

Image Forgery Detection through Fusion of Xception CNN and Thepade SBTC Features using ML Classifiers and Ensembles

Dr. Amruta Mahajan¹, Siddhant Kotkar², Murtuza Kapasi³, Monika Khivasara⁴, Radhey Kedar⁵ and Chhaya Nayak⁶

¹⁻⁶Pimpri Chinchwad College of Engineering, Pune, India

Email: {amrutamahajan.work, sidkot27, murtuzakapasi.official, monika.jain.0903, radheykedar28, chhaya2007}@gmail.com

Abstract— In today's dynamic digital landscape, verifying the authenticity of visual content is paramount. This research tackles the crucial task of image forgery detection that is distinguishing genuine images from manipulated ones. We propose a novel approach by harnessing the capabilities of Xception CNN for intricate pattern recognition and Thepade SBTC features for interpretability and resilience.

This study employs eight ML algorithms and top performing ensembles to assess effectiveness of our fusion methodology. Results indicate that ensembles surpass individual algorithms, achieving superior image forgery detection. Specifically, fusing Thepade SBTC and Xception CNN features demonstrates remarkable performance, outperforming individual feature sets. These findings not only propel image forensics but also provide a practical solution for safeguarding digital visual integrity in today's technology-driven milieu.

Index Terms—Image Forgery Detection, Xception CNN, Thepade SBTC, Machine Learning Algorithm, Ensembles.

I. INTRODUCTION

In today's digital age, image authenticity is a critical concern due to widespread manipulation. Detecting forged images is crucial for maintaining trust in digital communication. This report introduces an innovative approach that combines features from the pioneering Xception model with Thepade SBTC, enhancing the accuracy of image forgery detection. The Xception model excels in recognizing intricate patterns, complemented by Thepade SBTC's precision in extracting handcrafted features. This fusion creates a comprehensive framework to differentiate authentic visuals from manipulated ones. Through rigorous experimentation on the established CASIA V2 dataset, our strategy achieves an impressive 98% accuracy. As the digital landscape evolves, our approach not only safeguards visual integrity but also lays the foundation for more advanced and reliable methods in the field. In recent years, the proliferation of digital content and the ease of image editing tools have intensified the challenge of ensuring the authenticity of visual information. The growing sophistication of image manipulation techniques underscores the pressing need for robust forgery detection methods that can adapt to evolving threats in the digital space. By leveraging a hybrid approach that combines the strengths of deep learning and traditional feature extraction, our proposed method offers a promising solution to address these challenges and enhance the integrity of digital imagery.

II. TOOLS AND ALGORITHMS

A. Proposed Approach

We initiate the study by training our model on the CASIA V2 dataset. To enrich the feature set, we incorporate Error Level Analysis (ELA) images, a proven method for detecting digital manipulations. ELA images undergo feature extraction from the dense layer of the model. For extracting features using Xception, the current model, which is pre-trained, is considered. After which comes the step of unfreezing some of the convolutional blocks, which are fine-tuned later on. A feature vector having a length of 1024 is extracted by using the output of the second last dense layer. In conjunction with these techniques, we operate within the RGB color space, capitalizing on its ability to represent color information accurately.

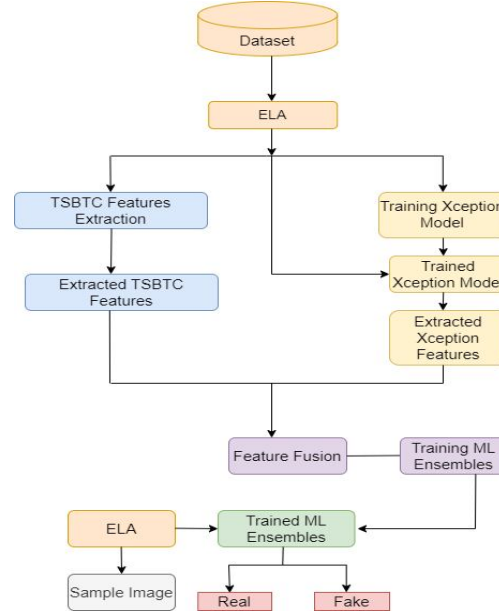


Fig. 1: The suggested method operates in two main stages: training and testing. In the training stage, the method's operations are executed, while in the testing stage, the results of the training are assessed.

Additionally, we integrate Thepade Sorted Block Truncation Coding (TSBTC) with an n-ary approach, combined with ELA images, yielding extra handcrafted features. These enhancements diversify and deepen our feature set. Subsequently, a suite of ML algorithms, including RF, SVM, Decision Tree (DT), and Logistic Regression (LR), is employed for model training. Each algorithm is rigorously trained on the fused feature set to distinguish authentic visuals from manipulated ones. Through rigorous experimentation on the CASIA V2 dataset, we evaluate the efficacy of our methodology, focusing on major performance metrics like precision, accuracy, recall, and F1 score. The integration of ELA images, dense layer features, and TSBTC, coupled with ensemble learning, represents a strategic advancement in image forgery detection. This approach not only enhances detection accuracy but also sets the stage for future innovations in the field.

B. Xception Model

The Xception model follows a distinct architecture known for its depth and efficient information flow. Xception employs a depth-wise separable convolution operation as its fundamental building block. This operation separates the spatial and channel-wise convolutions, resulting in a more efficient and parameter-efficient model. In terms of layer count, Xception comprises 126 layers, including 36 and 54 convolutional layers in entry and in middle flow respectively. The exit flow has 36 convolutional layers. This depth, combined with its unique architecture, allows Xception to capture intricate patterns and features in images, making it effective for various tasks of computer vision. The feature vector extracted from dense layer of Xception is of a fixed length, typically comprising 1024 elements.

C. Error Level Analysis

It is a pivotal technique in image forensics, adept at uncovering manipulations. It functions by compressing images at a specific quality level and subsequently comparing the resulting compression levels. This method is

particularly effective when an image undergoes editing followed by recompression. Within the RGB color model, ELA computes the average deviation in quantization tables for the Red, Green, and Blue channels. Notably, original images captured by digital cameras often exhibit high ELA values, manifested as white regions in the ELA image. As the image undergoes successive saves, ELA values tend to decrease. This technique is instrumental in revealing alterations, thus standing as a cornerstone in the field of image forensics.

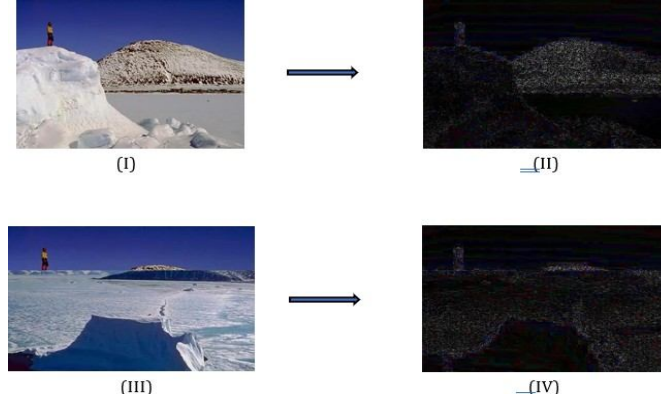


Fig. 2: System Architecture of Proposed Methodology: (I) Original Image (II) Original ELA Image (III) Tampered Image (IV) Tampered ELA Image

D. Thepade Sorted Block Truncation Coding (TSBTC)

In the context at hand, let us consider an input image denoted as $NM(x, y)$, characterized by its dimensions of $m \times n$, and making use of the Red, Green, and Blue colour channels. The corresponding feature vectors, originating from the 3-ary TSBTC method, can be precisely expressed as $[XR1, XG1, XB1]$. For the TSBTC-2 ary, which is one of the variations experimented with, the colour planes R, G, and B are transformed into unidimensional arrays and are sorted as 'sortR', 'sortG', and 'sortB'. The TSBTC-2ary feature vector is computed using the sorted unidimensional colour planes with the following equations:

$$X_{R1} = 2 \times r \times c \times \sum_{p=1}^{\frac{r \times c}{2}} \text{sortR}(p) \quad (1)$$

$$X_{G1} = 2 \times r \times c \times \sum_{p=1}^{\frac{r \times c}{2}} \text{sortG}(p) \quad (2)$$

$$X_{B1} = 2 \times r \times c \times \sum_{p=1}^{\frac{r \times c}{2}} \text{sortB}(p) \quad (3)$$

The respective clusters formed by these distinct colour channels are aptly represented by the 'i' values, now referred to as R-new, G-new, and B-new.

E. Feature Fusion of TSBTC and Xception

The study utilized two distinct methods for extracting features. Firstly, handcrafted color features were employed, specifically the TSBTC 10-ary, which possesses a dimensionality of 30. Secondly, auto-generated features were obtained through the utilization of the convolutional neural network (CNN), specifically Xception, which produces 1024 sized feature set. To improve the image identification accuracy, both TSBTC 20-ary and Xception features underwent a finetuning process. Subsequently, they were concatenated horizontally, resulting in a unified feature vector with a dimensionality of 1057 (1024+30). This crucial step was undertaken so as to fine tune the feature vectors for the task for classification.

F. Testbed

This study uses the CASIA2 testbed from Kaggle, which is widely regarded as a reliable benchmark for evaluating image tampering detection. This testbed comprises of 7492 authentic images and 5124 tampered

images, covering different types of forgery such as splicing and copy-move alterations. One of the major strength of the testbed is variability, including pictures with different resolutions and file formats, reflecting real-world scenarios of image forgery.



Fig. 3: Sample images from Dataset CASIA2

G. Performance Metrics

To thoroughly assess the effectiveness of our proposed method, we utilized a comprehensive set of performance metrics that serve as quantitative indicators of the accuracy and efficiency of our system. These metrics cover various aspects of our system's performance:

Accuracy (ACC): ACC measures the percentage of correctly identified forged and authentic images.

Precision (PR): Evaluates system's ability to correctly classify forged images among those predicted forged.

Recall (RC): RC examines the system's capability to correctly classify all actual forged images.

F1 Score (F1): The F1 score strikes a balance between precision and recall, providing a single value that reflects the overall performance of the system.

By employing these metrics, we were able to comprehensively evaluate our system's accuracy, precision, recall, and overall effectiveness in detecting image tampering.

III. AUTHORS & AFFILIATION

Numerous studies have been conducted in the field of image forgery detection, focusing on the development of robust techniques to identify manipulated images. Researchers have explored a variety of approaches, ranging from traditional methods to advanced deep learning algorithms, to address the challenges posed by increasingly sophisticated forgery techniques.

M. Pandiyan [1] in 2023 proposed a way to differentiate between tampered and authentic images using a CNN based classifier, leveraging Xception Model which is pre-trained and is used for feature extraction. The model undergoes three key modules: Preprocessing, Feature Extraction, and Classification. Preprocessing involves resizing images to 256x256 and applying ELA to identify potential areas of digital modification. The Feature extractor utilizes the model to extract the required features from the preprocessed images. Finally, the Classification module employs a Global Average pooling layer followed by two Dense layers with activation function named softmax to classify images. Experimental results on the CASIA ITDE v2 testbed demonstrate promising performance, achieving correctness of 88% on the validation dataset and 95% on the testing dataset. While the proposed model shows strong potential, further refinement and evaluation on a larger dataset could lead to even better results.

A sophisticated approach was provided by Khachane et al. [2] 2023 provides tampering detection. By harnessing the analytical prowess of ELA and the computational strength of a concatenated ResNet-XceptionNet architecture, the research achieves a noteworthy stride in authentication technology. ELA forms the cornerstone of this methodology. Complementing this, the concatenated model amalgamates the distinct capabilities of ResNet and XceptionNet, resulting in a synergistic enhancement of tampering detection capabilities. The performance of this approach has accuracy rate of 98.58%.

A method is proposed by Sudiarmika [4] et al 2018 which integrates ELA and CNN techniques for image forgery detection. By utilizing the CASIA dataset, the research involves preprocessing steps such as resizing to 224x224 pixels and dataset division. ELA is employed to reveal compression-induced discrepancies, while the VGG16 architecture in CNN aids in feature extraction. The results showcase a accuracy of 92.2% for training and accuracy of 88.46% for validation, underscoring the efficacy of the proposed methodology in distinguishing

between authentic and altered images. This amalgamation of ELA and CNN holds promise for advancing image forensics.

Aman et al [5] 2023 experimented with Random Forest (RF) and Support Vector Machine (SVM) algorithms for forgery detection, yielding a mean efficiency of 84.5% for Random Forest and 89% for SVM. The research suggests SVM's potential superiority in the encoder-decoder framework, as it achieved an efficiency of 94% compared to Random Forest's 78%. The proposed Machine learning model significantly advances Multispectral Satellite Image Segmentation, enabling accurate image descriptions.

Joshi et al [6] proposed a method for utilization of deep learning in computer vision, specifically focusing on image forensics and forgery detection. It employs ELA to detect image forgeries, transforming the task into a binary classification challenge suitable for various convolutional neural network (CNN) architectures. By implementing transfer learning with renowned image classification models like VGG-19, Inception-V3, ResNet-152-V2, XceptionNet, and EfficientNet-V2L on the CASIA v.2 dataset induced with ELA, the study aims to enhance forgery detection accuracy. The paper presents results like training and validation accuracy, precision, recall, RoC curves, AUC values, and F-Measure for each model.

The survey provided by Walia [8] presents an innovative method that merges handcrafted features based on color characteristics with deep features to improve forgery detection accuracy in digital images. The approach involves two streams: Stream I computes 648-dimensional Markov-based features from the discrete cosine transform, while Stream II extracts a 512-dimensional feature vector 'ResFeats' by processing Local Binary Patterns from the luminance channel using a pre-trained ResNet-18 model. Combining these features results in a 1160-dimensional vector for classification with a shallow neural network. Achieving a high accuracy of 99.3% on CASIA v1 and CASIA v2 datasets, the method aims to enhance forgery detection accuracy by uncovering patterns crucial for forgery detection in images.

Several studies have investigated leveraging feature fusion from various extractors to enrich data for classification algorithms, potentially boosting their efficacy. Additionally, a few have experimented with ensemble classification methods, amalgamating multiple algorithms to enhance results. This paper seeks to evaluate the effectiveness of unsupervised algorithms for classification tasks through the application of feature fusion and ensemble techniques, aiming for a thorough assessment of their performance.

IV. RESULTS AND DISCUSSIONS

This paper introduces a unique approach to detect image forgery by employing all features of TSBTC n-ary. This research found that utilizing TSBTC 10-ary features led to superior accuracy compared to features with lower arity. The study shown in Figure 4 conducted experiments involving eight distinct ML algorithms, including RF, SVM, LR, and DT. Additionally, it explored three ensemble techniques: "SVM+LR+RF", "SVM+RF+DT+LR", "RF+DT+SVM", and "LR+SVM+DT".

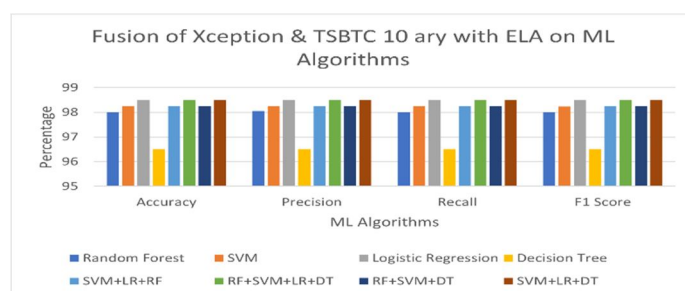


Fig. 4: Values of various metrics on TSBTC 10-ary+Xception fusion for all the classifiers and ensembles.

The study assessed the accuracy of detecting image forgery by examining different iterations of extracted features from TSBTC n-ary along with their respective combinations of ML algorithms and ensembles. When ML algorithms and classifiers were implemented on TSBTC 10-ary, TSBTC 15-ary, TSBTC 20-ary, it was seen that ensembles of the classifier demonstrated good performance specifically for TSBTC 10-ary.

The Xception model automatically generates features of 1024 dimensions, which are then employed as input for various ML classifiers and ensembles. Through a selection process, the most effective machine learning algorithms are identified for ensemble use. This strategic approach leads to a progressive improvement in ensemble accuracy, underscoring its efficacy. Among the ensembles, "RF+SVM+DT" stands out as the highest-performing combination.

TABLE I. SUMMARY OF AUTHORS, TECHNIQUES, TESTBED AND ACCURACY

Authors	Technique	Testbed	Accuracy
N.M.Pandiyan, 2023	ELA, Xception	CASIA 2	95%
Khachane et al., 2023	ELA, Concatenation	CASIA	Xception 96.87%, ResNet 96.58%, Concatenated 98.58%
Doegar et al., 2019	AlexNet, Random Forest	MICC-F220	91.81%
Sudiatmika et al., 2018	ELA, VGG16	CASIA V2	Training 92.2%, Validation 88.46%
Walia et al., 2021	ResNet 18, Handcrafting Features	CASIA V1, V2	CASIA V1: 99.3%, CASIAV2: 97.94%
Dr. N P Nethravathi et al., 2023	Pre-trained VGG-16, ELA+CNN	CASIA V1	VGG16: 75.87%, ELA+CNN: 75.58%
Proposed Approach	ELA+XceptionNet+10 ary TSBTC	CASIA V2	RF: 98%, SVM: 98.25%, LR: 98.5%, DT: 96.5%, Ensembles: 98.25%-98.5%

Only the 30 extracted features using TSBTC 10-ary are generated as inputs to the classifiers and ensembles. The accuracy is increased when ensembling technique is applied as compared to only classifiers. The best result providing ensemble comes out to be “SVM+LR+DT+RF”. The features automatically generated from Xception are combined with TSBTC 10-ary and are utilized to train machine learning ensembles and algorithms. These combinations are then analyzed for their outcomes. Among them, the “RF+SVM+LR+DT” and “SVM+LR+DT” ensembles demonstrate the most promising performance. This underscores the superiority of merging methods over the use of individual techniques.

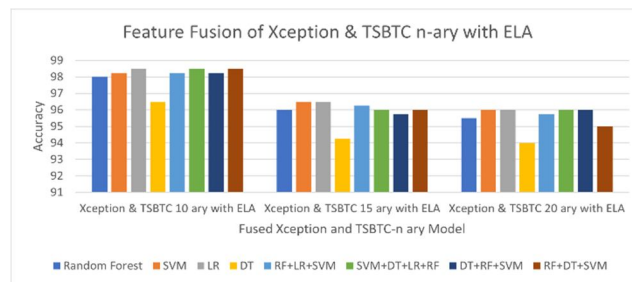


Fig. 5: The accuracy of image forgery detection utilizing different ML algorithms and ensembles can be calculated utilizing the feature extraction on TSBTC n-ary along with ELA.

Hence the study shows that fusion of TSBTC 10-ary with Xception model along with ELA performs better than other methods.

V. CONCLUSION

The paper presents a comprehensive study on image forgery detection utilizing a novel approach employing TSBTC n-ary global features. The research demonstrates that employing TSBTC 10-ary features yields notably higher accuracy of compared to features with lower arity. A range of experiments with diverse ML algorithms and ensemble techniques were conducted, showcasing promising results. Notably, the ensemble technique “SVM+LR+DT+RF” emerges as the most effective combination. Furthermore, the fusion of features extracted from TSBTC 10-ary and Xception, as well as individual feature extraction techniques, were evaluated. The results affirm that the fusion of features, particularly when combined with ELA, outperforms individual methods across various ML algorithms and ensembles. This study marks a significant advancement in image forgery detection, highlighting the efficacy of the proposed approach.

REFERENCES

- [1] Pandiyan, N. M. (2023, January). Digital Image Forgery Detection Using Pre-Trained Xception Model as Feature Extractor. In 2023 International Conference for Advancement in Technology (ICONAT) (pp. 1-5). IEEE.
- [2] Khachane, S., Mondal, D. Image Tampering Detection using Error Level Analysis and Concatenated Neural Networks..
- [3] Doegar, A., Dutta, M., Gaurav, K. (2019). Cnn based image forgery detection using pre-trained alexnet model. International Journal of Computational Intelligence IoT, 2(1).

- [4] Sudiatmika, I. B. K., Rahman, F., Trisno, T., Suyoto, S. (2019). Image forgery detection using error level analysis and deep learning. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, 17(2), 653-659.
- [5] Alhindi, T. J., Kalra, S., Ng, K. H., Afrin, A., Tizhoosh, H. R. (2018, July). Comparing LBP, HOG and deep features for classification of histopathology images. In 2018 international joint conference on neural networks (IJCNN) (pp. 1-7). IEEE.
- [6] Joshi, R., Gupta, A., Kanvinde, N., Ghonge, P. (2022, October). Forged Image Detection using SOTA Image Classification Deep Learning Methods for Image Forensics with Error Level Analysis. In 2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
- [7] Zanardelli, M., Guerrini, F., Leonardi, R., Adami, N. (2023). Image forgery detection: a survey of recent deep-learning approaches. *Multimedia Tools and Applications*, 82(12), 17521-17566.
- [8] Walia, S., Kumar, K., Kumar, M., Gao, X. Z. (2021). Fusion of handcrafted and deep features for forgery detection in digital images. *IEEE Access*, 9, 99742-99755
- [9] Yue, G., Duan, Q., Liu, R., Peng, W., Liao, Y., Liu, J. (2022). SMDAF: A novel keypoint based method for copy-move forgery detection. *IET Image Processing*, 16(13), 3589-3602.
- [10] Sasaki, Y. (2007). The truth of the F-measure. *Teach tutor mater*, 1(5), 1-5.
- [11] Bourouis, S., Alroobaea, R., Alharbi, A. M., Andejany, M., Rubaiee, S. (2020). Recent advances in digital multimedia tampering detection for forensics analysis. *Symmetry*, 12(11), 1811.
- [12] Sedeeq, I. (2023). Image Splicing Detection Based on Discrete Wavelet Transform and co-occurrence Matrix. *Iraqi Journal of Science*, 5940-5951. [14] Tahaoglu, G., Ulutas, G., Ustubioglu, B., Ulutas, M., Nabiyeve, V. V. (2022). Ciratefi based copy move forgery detection on digital images. *Multimedia Tools and Applications*, 81(16), 22867-22902.
- [13] Mehta, R., Aggarwal, K., Koundal, D., Alhudhaif, A., Polat, K. (2021). Markov features based DTCWS algorithm for online image forgery detection using ensemble classifier in the pandemic. *Expert Systems with Applications*, 185, 115630.
- [14] Thepade, S. D., Chaudhari, P. R. (2021). Land usage identification with fusion of thepade SBTC and sauvola thresholding features of aerial images using ensemble of machine learning algorithms. *Applied Artificial Intelligence*, 35(2), 154-170.
- [15] 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.
- [16] Freund, Y., Schapire, R. E. (1996, July). Experiments with a new boosting algorithm. In *icml* (Vol. 96, pp. 148-156).
- [17] Patel, H. H., Prajapati, P. (2018). Study and analysis of decision tree based classification algorithms. *International Journal of Computer Sciences and Engineering*, 6(10), 74-78.
- [18] Kumari, K., Yadav, S. (2018). Linear regression analysis study. *Journal of the practice of Cardiovascular Sciences*, 4(1), 33-36.
- [19] Keerthi, S. S., Shevade, S. K., Bhattacharyya, C., Murthy, K. R. K. (2001). Improvements to Platt's SMO algorithm for SVM classifier design. *Neural computation*, 13(3), 637-649.
- [20] Basilio, J. A. M., Torres, G. A., Perez, G. S., Medina, L. K. T., Meana, H. M. P. (2011). Explicit image detection using YCbCr space color model as skin detection. *Applications of Mathematics and Computer Engineering*, 123-128.
- [21] Tammina, S. (2019). Transfer learning using vgg-16 with deep convolutional neural network for classifying images. *International Journal of Scientific and Research Publications (IJSRP)*, 9(10), 143-150.
- [22] Hebbar, Nagaveni K., and Ashwini S. Kunte. "TRANSFER LEARNING APPROACH FOR SPLICING AND COPY-MOVE IMAGE TAMPERING DETECTION." *ICTACT Journal on Image Video Processing* 11.4 (2021).