EasyChair Preprint

№ 11523

Evaluation of Machine Learning Algorithm for Copy Move Forgery Detection

Vijay Bharti Punia and Rohini Goel

December 14, 2023

Evaluation of Machine Learning Algorithm for Copy Move Forgery Detection

Vijay Bharti[1]
Research Scholar
bhartivijay2@gmail.com

Dr. Rohini Goel[2]
Associate Professor
rohini@mmumullana.org

[1,2]Department of Computer Science and Engineering, MM Engineering College, Maharishi Markandeshwar (Deemed to be University), Mullana-Ambala, Haryana, India 133207

1.1 Abstract

Recently the need for verifying the authenticity of digital images continues to grow, extensive research efforts are dedicated to exploring techniques for detecting image forgeries. Among the prevalent forms of digital tampering, copy-move forgery (CMF) stands out as a widely studied challenge. This manipulation involves duplicating a portion of an image and subsequently pasting it either within the same image or onto a different one. The consequence of such forgery is the obfuscation of the original image content. This study, presents a comprehensive evaluation of four machine learning algorithms, namely k-Nearest Neighbours (kNN), Regression (LR), Naïve Bayes (NB), and Convolutional Neural Network (CNN), for the task of detecting copy-move forgery in images. Our research leverages the CoMoFoD dataset, a widely recognized benchmark for image forensics, to conduct a rigorous assessment of these algorithms.Through analysis, we reveal the strengths and weaknesses of each algorithm in addressing the challenges posed by copy-move forgery detection (CMFD).

Keywords: Copy-Move Forgery Detection, Machine Learning Algorithms, kNN, LR, NB, CNN.

1.2 Introduction

Digital forensics is a branch of forensic science that involves the recovery, preservation, and analysis of digital data for the purpose of investigating and presenting evidence in legal cases. It encompasses a wide range of activities aimed at examining digital devices and data to uncover and document information related to computer crimes, fraud, and other digital incidents[1][2]. Digital forensics is crucial in the modern world due to the prevalence of digital technology and the increasing reliance on digital devices and data in both personal and professional contexts.Image-based forgery detection is a specific area within digital forensics that focuses on identifying and proving the authenticity of digital images[3]. Image forgery refers to the manipulation or alteration of images to create fake or misleading visual content. In criminal and civil cases, it is essential to determine the authenticity of digital images presented as evidence. Detecting image forgeries helps ensure the integrity of the legal process. In a world where images play a significant role in news, social media, and digital communication, the ability to verify the authenticity of images is critical for national security and the prevention of misinformation and deception. Businesses and individuals rely

on images to protect their intellectual property[4][5]. Detecting image-based forgeries helps safeguard copyrights and trademarks. Image forgeries can erode trust in media and information sources. Detection tools and methods are necessary to maintain trust and credibility in digital content.

To meet the need for image-based forgery detection, digital forensics experts and researchers develop techniques and tools to analyse images and detect any signs of manipulation or tampering. Document recognition, particularly through Optical Character Recognition (OCR), transforms printed or handwritten text into machine-readable data, facilitating document digitization[29].

These methods often involve examining metadata, image compression artifacts, inconsistencies in lighting and shadows, and other digital footprints left behind during the forgery process. Advancements in machine learning and computer vision have also contributed to more accurate and efficient forgery detection techniques.This evaluation study conducted in this research paper addresses a critical need in the field of image forensics and digital image authenticity verification. As the proliferation of digital media continues to grow, the incidence of image manipulation and forgery has also increased significantly. Detecting copy-move forgery, a common and often deceptive technique, is paramount for ensuring the integrity and authenticity of digital images. This evaluation study aims to assess and compare the performance of various machine learning algorithms, namely kNN, LR, Naïve Bayes, and CNN, in detecting copy-move forgery[6]. By conducting this comprehensive evaluation, we aim to provide valuable insights into the strengths and weaknesses of each algorithm, enabling practitioners and researchers to make informed decisions when choosing an appropriate method for image forgery detection.Feature-based methods are centered on isolating distinctive characteristics, such as edges or textures, and subsequently matching them against predefined features within a database[30].Recent successes in deep learning, particularly with Convolutional Neural Networks (CNNs),

provide optimism for overcoming the challenge by automatically learning complex patterns and semantic information from images[31].

1.3 Related work

In a previous study, an algorithm for copy-move forgery (CMF) detection was proposed, utilizing the Discrete Wavelet Transform[7]. Another efficient CMF detection method relied on DCT and SVD[8], making it particularly effective for scenarios involving multiple CMFs. This approach combined the Invariant Feature Transform (SIFT)[9] and Singular Value Decomposition (SVD)[10], resulting in a robust method for automatically identifying duplicated regions within the same image, demonstrating resilience to geometric transformations.

An alternative approach for CMF detection involved 2-Level DWT to separate bands and blocks[11], complemented by SURF for feature extraction. Another novel technique utilized key points and feature descriptors[12], resulting in a stable and accurate CMF detection algorithm. Furthermore, a technique merging DCT

and SVD yielded an efficient CMF detection algorithm capable of achieving high accuracy, even in the presence of various image deformations. Another unique CMF detection technique involved SIFT and reduced LBP[13], exhibiting superior performance compared to existing methods.

Deep learning, a widely explored topic across various fields, including CMFD[14], primarily relies CNNs. In CMFD, CNNs play a pivotal role, undergoing multiple stages where they generate sets of features. Some of these features serve as training data. Deep learning-based methods consistently outperform traditional and moment-based approaches in this context. Several recent CMFD approaches have embraced deep learning principles.

In a recent study, an efficient CMFD approach based on CNN achieved remarkable accuracy when tested on different datasets. Another CMFD system centred around a novel technique called dual branch CNN[15] delivered strong results in terms of both time efficiency and performance. Furthermore, two deep learning-based CMFD approaches were proposed[16][17], including a custom architecture model and a transfer learning model, which underwent rigorous testing across multiple benchmark datasets. Additionally, an efficient system for detecting and localizing image forgeries using deep CNN and semantic segmentation achieved accuracy rates exceeding 98%.[18] Another CMFD model featured multi-scale input and two distinct blocks of convolutional layers: encoder and decoder blocks[19].

1.4 k-Nearest Neighbours (kNN)

kNN is a supervised machine learning algorithm used for classification tasks, such as image forensics in CMFD[20]. It's a simple yet effective algorithm that operates based on the principle of similarity.When well-tuned and with appropriate features, kNN can be highly effective in identifying copy-move forgeries. The first step in using kNN for CMFD involves extracting relevant features from the image. These features are numerical representations of specific characteristics within the image, such as colour, texture, or shape. In the context of forgery detection, the chosen features should be discriminative enough to distinguish between genuine and forged regions.Each region of the image is represented as a feature vector in a multidimensional space, where each dimension corresponds to a specific feature. The goal is to find regions in the image that are similar to each other in this feature space.

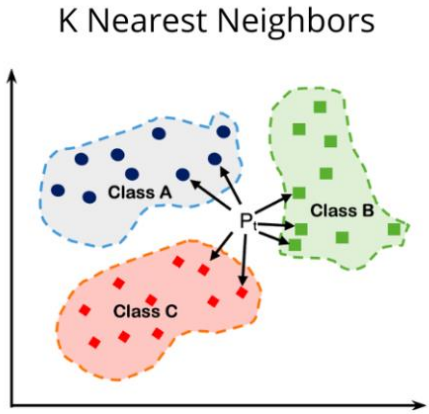

Figure 1: illustration of kNN classifier for image forgery detection [21]

The kNN algorithm is trained on a labelled dataset that includes examples of both genuine (non-forged) regions and copy-move forged regions. Each example is associated with its feature vector and a label indicating whether it's genuine or

forged.When a new, unseen region of an image needs to be classified, the kNN algorithm calculates the distance**'p'** between the feature vector of the new region and the feature vectors of its kNN in the training dataset as shown in the figure above. The parameter **"k"** represents the number of nearest neighbours to consider. Typically, **k** is chosen based on cross-validation or other techniques.Once the distances to the kNN are calculated, the algorithm performs a majority vote among these neighbours to determine the class label of the new region. In the context of CMFD, if the majority of the kNN are labelled as forged, the new region is also classified as a copy-move forgery.

1.4.1 Logistic Regression (LR)

LR is a supervised learning algorithm primarily used for binary classification tasks, making it suitable for tasks like image forensics in CMFD[22]. It models the probability of a given input belonging to one of two classes using the logistic function.The process starts with the extraction of relevant features from the image regions or segments. These features can include characteristics like colour histograms, texture patterns, or other discriminative properties that help distinguish between genuine and forged regions.

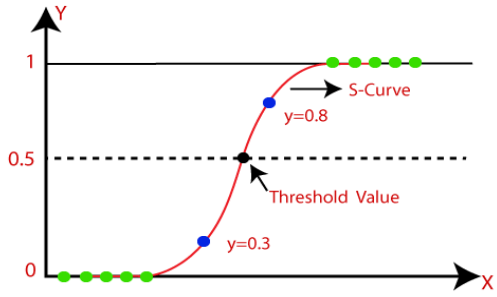

Figure 2: Working of logistic regression with thresholds [23]

Each image region is represented by a feature vector. This vector contains values corresponding to the extracted features. The goal is to use these feature vectors to predict the probability of a region being genuine or a copy-move forgery.LR requires a labelled dataset for training. This dataset should consist of feature vectors from various image regions, along with their corresponding labels (0 for genuine, 1 for forged).The LR model is trained on the labelled dataset to learn the relationship between the features and the probability of a region being a copy-move forgery. The model estimates the coefficients (weights) associated with each feature and the intercept (bias term) through an optimization process, typically using methods like gradient descent.Once the model is trained, it can estimate the probability of a new, unseen image region being a copy-move forgery. The logistic function (sigmoid function) transforms the output into a probability value between 0 and 1. A threshold value (e.g., 0.5) is chosen to classify the probability estimates. If the estimated probability is above the threshold, the region is classified as a copy-move forgery; otherwise, it is classified as genuine.

1.4.2 Naïve Bayes (NB)

NB is a supervised machine learning algorithm commonly used for classification tasks, including text classification and image analysis. It is based on Bayes' theorem and makes the "naïve" assumption that features are conditionally independent, which simplifies the probability calculations.The process begins with the extraction of relevant features from image regions or segments. These features could include colour histograms, texture descriptors, or

other characteristics that help distinguish between genuine and forged regions.Each image region is represented as a feature vector, where each feature corresponds to a specific attribute or property extracted from the region.NB requires a labelled dataset for training. This dataset should contain feature vectors from various image regions, along with their corresponding labels (0 for genuine, 1 for forged).

The NB model is trained on the labelled dataset to learn the conditional probabilities of each feature given a class label (genuine or forged). It estimates the prior probabilities of each class based on the training data.When presented with a new, unseen image region, the NB model calculates the posterior probabilities of the region belonging to each class (genuine or forged) using Bayes' theorem.The model assigns a class label to the region based on the class with the highest posterior probability. In other words, it classifies the region as either genuine or a copy-move forgery.

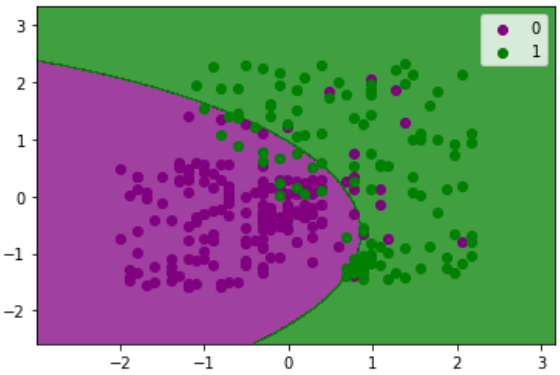

Figure 3: Naïve bayes classifier for CMFD [24]

1.5 Convolutional Neural Network (CNN)

A CNN is a type of deep learning model designed specifically for processing and analysing visual data, such as images and videos[25]. CNNs are composed of multiple layers, including convolutional layers that can automatically learn and extract relevant features from input images[26].The first step is to prepare a labelled dataset containing genuine (non-forged) images and images with copy-move forgeries. Each image is labelled according to whether it contains forgeries or not.The input to the CNN is an image region or patch that needs to be classified as either genuine or a copy-move forgery. These patches can be extracted from the original image. CNNs consist of multiple convolutional layers that automatically learn and extract hierarchical features from the input image. These layers apply a set of learnable filters (kernels) to the image, scanning for patterns and features.After each convolutional layer, pooling layers are often used to reduce the spatial dimensions of the feature maps and retain essential information. Max-pooling is a common pooling technique used in CNNs.

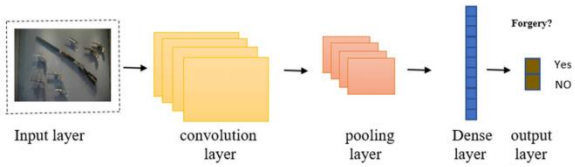

Figure 4: CNN Model to Detect Copy-Move Image Forgery[27]

The output from the final convolutional and pooling layers is flattened into a one-dimensional feature vector.The flattened feature vector is then fed into one or more fully connected layers. These layers perform complex transformations and eventually produce an output.The output layer typically consists of a single neuron with a sigmoid activation function. This neuron produces an output value between 0 and 1, representing the probability of the

input region being a copy-move forgery. A value closer to 0 indicates a genuine region, while a value closer to 1 indicates a forgery.

1.6 Experimental Results

For our experiments, we employed the CoMoFoD dataset [28] to conduct CMFD. This dataset comprises a total of 260 sets of forged images. The images within this dataset were partitioned into blocks of dimensions 8 × 8 pixels. All of our experimental work was carried out on a desktop computer equipped with an Intel i5 12400F CPU, 8GB of RAM, running Windows 11 with a 64-bit operating system, and utilizing MATLAB R2019a.In the proposed work precision, recall, accuracy, and F1-score are key performance metrics used to evaluate the effectiveness of a CMFD algorithms.

Table 1: Evaluation Results of CMFD algorithms on the CoMoFoD dataset

Metric	Knn	LR	NB	CNN
Precision	95.11	76.21	82.54	95.46
Recall	88.46	69.72	77.41	90.62
Accuracy	81.81	63.23	72.27	85.79
F1-Score	97.11	75.21	82.54	93.46

1.6.1 Precision

Precision, also known as positive predictive value, measures the accuracy of the positive predictions made by the CMFD algorithm. In CMFD, it quantifies the proportion of correctly detected copy-move forgeries (true positives) out of all images classified as forgeries by the algorithm (true positives + false positives).

$$Precision = \frac{Tp}{(TP + FP)}$$

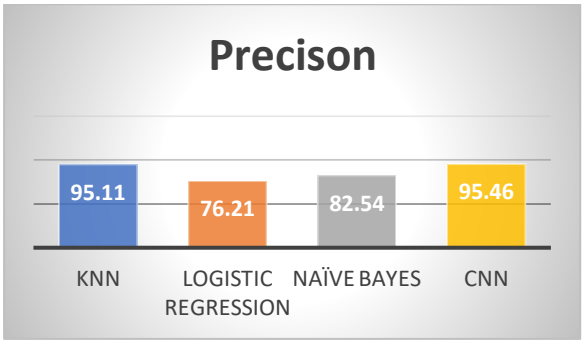

Figure 5: Precision score for CMFD of kNN, LR, NB and CNN algorithms

The results in Figure 5show that kNN and CNN exhibit particularly high precision scores, while LR and NB also demonstrate respectable performance in this regard. These findings can be crucial for selecting the most suitable algorithm for CMFD based on the precision criterion in your research.

In other words, the kNN algorithm tends to make fewer false positive predictions, which is crucial in image forensics to avoid incorrectly flagging non-forged. he results show that kNN and CNN exhibit particularly high precision scores, while LR and NB also demonstrate respectable performance in this regard.

1.6.2 Recall

Recall, also known as true positive rate or sensitivity, measures the ability of the CMFD algorithm to correctly identify all actual copy-move forgeries in the dataset. It quantifies the proportion of true positives out of all the actual copy-move forgeries (true positives + false negatives).

$$Recall = \frac{Tp}{(TP + FN)}$$

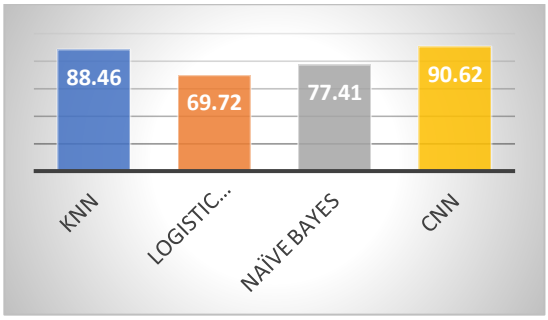

Figure 6:Recall score for CMFD of kNN, LR, NB and CNN algorithms

Recall measures the ability of each algorithm to correctly identify copy-move forgeries, emphasizing their sensitivity to detecting true positives. The results show that CNN and kNN exhibit particularly high recall scores, indicating their effectiveness in detecting genuine forgeries. While LR and NB have lower recall scores, they still perform reasonably well in capturing a substantial portion of the forgeries.

1.6.3 Accuracy

Accuracy measures the overall correctness of the CMFD algorithm's predictions, including both genuine and forged regions. It quantifies the proportion of correctly classified images (true positives + true negatives) out of the total number of images.

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

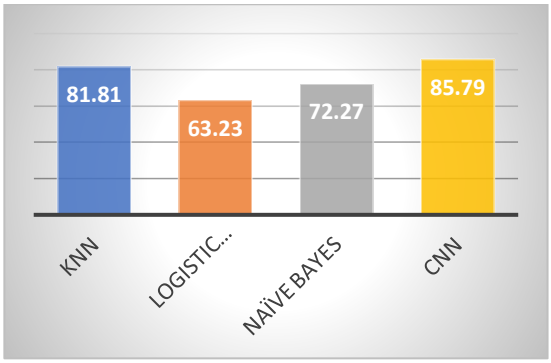

Figure 7:Accuracy for CMFD of kNN, LR, NB and CNN algorithms

The CNN model achieved a high accuracy score of 85.79%, indicating its ability to correctly classify approximately 85.79% of all image regions in the dataset. CNNs excel in capturing intricate patterns and features in images, contributing to their high overall accuracy in copy-move forgery detection.The Figure 7 result show that CNN and kNN exhibit particularly high accuracy scores, indicating their effectiveness in correctly classifying image regions as either authentic or copy-move forgeries. While Logistic Regression and Naïve Bayes have lower accuracy scores, they still provide meaningful results in this context.

1.6.4 F1-score

The F1-score is the harmonic mean of precision and recall and provides a balanced measure of a CMFD algorithm's performance. It takes into account both false positives and false negatives, making it particularly useful when the dataset is imbalanced.

$$F1 - Score = 2 * \frac{Precision * Recall}{(Precision + Recall)}$$

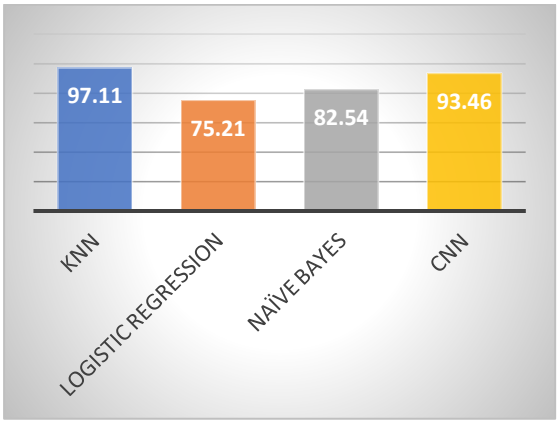

Figure 8: F1-Score for CMFD of kNN, LR, NB and CNN algorithms

F1-Score is a valuable metric that considers both precision and recall, providing a comprehensive assessment of

an algorithm's performance. The results show that kNN, CNN, and NB achieve high F1-Scores, indicating their effectiveness in copy-move forgery detection. While Logistic Regression has a lower F1-Score, it still offers a reasonable balance between precision and recall.

The results demonstrates that kNN provides high precision and F1-Score, indicating a low rate of false positives and a good balance between precision and recall. It also achieves a high recall rate, capturing a substantial portion of copy-move forgeries, and high accuracy in overall classification. LR shows a reasonable balance between precision and recall, making it a suitable choice for CMFD. While it has lower accuracy than some other algorithms, it provides meaningful results. NB offers a good balance between precision and recall, making it effective in identifying copy-move forgeries. It achieves a respectable level of accuracy and F1-Score. CNN excels in precision, recall, accuracy, and F1-Score, indicating its strong performance in CMFD. Its ability to capture intricate patterns in images leads to high accuracy and precision.

1.7 Conclusion and Future Work

In this research, we conducted a comprehensive evaluation of four machine learning algorithms kNN, LR, NB, and CNN - for the task of CMFD on the CoMoFoD dataset. We assessed their performance using essential evaluation metrics such as Precision, Recall, Accuracy, and F1-Score. Our findings reveal that kNN and CNN emerge as strong contenders in CMFD. kNN demonstrates exceptional precision, recall, and F1-Score, indicating its ability to accurately identify forgeries while minimizing false positives. CNN, known for its capacity to capture intricate image patterns, exhibits outstanding performance in both precision and recall, resulting in a high F1-Score. LR and NB, although having lower overall performance scores, still provide reasonable results and can be suitable choices for certain applications. In Future, more advanced deep learning architectures and CNNs, such as deep CNN variants (e.g., ResNet, Inception) and recurrent neural networks (RNNs) can be explored, to further improve accuracy and efficiency in forgery detection.

1.8 References

[1]. Kävrestad, J. (2020). Fundamentals of Digital Forensics. Springer International Publishing.

[2]. Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. Journal of Information Processing Systems, 14(2).

[3]. Teerakanok, S., & Uehara, T. (2019). Copy-move forgery detection: A state-of-the-art technical review and analysis. IEEE Access, 7, 40550-40568.

[4]. Zhong, J. L., & Pun, C. M. (2019). An end-to-end dense-inceptionnet for image copy-move forgery detection. IEEE Transactions on Information Forensics and Security, 15, 2134-2146.

[5]. Teerakanok, S., & Uehara, T. (2019). Copy-move forgery detection: A state-of-the-art technical review and analysis. IEEE Access, 7, 40550-40568.

[6]. Ashraf, R., Mehmood, M. S., Mahmood, T., Rashid, J., Nisar, M.

W., & Shah, M. (2020, October). An efficient forensic approach for copy-move forgery detection via discrete wavelet transform. In 2020 International Conference on Cyber Warfare and Security (ICCWS) (pp. 1-6). IEEE.

[7]. Priyanka, Singh, G., & Singh, K. (2020). An improved block based copy-move forgery detection technique. Multimedia Tools and Applications, 79, 13011-13035.

[8]. Alberry, H. A., Hegazy, A. A., & Salama, G. I. (2018). A fast SIFT based method for copy move forgery detection. Future Computing and Informatics Journal, 3(2), 159-165.

[9]. Rathore, N. K., Jain, N. K., Shukla, P. K., Rawat, U., & Dubey, R. (2021). Image forgery detection using singular value decomposition with some attacks. National Academy Science Letters, 44, 331-338.

[10]. Singh, R., Verma, S., Yadav, S. A., & Singh, S. V. (2022, April). Copy-move Forgery Detection using SIFT and DWT detection Techniques. In 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM) (pp. 338-343). IEEE.

[11]. Wang, X. Y., Jiao, L. X., Wang, X. B., Yang, H. Y., & Niu, P. P. (2018). A new keypoint-based copy-move forgery detection for colour image. Applied Intelligence, 48(10), 3630-3652.

[12]. Shahrokhi, M., Akoushideh, A., &Shahbahrami, A. (2022). Image Copy–Move Forgery Detection Using Combination of Scale-Invariant Feature Transform and Local Binary Pattern Features. International Journal of Image and Graphics, 22(05), 2250048.

[13]. Agarwal, R., & Verma, O. P. (2020). An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimedia Tools and Applications, 79(11-12), 7355-7376.

[14]. Goel, N., Kaur, S., & Bala, R. (2021). Dual branch convolutional neural network for copy move forgery detection. IET Image Processing, 15(3), 656-665.

[15]. Wu, Y., Abd-Almageed, W., & Natarajan, P. (2018, March). Image copy-move forgery detection via an end-to-end deep neural network. In 2018 IEEE Winter Conference on Applications of Computer Vision (WACV) (pp. 1907-1915). IEEE.

[16]. Barad, Z. J., & Goswami, M. M. (2020, March). Image forgery detection using deep learning: a survey. In 2020 6th international conference on advanced computing and communication systems (ICACCS) (pp. 571-576). IEEE.

[17]. Rhee, K. H. (2021). Generation of novelty ground truth image using image classification and semantic segmentation for copy-move forgery detection. IEEE Access, 10, 2783-2796.

[18]. El Biach, F. Z., Iala, I., Laanaya, H., &Minaoui, K. (2021). Encoder-decoder based convolutional neural networks for image forgery detection. Multimedia Tools and Applications, 1-18.

[19]. Paul, K. H., Akshatha, K. R., Karunakar, A. K., & Seshadri, S.

(2020). SURF based copy move forgery detection using kNN mapping. In Advances in Computer Vision: Proceedings of the 2019 Computer Vision Conference (CVC), Volume 2 1 (pp. 234-245). Springer International Publishing.

[20]. Siddique, A. (2023) Exploring KNN with different distance metrics, Medium. Available at: https://blog.devgenius.io/exploring-knn-with-different-distance-metrics-85aea1e8299

[21]. Babu, S. T., & Rao, C. S. (2020, July). Statistical features based optimized technique for copy move forgery detection. In 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.

[22]. Jaiswal, S. (2021) Logistic regression in machine learning - javatpoint, www.javatpoint.com. Available at: https://www.javatpoint.com/logistic-regression-in-machine-learning

[23]. Kumari, R., Garg, H., & Chawla, S. (2023). Two-Stage Model for Copy-Move Forgery Detection. In Computational Intelligence for Engineering and Management Applications: Select Proceedings of CIEMA 2022 (pp. 831-844). Singapore: Springer Nature Singapore.

[24]. Jaiswal, S. (2022) Naive Bayes classifier in machine learning - javatpoint, www.javatpoint.com. Available at: https://www.javatpoint.com/machine-learning-naive-bayes-classifier

[25]. Chauhan, R., Ghanshala, K. K., & Joshi, R. C. (2018, December). Convolutional neural network (CNN) for image detection and recognition. In 2018 first international conference on secure cyber computing and communication (ICSCCC) (pp. 278-282). IEEE.

[26]. Abdalla, Y., Iqbal, M. T., & Shehata, M. (2019). Convolutional neural network for copy-move forgery detection. Symmetry, 11(10), 1280.

[27]. Hosny, K. M., Mortda, A. M., Fouda, M. M., &Lashin, N. A. (2022). An efficient CNN model to detect copy-move image forgery. IEEE Access, 10, 48622-48632.

[28]. Tralic, D., Zupancic, I., Grgic, S., & Grgic, M. (2013, September). CoMoFoD—New database for copy-move forgery detection. In Proceedings ELMAR-2013 (pp. 49-54). IEEE.

[29]. Goel, Rohini, Avinash Sharma, and Rajiv Kapoor. "Object recognition using deep learning." Journal of Computational and Theoretical nanoscience 16.9 (2019): 4044-4052.

[30]. Goel, Rohini, Avinash Sharma, and Rajiv Kapoor. "State-of-the-art object recognition techniques: a comparative study." Soft Computing: Theories and Applications: Proceedings of SoCTA 2018. Singapore: Springer Singapore, 2020. 925-932.

[31]. Kapoor, Rajiv, Deepak Sharma, and Tarun Gulati. "State of the art content based image retrieval techniques using deep learning: a survey." Multimedia Tools and Applications 80.19 (2021): 29561-29583.