication fraud, automobile insurance, credit card fraud, healthcare insurance fraud, and online auction fraud. It can be detected through logistic regression, Decision Tree, SVM, Artificial Neural Network(ANN), and genetic algorithms[1]. Josephine et. al. proved that ML algorithms efficiently handled the fraud detection. Random Forest outperformed well in detecting fraudulent cases [2]. An adaptive segmentation algorithm was applied to detect forged educational credentials [3].

Deep learning techniques are widely used in recognizing fake currency notes(FCN). The Convolutional Neural Network(CNN) model acknowledges forged currency of 500 and 2000 [4,5]. A novel approach to notice forged Indian currency using a deep CNN model, which obtained 96.6% accuracy. This approach extracted the features, followed by image transformation, edge detection, and segmentation. It identified the actual and forged ones by using pattern matching method[6]. The VGG-16 model was used to recognize the fake currency of 500, and 2000 [7]. The AlexNet model acknowledged the FCN of 500,2000, 200, and 50 [8]. The performance of two pretrained models, AlexNet and ResNet18, was compared in the recognition of FCN. Further, customized CNN model was proposed [9].

As Histogram features are commonly used in image retrieval and medical imaging [10-13], we focused on applications of histogram features. Histogram-based features are trained using a deep CNN to analyze the grain size [14], anomaly detection [15], analyzing audio from laryngoscope images [16], and diagnosing kidney diseases [17].

The subsequent works are show the impact of ML algorithms: used in healthcare for diagnosing COVID-19[18, 19], cirrhosis, fibrosis, and hepatitis [20], and metabolomics [21]; analyzing the quality of Soybean seed[22]; classifying neutron stars[23], rainy days[24]; network anomaly detection[25], and traffic attack [26].

This literature review identified that ML algorithms are used in a widespread applications, with healthcare being one of the most highly used. Histogram features are employed to increase the efficiency in image processing. Due to limited work in detecting educational credentials, we focused on fake currency detection. This study fills the gap in the detection of fraudulent degree certificates. Further, this study will be useful in detection of forged images, currency, and so on.

Our primary contribution is identifying forged credentials through a comparative study of various ML algorithms with hyperparameter fine-tuning. The datasets acquired, methodology followed, and the empirical study's outcomes are discussed in next Sections.

3. MATERIALS AND METHODS

3.1 Materials

The four hundred scanned copies of the genuine degrees were collected from Bangalore University to conduct the empirical study. The dataset was scanned using the FUJITSU scanner with 300 dpi (dots per inch), and stored as image files. Additionally, a hundred fabricated credentials were created using Adobe Photoshop ID3 for research purposes. Additionally, we have created three hundred samples from these fabricated credentials using data augmentation techniques such as brightness, and rotation for research purposes. The dataset contains four hundred genuine and fake samples. We have split the dataset into 4:1 ratio for training and testing. The genuine and fake samples are exposed in Figure 1, the count of these samples is represented in Figure 2.



(a) (b)

Figure.1 Data samples: (a) genuine, (b) fake

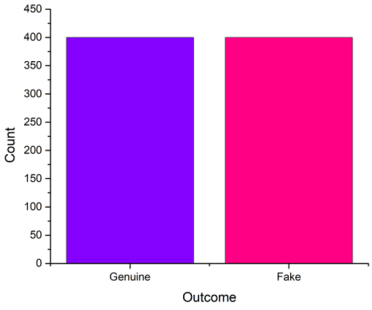


Figure.2 Data samples count: (a) genuine, (b) fake.

3.2 Methodology

The supervised ML algorithms classify degree certificates as either 'genuine' or 'fake'. The methodology is illustrated in Figure 3. We have used the Jupyter notebook platform to train ML algorithms. The datasets were preprocessed to extract the histogram features. These features were put in storage. Further, the ML models were trained to classify the degree certificate. Finally, the performance of algorithms was evaluated using statistical metrics. The entire methodology of detecting fraudulent degree certificate is defined in Algorithm-1. In preprocessing both genuine, and fake credentials are converted to grayscale from RGB, and resized to 256 ^{x} 256. The extracted HF features were moved to a database(DB). Generally, the datasets are split in a ratio of 4:1 to train ML

models and test them. We have trained using six ML algorithms. When the accuracy of model is not greater than ninety-nine, which is a good accuracy, we fine-tuned the hyperparameters of the model. Finally, we evaluated the performance of model using confusion matrix, and AUC score.

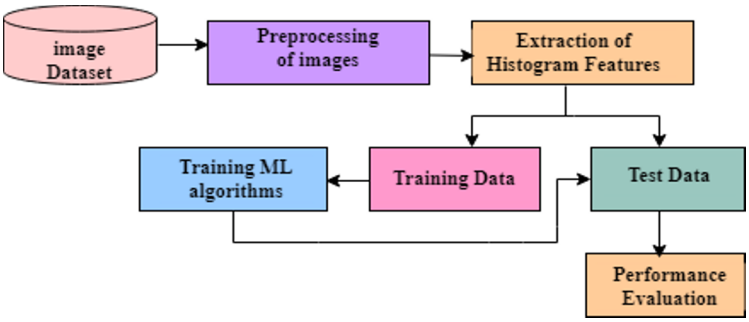


Figure.3. Proposed methodology

Algorithm 1: Fraudulent detection of degree certificates

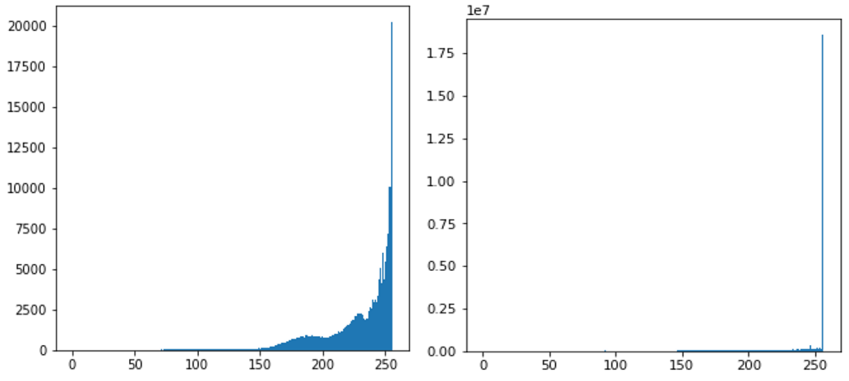
Dataset: scanned image dataset of degree certificates
Input: [{e_1, e_2, . . ., e_m}] //m=800
Initilize j=1
//Preprocessing
1. Repeat read img until img in list
   gray ← convert_to_gray(img)
   img ← Resize(gray, (256,256))
   End Repeat
2. DB ← extracted histogram features //DB-Database
3. Split the data samples into 4:1 ratio to train and test
4. Repeat j until j reaches 6 :
5. $Model_j$ ← train the ML model with alg_j
6. $Pred_j$ ← $Model_j$. predict(test_data)
7. If accuracy($Pred_j$)> 99:
   j=j+1
8. Else:
   Fine-tune the hyperparameters
9. End Repeat j
10. Evaluate the performance

Preprocessing*:* The image datasets were resized to 256 ˣ 256 from raw size to train ML algorithms, and converted from RGB to grayscale to reduce the computational time.

Histogram analysis: A Histogram is a graphical view of the data, used to show the frequency distribution of numerical data, or an image based on pixel intensities. It is generally used with continuous numerical data. It is widely used in applications to analyze sales data, exam scores, image analysis, and manufacturing fault detection. The probability score is calculated as mentioned in Eq.1. The histogram analysis of both genuine and fake samples is illustrated in Figure.4

$$P_u(x) \triangleq Prob[u = x] \approx \frac{no.of\ pixels\ with\ gray\ level\ x}{total\ no.of\ pixels\ is\ the\ region} \quad (1)$$

where, u be the random variable, and x denotes gray level(L) form 0 to L-1.



(a) (b)

Figure.4. Histogram analysis of data sample: (a) genuine, (b) fake

Histogram Features: The five histogram features, such as skewness, mean, kurtosis, standard deviation, and entropy, were extracted from the preprocessed image dataset using the HF method. In this, mean μ, and standard deviation σ are mentioned in Eq.2, and Eq.3. Further, inequality, and peak of pixel intensity are mentioned in Eq. 4. and Eq. 5. The randomness of the image measured by Eq. 6. The correlation between the input features and outcome is illustrated in Figure.5

$$\text{Mean}(\mu) = \sum_{b=1}^{L} \text{b}\, P(b) \tag{2}$$

$$\text{Stddev}(\sigma) = \sqrt{\sum_{b=1}^{L} (b-\mu)^2\, P(b)} \tag{3}$$

$$\text{Skewness} = \frac{1}{(\sigma)^3} \sum_{b=1}^{L} (b-\mu)^3\, P(b) \tag{4}$$

$$\text{Kurtosis} = \frac{1}{(\sigma)^4} \sum_{b=1}^{L} (b-\mu)^4\, P(b) \tag{5}$$

$$\text{Entropy} = -\sum_{b=1}^{L} P(b)\, log_2[P(b)] \tag{6}$$

where, L represents the number of bins, $P(b)$ is the probability distribution of bin b.

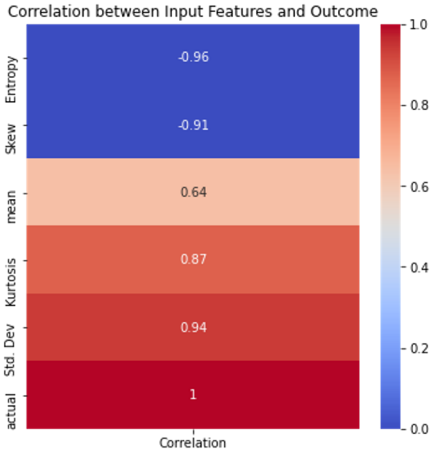


Figure 5. Correlation between Input features and outcome

Classifier: The supervised ML classifiers are trained with labelled datasets. Here, we employed six classification algorithms: Logistic Regression, SVM, Naïve Bayes, Random Forest, KNN, and Decision Tree. SVM constructs the hyperplane to classify the data samples by boundary, and is efficient in high-dimensional spaces. The optimisation problem to detect outliers is stated in Eq.7. Here, the performance of SVM was compared by varying the kernel methods such as 'linear', 'rbf', 'poly', 'sigmoid', and 'precomputed'.

$$\text{opt} = \underset{w,b}{\text{minimize}} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{m} \varsigma_i \quad (7)$$

Subject to constraint:

$$y_i\left(w^T x_i + b\right) \geq 1 - \varsigma_i \text{ for i} = 1,2,\ldots.n$$

Where, y_i is the actual class label, x_i is the feature vector, n is the number of training samples, ς_i is the slack variable, and C denotes the regularisation parameter.

Naïve Bayes(NB) is commonly used in spam detection or document classification based on the probability. The naiveBayes theorem mentioned in Eq.8, and predicted value is represented in Eq.9. This study compared various Naïve Bayes algorithms to analyze the efficiency of the model.

$$P(y|x_1, x_2, \ldots. x_n) = \frac{P(y).\prod_{i=1}^{n} P(x_i|y)}{P(x_1)\,P(x_2)\ldots P(x_n)} \quad (8)$$

$$\hat{y} = \arg\max_y P(y).\prod_{i=1}^{n} P(x_i|y) \quad (9)$$

where y and $\hat{y}$ are actual and predicted values, x is the feature, and n represents the number of features.

Decision Tree forms a tree based on features. It follows 'entropy' and 'gini' criterion methods as illustrated in Eq. 10, and Eq.11. Random Forest supports a parallel ensemble classification technique. As, decision tree, it utilizes metrics such as 'entropy' and 'gini'.

$$\text{Entropy} = -\sum_{i=1}^{n} p(x_i)\, log_2\, p(x_i) \quad (10)$$

$$\text{Gini} = 1 - \sum_{i=1}^{c} p_i{}^2 \quad (11)$$

Logistic Regression works based on the sigmoid function that estimates the parameters, as stated in Eq.12. The efficiency was evaluated using the 'solver' parameter, including 'lbfgs', 'liblinear', 'newton-cg', 'newton-cholesky', 'sag', and 'saga'. All solver methods executed well except 'sag' and 'saga'.

$$\sigma(z) = \frac{1}{1+e^{-z}} \quad (12)$$

where, $z = \sum_{i=1}^{n} w_i\, x_i + b$, w is the weights, x is the features, b represents bias value.

KNN is a non-parametric, and supervised classifier algorithm. Here, we have fine-tuned the number of neighbours i.e., n., and chosen n=3. The difference between each point is calculated using the Euclidean metric as mentioned in Eq.13.

$$d = \sqrt{((x_2 - x_1)^2 + (y_2 - y_1)^2)} \quad (13)$$

3.3 Performance analysis

To evaluate the competence of the classification task, the model's prediction accuracy is a crucial metric to examine the generalized prediction of ML models. Further, one can assess the model's efficiency using AUC score. The statistical metrics, such as recall, accuracy, F1-score, and precision, are mentioned in Eqs. 14 -17.

$$\text{Precision} = \frac{TP}{TP+FP} \quad (14)$$

$$\text{Recall} = \frac{TP}{TP+FN} \quad (15)$$

$$\text{F1-score} = 2 \times \frac{precision \times Recall}{Precision + Recall} \quad (16)$$

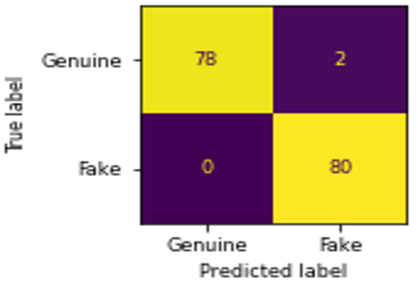
$$\text{Accuracy} = \frac{TP + TN}{TP+TN+FP+FN} \quad (17)$$

4. Results and Discussion

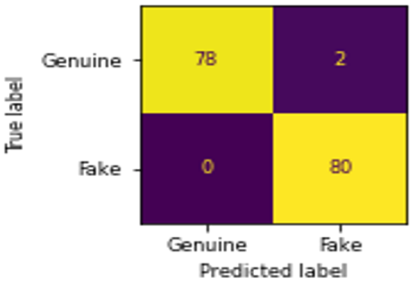
The comparative study of ML algorithms by fine-tuning hyperparameters is represented in Table 1. The six classifiers' performance is discussed as follows: (i) Random Forest: it outperforms other algorithms since it learned the features, and classified by voting criteria. (ii) SVM: SVM with a 'linear' and 'rbf' kernel performed better than others. (iii) Naïve Bayes: Gaussian NB performed better than others, and Bernoulli NB works well only with discrete features, which achieves less accuracy, (iv) Decision Tree: In decision tree both 'entropy' and 'gini' criterion performed well, (v) Logistic Regression: it provides the best result all solver except 'sag' and 'saga', these solvers are suitable for multinomial logistic regression. Hence, these two solvers provide less accuracy in binary classification. (vi) KNN: it works well when the number of neighbours is odd; here we used n value as 3. The confusion matrices of all algorithms are illustrated in Figures 6(a) – 6(f). The AUROC curve is shown in Figures 7(a) and 7(b), and the efficiency of ML algorithms is presented in Figure 8.

Table. 1. Comparative study of ML algorithms

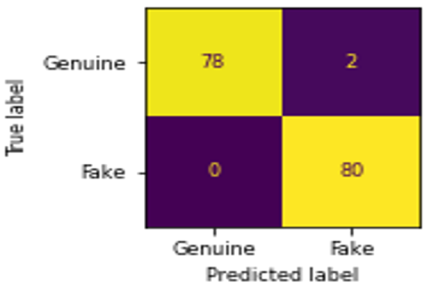
Sl. No	Classifiers	Method /Parameter	Parameters used	Accuracy
1.	SVM	Kernel	linear	98.8
			poly	97.5
			rbf	98.8
			sigmoid	56.4
2.	Naïve Bayes (NB)	Gaussian NB	var_smoothing =1e-09	98.2
		Multinomial NB		80.0
		Complement NB		80.0
		Bernoulli NB		50.0
3.	Decision Tree(DT)	Criterion	entropy	98.2
			gini	98.2
4.	Logistic Regression (LR)	Solver	saga	79.4
			sag	80.0
			liblinear	97.0
			lbfgs	97.0
			newton-cholesky	97.0
			newton-cg	99.4
5.	KNN	Number of neighbours	3	98.2
6.	Random Forest(RF)	Criterion	entropy	99.4
			gini	99.4



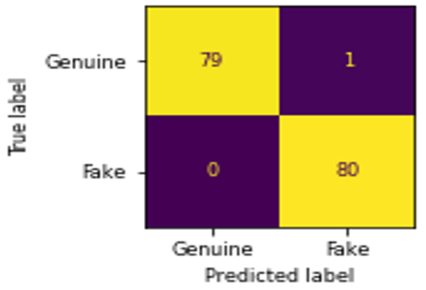
(a) SVM



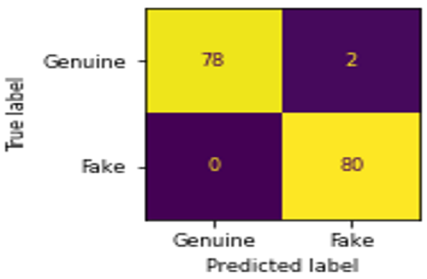
(b) NaiveBayes



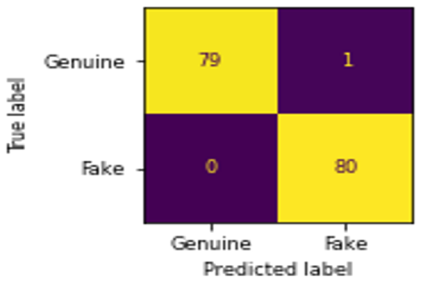
(c) Decision Tree



(d) Logistic Regression



(e) KNN



(f) Random Forest

Figure 6: Confusion Matrix of ML algorithms

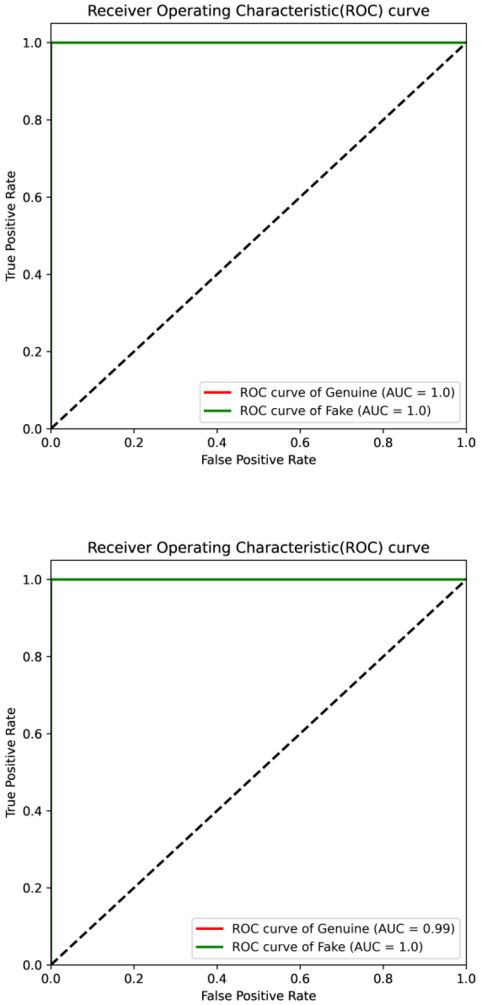


Figure 7. AUROC of ML algorithms: (a) RF, LR, (b) SVM, NB, KNN, DT,

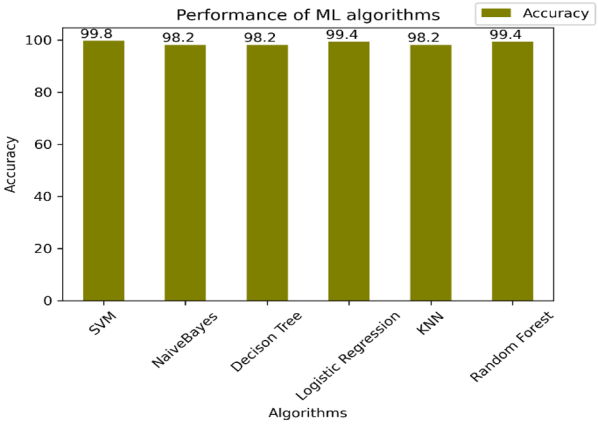


Figure.8. Accuracy of ML algorithms

5. Conclusion

Histogram features were extracted from the preprocessed image datasets to identify fraudulent degree certificates. ML algorithms were employed to classify certificates as 'genuine' or 'fake'. Among them, SVM obtained an accuracy of 98.8%, while NaïveBayes, KNN, and Decision Tree each yielded an accuracy of 98.2%. Random Forest, and Logistic Regression outperformed the others with an accuracy of 99.4%. Although these algorithms demonstrated high classification accuracy, it has limitations in predicting newly generated fraudulent degree certificates, as they rely on a supervised approach trained on labelled data. To address this task, future work will explore semi-supervised approach using deep learning techniques.

Acknowledgements. The authors thank Bangalore University for providing the scanned datasets of the mark cards used in this research. The author, Sarala M, also acknowledges the Department of Science and Technology (DST), Karnataka Science and Technology Promotion Society (KSTePS), Government of Karnataka, India, for fellowship support during the research.

References

[1] Abdallah, A., Maarof, M.A. and Zainal, A., 2016. Fraud detection system: A survey. Journal of Network and Computer Applications, 68, pp.90-113.

[2] Josephine Isabella, S., Srinivasan, S. and Suseendran, G., 2021. An efficient study of a fraud detection system using ML techniques. In Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2019 (pp. 59-67). Singapore: Springer Singapore.

[3] Mallikarjuna kethepalli, Pushan Kumar Dutta, and N Sateesh Kedarnath Kumar, 2019, Detecting forged scan of educational certificates using a new feature set matching algorithm. Vol.32(1), pp.75-88.

[4] Muhamad, S. and Ahmed, T., 2021. Counterfeit currency recognition using deep learning: A review.Technium, Vol.3, Issue 7, pp.14-26.

[5] Kamble, K., Bhansali, A., Satalgaonkar, P. and Alagundgi, S., 2019, December. Counterfeit currency detection using deep convolutional neural network. In 2019 IEEE Pune Section International Conference (PuneCon) (pp. 1-4). IEEE.

[6] Kumar, S.N., Singal, G., Sirikonda, S. and Nethravathi, R., 2020, December. A novel approach for detection of counterfeit Indian currency notes using deep convolutional neural network. In IOP conference series: materials science and engineering (Vol. 981, No. 2, p. 022018). IOP Publishing.

[7] Jain Hritik, and S.K. Pal, 2018, Fake currency note identification using deep convolutional neural networks. IJCA, Vol.13, Issue 2, pp.233-239.

[8] Laavanya, M. and Vijayaraghavan, V., 2019. Real-time fake currency note detection using deep learning. Int. J. Eng. Adv. Technol.(IJEAT), 9.

[9] Pachon, C.G., Ballesteros, D.M. and Renza, D., 2021. Fake banknote recognition using deep learning. Applied Sciences, 11(3), p.1281.

[10] Malik, F. and Baharudin, B., 2013. The statistical quantized histogram texture features analysis for image retrieval based on median and laplacian filters in the dct domain. The International Arab Journal of Information Technology, 10(6), pp.1-9.

[11] Appiah, O. and Hayfron-Acquah, J.B., 2018. Fast generation of image's histogram using approximation technique for image processing algorithms. International Journal of Image, Graphics and Signal Processing (IJIGSP), 10(3), pp.25-35.

[12] Singh, T., Singh, M., Sugandh, U. and Panwar, A., 2024, November. Feature Extraction in Image Processing using Medical Scans: Detailed Survey. In 2024 International Conference on IoT, Communication and Automation Technology (ICICAT) (pp. 1587-1592). IEEE.

[13] Li, X.P., Liu, G.H. and Lu, F., 2025. Image Retrieval Using Multi-layer Orientation Histograms. Neural Processing Letters, 57(2), pp.1-21.

[14] Wei, W., Xu, X., Hu, G., Shao, Y. and Wang, Q., 2024. Deep Learning and Histogram-Based Grain Size Analysis of Images. Sensors, 24(15), p.4923.

[15] Nassar, M., Salama, R.A., Saleeb, A.A., El-bahnasawy, N.A., Ahmed, H.E.H. and Abd El-Samie, F.E., 2024. Cumulative histogram as a feature selection technique for anomaly detection. Multimedia Tools and Applications, pp.1-13.

[16] Dong, X., Xiao, N., Ma, Y., Wang, C., Yu, D. and Wang, D., 2025. Research on Algorithm for Feature Extraction of Laryngoscope Image Distribution and Texture Fusion. Journal of Voice.

[17] Gharahbagh, A.A., Hajihashemi, V., Machado, J.J. and Tavares, J.M.R., 2024. Feature Extraction Based on Local Histogram with Unequal Bins and a Recurrent Neural Network for the Diagnosis of Kidney Diseases from CT Images. Bioengineering, 11(3), p.220.

[18] Godbin, A. Beena, S. Graceline Jasmine., 2022. Screening of COVID-19 based on GLCM features from CT images using machine learning classifiers, SN Computer Science 4, no. 2, 133

[19] Jhansi, B., M. Ramesh, A. Deepak, P. R. Karthikeyan, 2022, Evaluating Textural Changes of Lung in CT Images using GLCM in Comparison with GLRLM. In: 2nd International Conference on Technological Advancements in Computational Sciences (ICTACS), pp. 857-862. IEEE.

[20] Fahad B Mostafa, Easin Hasan., 2021, Machine Learning Approaches for Binary Classification to Discover Liver Diseases using Clinical Data, DOI:10.1101/2021.04.26.21256121.

[21] Mendez, Kevin M., Stacey N. Reinke, David I. Broadhurst, 2019. A comparative evaluation of the generalised predictive ability of eight machine learning algorithms across ten clinical metabolomics data sets for binary classification. Metabolomics 15:1-15.

[22] Çetin, Necati., 2022, Machine learning for varietal binary classification of soybean (Glycine max (L.) Merrill) seeds based on shape and size attributes. Food Analytical Methods 15, no. 8: 2260-2273.

[23] de Beurs, Zoe L., N. Islam, G. Gopalan, S. D. Vrtilek., 2022, A Comparative Study of Machine-learning Methods for X-Ray Binary Classification, The Astrophysical Journal 933, no. 1: 116 .

[24] Hudnurkar, Shilpa, Neela Rayavarapu. 2022, Binary classification of rainfall time-series using machine learning algorithms, International Journal of Electrical & Computer Engineering (2088-8708) 12, no. 2

[25] Nawir, Mukrimah, Amiza Amir, Ong Bi Lynn, Naimah Yaakob, R.Badlishah Ahmad, 2018, Performances of machine learning algorithms for binary classification of network anomaly detection system, In: Journal of Physics: Conference Series, vol. 1018, pp. 012015. IOP Publishing.

[26] Kirichenko, Lyudmyla, Tamara Radivilova, Vitalii Bulakh, 2020, Binary classification of fractal time series by machine learning methods, In: Lecture Notes in Computational Intelligence and Decision Making: Proceedings of the XV International Scientific Conference on Intellectual Systems of Decision Making and Problems of Computational Intelligence(ISDMCI'2019), Ukraine, May 21–25,15, pp. 701-711. Springer International Publishing.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

