International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume 15 (2023) pp. 479-488
© MIR Labs, www.mirlabs.net/ijcisim/index.html

# Machine Learning Based Image Forgery Detection using Feature Fusion of Otsu Binarization and Thepade SBTC

**Sudeep D. Thepade[1], Sanjit W. Jha[2]**

[1,2] Computer Engineering, Pimpri Chinchwad College of Engineering,
*Pune, India*
*[1]sudeepthepade@gmail.com, [2]jhas10474@gmail.com*

***Abstract*: Digital images are essential in every field, including clinical imaging, media broadcasting, crime analysis, and scientific research. The development of robust image editing software has simplified the process of manipulating photographs and changing their content. The image may now have important aspects added, modified, or removed without leaving any visible indications of manipulation. As a result, there is a need to design reliable methods to detect such manipulations. The paper proposes a technique for detecting tampered images using machine learning models trained on feature vectors generated by a fusion of the local features generated with the Otsu binarization technique and global features formed with Thepade Sorted Block Truncation Coding (Thepade SBTC). The proposed forgery detection methodology is empirically validated on the MICC-F220 dataset of 220 photos (with equal tampered and genuine images) using ten machine-learning classifiers and four ensembles. The best performance is given by the majority voting ensemble of Random Forest+ Random Tree + IBK with the feature fusion of Otsu binarization with Thepade SBTC 10-ary features. The fusion of features has shown better image forgery detection capability over consideration of individual features.**

***Keywords:*** Image Forgery Detection, Otsu Binarization, Thepade's SBTC, Machine Learning Classifiers, Ensembles

## I. Introduction

Rapid development in the field of technology has simplified the process of sharing images. Public opinions are shaped by circulating images to a broad audience. The various image editing tools available on the Internet are very convenient, making digital images vulnerable to manipulation. Such photos are widely circulated on social media and can result in the spread of false information. Image forgery is modifying images to offer misleading information or conceal valuable facts. Splicing, retouching, and copy-move are some techniques for tampering with images. Copy-Move is a technique that can be used to alter an image. It involves copying a part of it into the same image. Splicing involves performing image manipulation by integrating a part of another image. The process of modifying the subject's appearance in an image is retouching.

Such manipulations lead to inconsistent image-specific properties. These inconsistencies are used for detecting image manipulations. The feature vector of an image is generated using various feature extraction methods. Classifiers are trained on these feature vectors to detect whether the image is pristine or forged. Classifiers use artificial intelligence to detect forgeries that are invisible to the naked eye.

The research here investigates the extraction and representation of appropriate image contents to build feature vectors and integrate these descriptors to identify tampered images better. The paper proposes combining local and global image features obtained from the image using the Otsu binarization and Thepade SBTC methods.

The novelty of the methodology proposed here is:

- Feature fusion of local and global image features extracted using Otsu binarization and Thepade SBTC for improved detection of image tampering
- Exploration of variations of Thepade SBTC from 2-ary to 10-ary for the proposed image tampering detection method
- Validation of ten different machine learning algorithms and four different ensembles through experimentation in the proposed method for detecting tampered images

## II. Literature Survey

The digital evolution of image editing tools has made image tampering very easy. Detection of image tampering is becoming difficult with the bare eye. There is a need for techniques to detect the tampering of digital images. In literature, attempts are mainly made to devise image tampering detection methods in broadly three categories alias with machine learning algorithms being trained on explicitly extracted features, deep learning models and a hybrid of machine and deep learning models. In the machine learning model-based image tampering detection attempts, the image features are extracted individually as local or global feature

| Authors | Year of Publication | Feature Extractors | Classifier | Dataset | Performance |
|---|---|---|---|---|---|
| Alahmadi et al. [1] | 2013 | DCT | SVM | CASIA | Accuracy: 97% |
| He et al. [2] | 2012 | DWT, DCT | SVM-RFE | CASIA | Accuracy: 89.76% |
| Bunk et al. [4] | 2017 | CNN, LSTM | Deep Neural Network | NIST Nimble 2016 | Accuracy: 94.86%, AUC: 0.9138 |
| Kaur and Gupta [8] | 2016 | DWT | SVM | CASIA, Columbia | Accuracy: 97.34%, AUC: 0.9935 |
| Rao and Ni [3] | 2016 | SRM-CNN | SVM | CASIA V1.0 | Accuracy: 98.04% |
| Zhao et al. [7] | 2015 | BDCT, DMWT | SVM | DVMM | TPR: 92.99%, TNR: 93.75%, Accuracy: 93.36% |
| Vidyadharan et. al. [5] | 2017 | STP | Random Forest | CASIA | Precision: 98.14%, Recall: 96.76%, TNR: 97.33%, Accuracy: 96.99% |
| Abrahim et al. [6] | 2019 | LBP, HOG | ANN | CASIA v1 | Accuracy: 97.4% |
| Deogar et al. [9] | 2019 | Pre-trained AlexNet | SVM | MICC-F220 | Accuracy: 93.94% |
| Agarwal and Verma [10] | 2020 | SLIC, VGGNet | APM | MICC-F220 | Accuracy: 95%, Recall: 89.58%, FPR: 0.55 |
| Yue et al. [11] | 2022 | SIFT | AdaLAM | CASIA, MICC-F220, CoMoFoD, Coverage | Precision: 0.867, Recall: 0.945, F1: 0.904 |
| Tahaoglu et al. [12] | 2022 | SIFT | key point- matching, Ciratefi | GRIP, CMH | F1: 0.96 |
| Mehta et al. [13] | 2021 | DCT, DWT, Spatial | Ensemble Classifier | DVMM | Accuracy: 99.96% |
| Siddiqi et al. [14] | 2021 | DWT, LBP | SVM | DVMM, CASIA | Accuracy: 98.95%, TPR: 99.91%, |

*Table 1.* A review of existing image tampering detection algorithms

The fusion of local and global features for image tampering detection will be interesting.

The method for detecting image splicing given in [1] extracts chroma channel features based on the chrominance of an image. Each chroma's local binary pattern (LBP) is then translated into 16x16 blocks using DCT (Discrete Cosine Transform). The author calculated the standard deviation characteristics from these DCT coefficients. The SVM classifier trained with these attributes was used for classification.

A method for detecting tampered images through the image's DWT(Discrete Wavelet Transform) and DCT characteristics is proposed in the paper [2]. The Markov features are generated using the DWT and DCT (Discrete Wavelet Transform) coefficients, and SVM-RFE is utilized to minimize the feature set to reduce computational costs. The SVM algorithm is trained using the dataset and used for detecting forgeries.

Rao and Ni [3] present a novel deep learning-based method to detect splicing and copy-move forgeries, which extracts the image's hierarchical features based on manipulations using a supervised CNN [21]. Ten distinct layers make up the CNN architecture used for automatic feature learning. A pre-trained CNN extracts a feature-set from the query image. These are then combined to generate the final set of unique features. The SVM classifier uses these features for binary classification.

Paper [4] incorporated two ways of detecting image tampering. A deep neural network is utilized in the first technique to identify modified images using handcrafted features. The second technique uses an LSTM (Long Term Short Memory) network to study correlations between consecutive blocks of resampling characteristics and select relevant attributes. These features are then fed to the SoftMax layer for authenticating the image.

In the method proposed by [5], descriptors such as BGP, LBP, etc., are used to represent the image. After applying the Steerable Pyramid Transform, the texture attributes are retrieved from each subband [20]. A compact model of the image is generated by employing the relief feature selection approach. The Random Forest Classifier trained on the Casia v2 was used for the classification

The method produced 97% accurate results. The shortcoming of the method is that choosing only a single colour in the YCbCr colour space may result in data loss.

The technique proposed for classification by the author in [6] employs an Artificial Neural Network, and a combination of LBP, HOG and HOS (Higher Order Statistics) Features for forgery detection. The approach is very complex because LBP is determined for each colour channel.

A two-dimensional noncausal model proposed in [7] captures the underlying association between the pixels and their neighbours. Cross-domain characteristics are retrieved employing the DCT and DWT characteristics of the blocks. The method's main drawback is the feature vector's high dimensionality.

The DWT domain of the image is used to retrieve the LBP (Local Binary Patterns) in the technique proposed in [8]. The final image representation is generated by combining DWT feature combinations of all four subbands. The technique gives the most promising results when trained on the chrominance channel of the image using the SVM classifier.

The detection technique in [9] used a Pre-trained Alex Net model to detect image tampering operations. Using the MICC-F220 dataset, a Pre-trained Alex Net model extracts 4096-element deep feature vectors from input photos. After extracting characteristics, an SVM model classifies the image as original or faked.

To detect the alterations done to digital photographs for forensic purposes, [10] devised a deep learning-based approach. Using the SLIC(Simple Linear Iterative Clustering approach), an input image was fragmented into its constituent parts. The researchers utilized a VGGNet, which stands for Visual Geometry Group-net, to extract important features from input images. In order to identify tampered images, they employed the Adaptive Patch Matching (APM) method.

The image forgeries can be found using the methodology described by [11]. With the SIFT method's help, the input image's feature vector was calculated. Then, the level of resemblance between features was computed to identify the replicated regions. In the final stage, the AdaLAM algorithm isolates the manipulated region. The performance of the model drops for samples with huge-angle modifications.

Paper [12] developed an approach for detecting tampering operations in digital photos. The SIFT method was utilized to extract the image's textual content. Then, the modifications were identified by employing a key point-matching technique. The Ciratefi method was then implemented to localize the modified regions. The model demonstrates improved image forgery detection capabilities against scaling and rotation attacks but struggles with photos with intense brightness changes.

In [13], the author put forth a method for image forgery detection by analyzing the image's Markov features through its DCT, DWT, and Spatial characteristics. These features are then processed using PCA to reduce their dimensionality and passed to an ensemble classifier with the AdaBoost algorithm to identify tampered images.

Another method was developed by [14] for detecting tampered images. This method explores the DWT domain of the image's Cb and Cr channels to retrieve the dominant rotated LBP (Local Binary Patterns). The final depiction of the image is generated by combining the DRLBP of all the subbands. The technique gives the most promising results using the SVM classifier.

Table 1 provides a tabular comparison of the relevant papers from the literature survey.

## III. Proposed Image Forgery Detection Technique Using Feature Fusion of Otsu Binarization and Thepade SBTC

Figure 1 shows the proposed technique for detecting image tampering. The proposed technique is split into two parts. The first part, i.e., the training phase, involves generating the feature vector and training machine learning algorithms. The feature vector of every image is attained using a fusion of Thepade SBTC and Otsu binarization techniques. Various classifiers and their ensembles learn using these feature vectors. The testing phase involves passing the extracted feature vector of the test sample to the trained classifiers/ ensembles. The model estimates image authenticity.

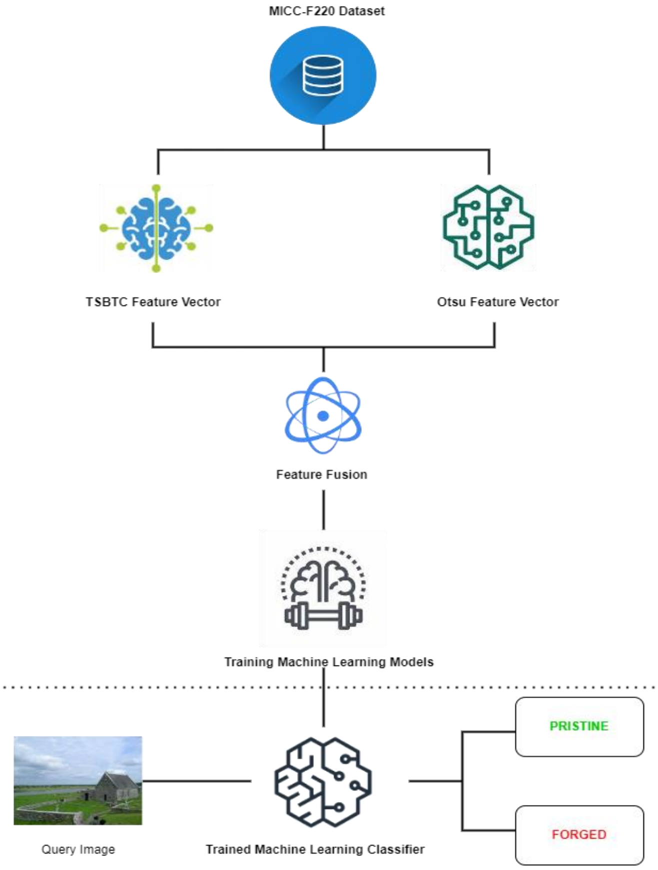

**Figure 1.** Proposed model for detecting image forgery using proposed feature fusion of Otsu binarization and Thepade SBTC

*A. Feature Extraction using Thepade SBTC:*

Let us consider an image made up of 'r*c' pixels. In the Thepade SBTC technique, RGB colour channels of the image are flattened to 1D arrays and sorted in nondecreasing order to get sortR, sortG, and sortB. The ordered arrays are then used to generate the Thepade SBTC N-ary feature vector [ $TB_{1\ldots n}$, $TG_{1\ldots n}$, $TR_{1\ldots n]}$ using the following equations:

$$TR_i = \frac{n}{r*c} \sum_{q=\frac{(r*c)*(i-1)}{n}+1}^{\frac{i*(r*c)}{n}} sortR(q) \qquad (1)$$

$$TG_i = \frac{n}{r*c} \sum_{q=\frac{(i-1)*(r*c)}{n}+1}^{\frac{i*(r*c)}{n}} sortG(q) \qquad (2)$$

$$TB_i = \frac{n}{r*c} \sum_{q=\frac{(i-1)*(r*c)}{n}+1}^{\frac{i*(r*c)}{n}} sortB(q) \qquad (3)$$

*B. Feature Extraction using Otsu Binarization technique:*

The Otsu binarization technique [17] finds an appropriate threshold to separate image color plane pixels into two classes. The discriminating parameter, which optimizes the separability between foreground and background classes, is used to decide the suitable threshold, which maximizes the inter-class variance. The Otsu thresholding technique determines the minimum and maximum values ($L_{min}$ and $L_{max}$) of the input image

The following equation normalizes the histogram of an image as a probability distribution:

$$p_i = \frac{l_i}{N} \text{ where } p_i \geq 0 \qquad (4)$$

$$\sum_{i=L_{min}}^{L_{max}} p_i = 1 \qquad (5)$$

Where '$l_i$' is the number of pixels having the intensity value 'i' in an image containing N pixels.

The threshold value k divides the pixel values into $class_0$ and $class_1$, where $class_0$ represents the image pixel value in the range ($L_{min}$, k) and $class_1$ represents the values in the range (k+1, $L_{max}$).

The next step in optimal threshold computation involves calculating the average and class probabilities using the following equations:

$$\underline{x}_0 = \sum_{i=L_{min}}^{k} i * p_i \qquad (6)$$

$$\underline{x}_1 = \sum_{i=k+1}^{L_{max}} i * p_i \qquad (7)$$

$$\omega_0 = \sum_{i=L_{min}}^{k} p_i \qquad (8)$$

$$\omega_1 = \sum_{i=k+1}^{L_{max}} p_i \qquad (9)$$

The formula for calculating the between-class variance is:

$$\sigma^2 = \omega_0 (\underline{x}_0 - \underline{x}_T)^2 + \omega_1 (\underline{x}_1 - \underline{x}_T)^2 \qquad (10)$$

Where,

$$\underline{x}_T = \sum_{i=L_{min}}^{L_{max}} i * p_i = \omega_1 \underline{x}_1 + \omega_0 \underline{x}_0 \qquad (11)$$

Substituting the value of $\underline{x}_T$ in equation 10,

$$\sigma^2 = \omega_1 * \omega_0 * (\underline{x}_0 - \underline{x}_1) \qquad (12)$$

The optimal threshold value k, which maximizes the between-class variance, is:

$$\sigma^2(k) = max(\sigma^2(i)) \text{ where } L_{min} \leq i \leq L_{max} \qquad (13)$$

For a given image, a threshold value is calculated using the Otsu thresholding technique, which calculates the average pixel intensity of class $C_0$ and $C_1$ for red, green and blue channels. These values are combined to create the image's feature vector.

*C. Ensemble of Classifiers [16,19]:*

The Bayesian, Functions, Lazy, and Tree classifiers are trained for detecting the image forgeries using the generated feature vectors. The Ensemble classifiers are built using The majority voting logic to assess the performance improvement of the presented method. The machine learning classifiers considered for experimentation in the proposed method are enlisted in Table 2.

| Family | Classifiers used |
|---|---|
| Bayes | Naive Bayes, BayesNet |
| Lazy | KStar, IBK |
| Tree | Random Forest ,J48, Random Tree |
| Functions | SMO, Simple Logistic, and Multilayer Perceptron |

*Table 2.* Classifiers considered for experimentation

*D. Dataset used for Model training:*

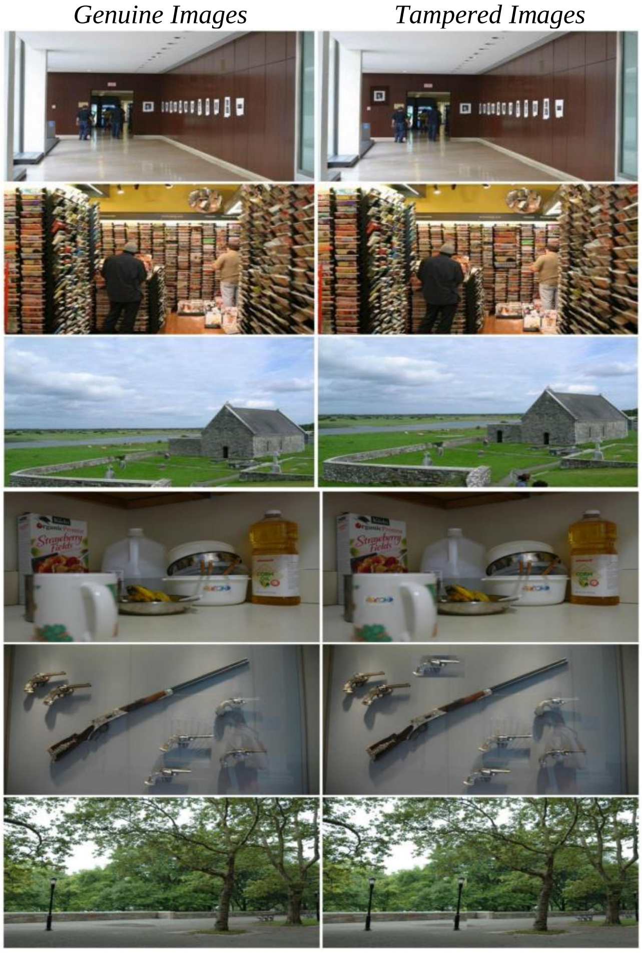

**Figure 2.** Samples of genuine and tampered images from the dataset [15]

To train and evaluate the image forgery identification algorithm, the MICC - F220 dataset has been utilized [15]. There are 220 pictures in the dataset(110 pristine and 110 forged). Images come in JPG format and vary in size from 722 x 480 to 800 x 600. Images were modified with the copy-and-paste method. Figure 2 shows a small selection of photos from the MICC-F220 dataset.

*E. Performance Metrics:*

1] Accuracy: Accuracy is a popular indicator for gauging a classifier's efficacy on evenly distributed training data. In other words, it is the proportion of successful forecasts to total model predictions. Accuracy is formally determined via equation 14:

$$Accuracy = \frac{TP+TN}{FP+TP+FN+N} \quad (14)$$

Where:

- The count of observations the model wrongly interpreted as negative is denoted by FN (False Negative).
- True Negative (TN) is the fraction of data points for which the model made an accurate negative prediction.
- True Positive (TP) denotes the count of observations that were correctly identified as positive by the model,
- The number of times the model wrongly classifies a set of observations as positive is the number of FPs (False Positive).

2] F-Measure: This is a popular statistic for gauging the efficacy of a binary classification model since it provides an overall measure of performance by incorporating both precision and recall into a single value [18]. For formal purposes, we use equation 15 to determine the F-measure:

$$F - measure = \frac{2 * precision * recall}{precision + recall} \quad (15)$$

Where:

- Precision is a measure of how many correct positive predictions the model makes relative to the overall positives predicted.
- Recall measures how many correct positive predictions were made relative to the total instances of positive observations.

## IV. Results and Discussion

The proposed approach of picture forgery detection was trained on the MICC-F220 dataset, having 110 original photos and 110 altered images. Ten different classifiers and four different ensembles were utilized during the training phase.

The f-measure and the percentage accuracy are going to be used as the performance metrics for evaluating the suggested method. The following discussion will focus on the findings of the experiment:

*A. Otsu binarization-based image forgery detection*

Performance analysis of 10 machine learning classifiers (SMO, Simple Logistic, NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, RandomForest) and their four ensembles (RandomTree + IBK + KStar, RandomForest+KStar+RandomTree, RandomForest + IBK+RandomTree, RandomForest + KStar + IBK) trained using features extracted by Otsu binarization technique is shown in Figure 3. The ensemble of 'RandomTree + RandomForest + IBK' gives the best percentage accuracy indicating better image forgery detection capability, followed by the RandomForest algorithm. Ensembles show better Accuracy as compared to individual classifiers.

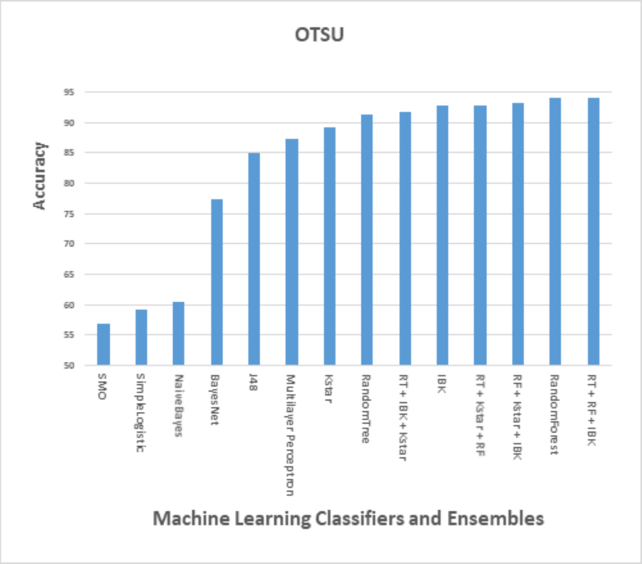

**Figure 3.** Performance comparison of various classifiers and their ensembles using Accuracy for

The F-Measure-based performance analysis of the ten classifiers (SMO, SimpleLogistic, NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, RandomForest) and four ensembles 'RandomTree + IBK + KStar', 'RandomForest+ KStar+ RandomTree', 'RandomForest+ IBK+ RandomTree', 'RandomForest + KStar + IBK' trained using the feature vector generated using Otsu thresholding technique is shown in Figure 4. The 'RandomTree + RandomForest + IBK' ensemble gives the best F-measure, followed by the RandomForest algorithm.

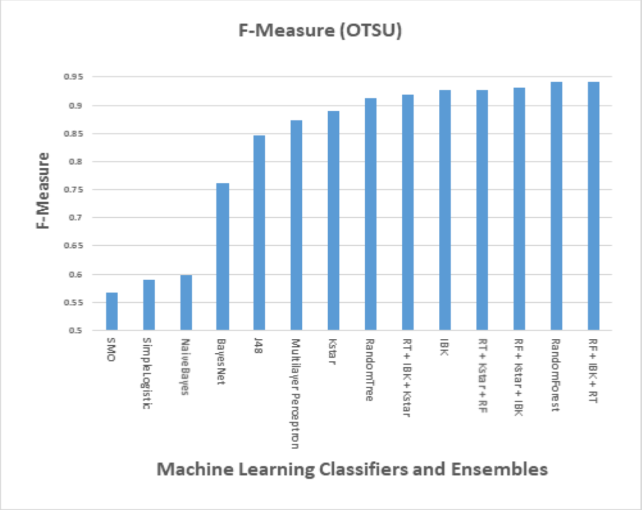

**Figure 4.** Performance comparison of various classifiers and their ensembles based on F-measure for Otsu binarization-based image forgery detection

*B. TSBTC-based image forgery detection*

Performance analysis of 10 classifiers (SMO, SimpleLogistic, NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, RandomForest) trained using features extracted by TSBTC N-ary technique is potrayed in Figure 5. It is observed from the graph that a combination of TSBTC 10-ary and Random Forest classifiers has the utmost accurate results, with an accuracy of 94.1%. Random Forest gives the best performance overall, followed by the IBK algorithm

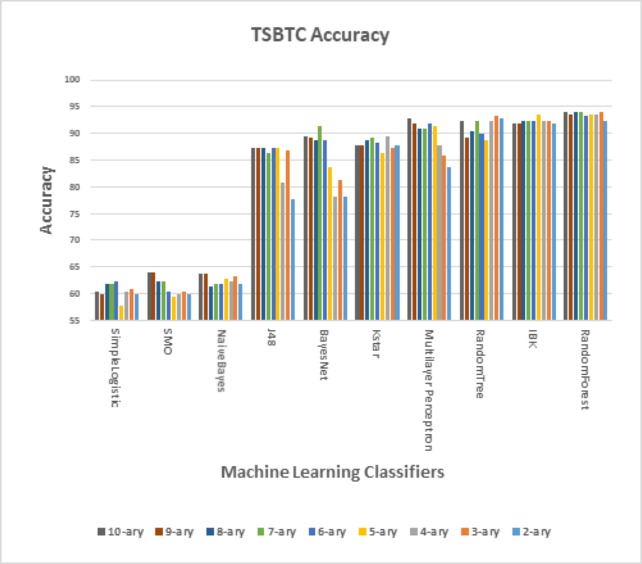

**Figure 5.** Performance comparison of various classifiers based on Accuracy for TSBTC N-ary method-based image forgery detection.

Figure 6 depicts the evaluation of the F- scores of 10 classifiers (SMO, SimpleLogistic, NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, RandomForest) trained on features extracted by TSBTC n-ary technique. The graph shows that Random Forest delivers the highest performance (0.941) for the feature vector generated using the TSCTC 10-ary technique. Random Forest outperforms the IBK algorithm in terms of overall performance.

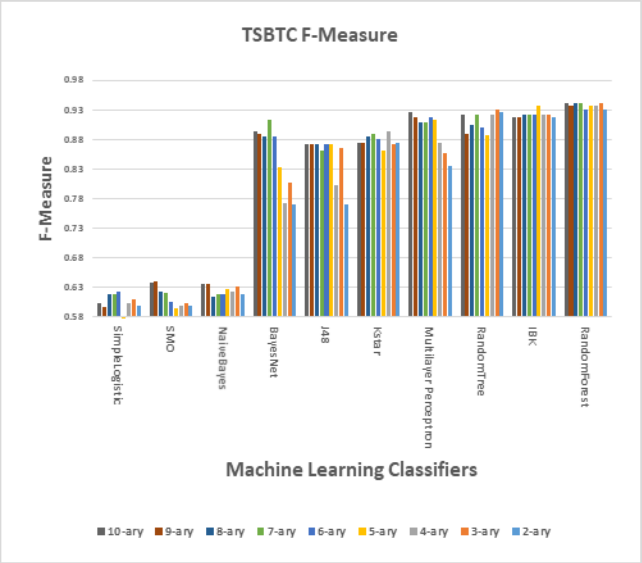

**Figure 6.** Performance evaluation of various classifiers based on F-measure for TSBTC N-ary method-based image forgery detection.

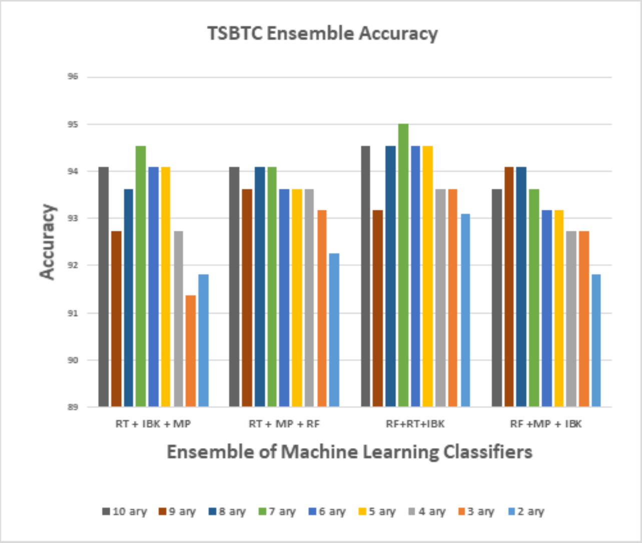

**Figure 7.** Performance comparison of the ensemble of classifiers based on Accuracy for the TSBTC N-ary method-based image forgery detection.

The graph in Figure 7 depicts the performance of ensembles(RandomTree + IBK + Multilayer Perceptron, RandomForest + Multilayer Perceptron + RandomTree, RandomForest + IBK+RandomTree, RandomForest + Multilayer Perceptron + IBK) using Accuracy as the performance metric. The graph shows that the ensemble of RandomForest + IBK+RandomTree for TSBTC 7-ary gives the best performance with Accuracy as high as 95%, which betters the previous best performance of RandomForest.

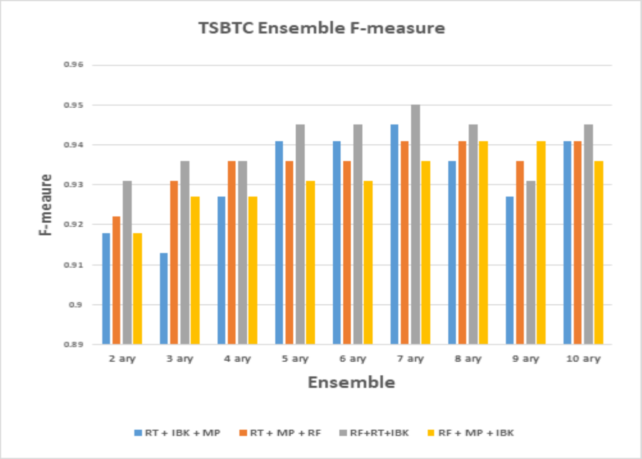

**Figure 8.** Performance evaluation of ensemble of classifiers based on F - measure for TSBTC N-ary method-based image forgery detection.

The graph in Figure 8 depicts the performance of ensembles (RandomTree + IBK + Multilayer Perceptron, RandomForest + Multilayer Perceptron + RandomTree, RandomForest + IBK+RandomTree, RandomForest + Multilayer Perceptron + IBK) using F-measure as the performance metric. The graph is similar to the Accuracy-based graph with RandomForest + IBK+RandomTree giving the best performance

*C. Fusion based image forgery detection*

Figure 9 depicts the Accuracy of 10 classifiers (SMO, SimpleLogistic, NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, RandomForest) trained using features extracted by a combination of TSBTC N-ary and Otsu binarization techniques. The graph shows that a combination of TSBTC 10-ary + Otsu and Random Forest classifiers has the maximum accurate results with an accuracy of 94.54%.

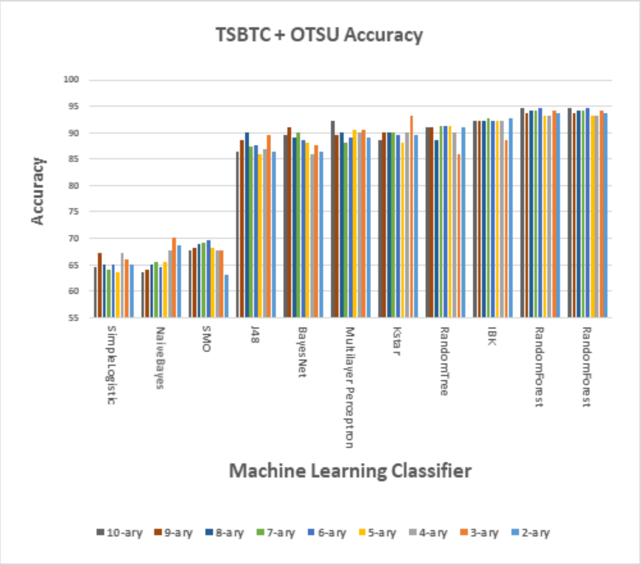

**Figure 9.** Performance evaluation of classifiers based on Accuracy for TSBTC N-ary + Otsu Binarization method-based image forgery detection.

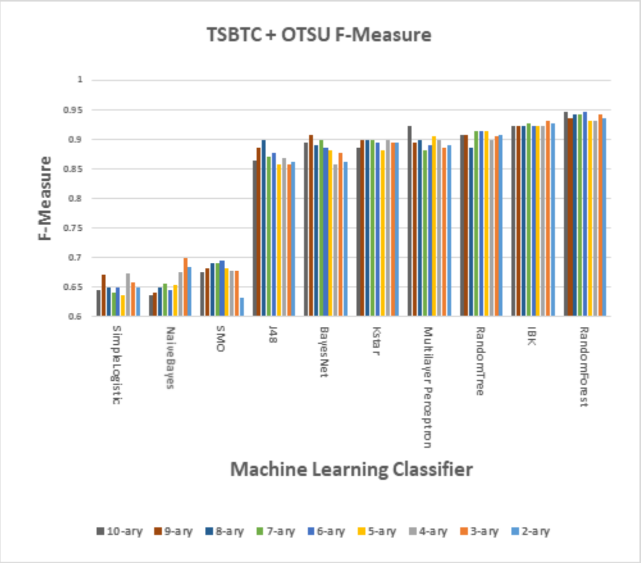

**Figure 10.** Performance evaluation of classifiers based on F-Measure for TSBTC N-ary + Otsu Binarization method-based image forgery detection.

Figure 10 depicts the evaluation of the F- Measures of 10 classifiers (SMO, SimpleLogistic, NaiveBayes, BayesNet, J48, Multilayer Perceptron, KStar, RandomTree, IBK, RandomForest) trained on features extracted by a fusion of TSBTC n-ary and Otsu binarization technique. The graph shows that Random Forest delivers the highest performance (0.945) for the feature vector generated using the TSCTC 10-ary technique. Random Forest outperforms the IBK algorithm in terms of overall performance.

| Paper | Year of Publication | Feature Extractor | Classifier | Dataset | Accuracy |
|---|---|---|---|---|---|
| [13] | 2021 | DCT, DWT, Spatial | Ensemble Classifier | DVMM | 99.96% |
| [14] | 2021 | DWT, LBP | SVM | DVMM, CASIA | 98.95% |
| [3] | 2016 | SRM-CNN | SVM | CASIA v1.0 | 98.04% |
| [1] | 2013 | DCT | SVM | CASIA | 97% |
| [8] | 2016 | DWT | SVM | Columbia, CASIA | 97.34% |
| [5] | 2017 | SPT | Random Forest | CASIA | 96.99% |
| **Proposed Model** | 2023 | TSBTC+OTSU | Ensemble Classifier | MICC-F220 | 95% |
| [4] | 2017 | CNN, LSTM | Deep Neural Network | NSIT Nimble 2016 | 94.86% |
| [9] | 2019 | Pre-trained AlexNet | SVM | MICC-F220 | 93.94% |
| [7] | 2015 | BDCT, DMWT | SVM | DVMM | 93.36% |
| [2] | 2012 | DWT, DCT | SVM-RFE | CASIA | 89.76% |
| [10] | 2020 | SLIC, VGGNet | APM | MICC-F220 | 95% |

*Table 3.* A tabular comparison of the performance of existing and Proposed methodology.

Figure 11 represents the Accuracy of the four ensembles (RandomTree + IBK + KStar, RandomForest + KStar + RandomTree, RandomForest + IBK + RandomTree, RandomForest + KStar + IBK) trained using the features extracted by a fusion of Otsu thresholding and TSBTC technique. The best performance is given by the ensemble of RandomForest + IBK + RandomTree for the feature vector generated using the TSBTC 10-ary and Otsu binarization technique. From the graph, we can conclude that ensembles give higher Accuracy than individual classifiers.

The above graph in Figure 12 depicts the performance of ensembles (RandomTree + IBK + Multilayer Perceptron, RandomForest + Multilayer Perceptron + RandomTree, RandomForest + IBK+RandomTree, RandomForest + Multilayer Perceptron + IBK) using F-measure as the performance metric. The graph shows that the ensemble of RandomForest + IBK + RandomTree has the highest F-Measure of 0.95 for the Feature vector generated using the TSBTC 10-ary and Otsu binarization technique. Ensembles have a comparatively higher F-measure than individual classifiers.

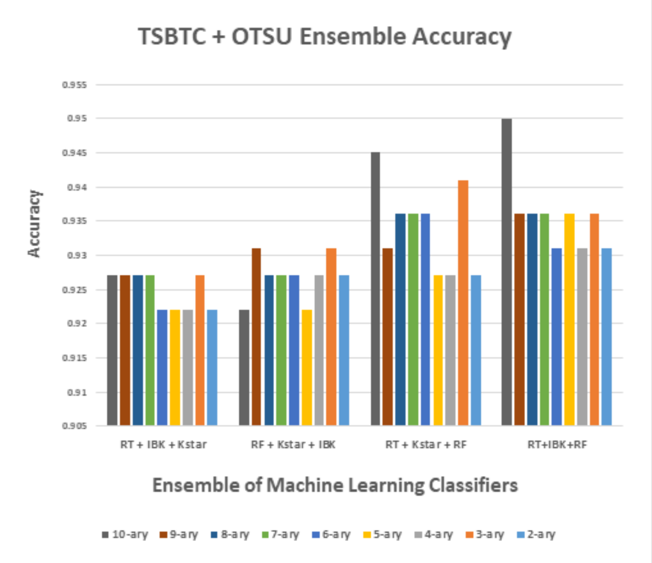

**Figure 11.** Performance comparison of the ensemble of classifiers using Accuracy as the performance metric for a combination of TSBTC n-ary and Otsu binarization-based image forgery detection.

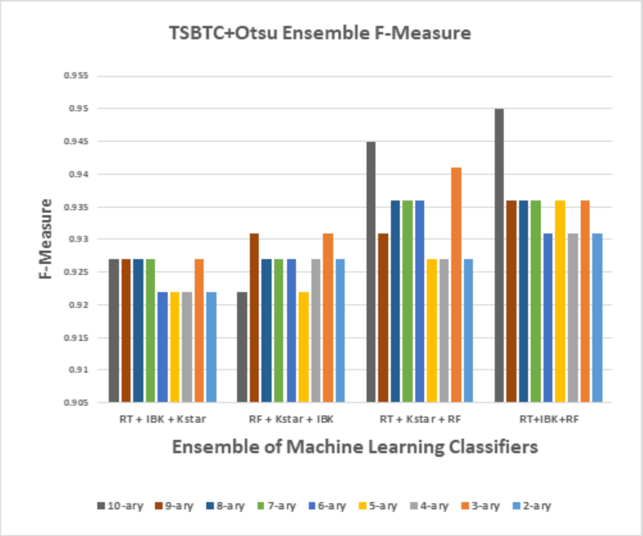

**Figure 12.** Performance evaluation of ensemble of classifiers based on F – measure for a combination of TSBTC n-ary and Otsu binarization-based image forgery detection.

A comparative performance analysis of the proposed and the existing techniques for detecting image forgeries using Accuracy as the metric has been tabulated in Table 3. The Accuracy (95%) of the proposed method is comparatively superior than the models proposed by [4,9,7,2,10]. A few state-of-the-art algorithms detect forgeries more accurately than the model proposed, and further studies could be undertaken to enhance the suggested model's potential for detecting manipulated image.

## V. Conclusion

With technological advancement, various sophisticated image manipulation tools have been developed to create forgeries undetectable to the naked eye. Therefore, there is a need for techniques that can efficiently and accurately detect the presence of invisible manipulations in images. The paper proposes a technique for training the various classifiers and their ensemble on image feature vectors extracted using a fusion of Otsu binarization and TSBTC techniques for improved image forgery detection. Experimentation on 220 images of the MICC- F220 dataset gives very good Accuracy. Overall, the feature vector generated using a feature-level fusion of TSBTC + Otsu detected image tampering more accurately. The feature vector generated using TSBTC 10-ary yielded the best performance(95% accuracy) for the ensemble of IBK + RandomForest + RandomTree. When compared to individual algorithms, ensembles delivered better results. In future, the effect of integrating several feature extraction algorithms for detecting image manipulations will be quite fascinating to investigate.

## VI. References

[1] Alahmadi, Amani A., Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, and George Bebis. "Splicing image forgery detection based on DCT and Local Binary Pattern." In 2013 IEEE Global Conference on Signal and Information Processing, pp. 253-256. IEEE, 2013.

[2] He, Zhongwei, Wei Lu, Wei Sun, and Jiwu Huang. "Digital image splicing detection based on Markov features in DCT and DWT domain." Pattern recognition 45, no. 12 (2012): 4292-4299.

[3] Rao, Yuan, and Jiangqun Ni. "A deep learning approach to detection of splicing and copy-move forgeries in images." In 2016 IEEE international workshop on information forensics and security (WIFS), pp. 1-6. IEEE, 2016.

[4] Bunk, Jason, Jawadul H. Bappy, Tajuddin Manhar Mohammed, Lakshmanan Nataraj, Arjuna Flenner, B. S. Manjunath, Shivkumar Chandrasekaran, Amit K. Roy-Chowdhury, and Lawrence Peterson. "Detection and localization of image forgeries using resampling features and deep learning." In 2017 IEEE conference on computer vision and pattern recognition workshops (CVPRW), pp. 1881-1889. IEEE, 2017.

[5] Vidyadharan, Divya S., and Sabu M. Thampi. "Digital image forgery detection using compact multi-texture representation." Journal of Intelligent & Fuzzy Systems 32, no. 4 (2017): 3177-3188.

[6] Abrahim, Araz Rajab, Mohd Shafry Mohd Rahim, and Ghazali Bin Sulong. "Splicing image forgery identification based on artificial neural network approach and texture features." Cluster Computing 22 (2019): 647-660.

[7] Zhao, Xudong, Shilin Wang, Shenghong Li, and Jianhua Li. "Passive image-splicing detection by a 2-D noncausal Markov model." IEEE Transactions on Circuits and Systems for Video Technology 25, no. 2 (2014): 185-199.

[8] Kaur, Mandeep, and Savita Gupta. "A passive blind approach for image splicing detection based on DWT and LBP histograms." In Security in Computing and Communications: 4th International Symposium, SSCC 2016, Jaipur, India, September 21-24, 2016, Proceedings 4, pp. 318-327. Springer Singapore, 2016.

[9] Doegar, Amit, Maitreyee Dutta, and Kumar Gaurav. "Cnn based image forgery detection using pre-trained alexnet model." International Journal of Computational Intelligence & IoT 2, no. 1 (2019).

[10] Agarwal, Ritu, and Om Prakash Verma. "An efficient copy move forgery detection using deep learning feature extraction and matching algorithm." Multimedia Tools and Applications 79, no. 11-12 (2020): 7355-7376.

[11] Yue, Guangyu, Qing Duan, Renyang Liu, Wenyu Peng, Yun Liao, and Junhui Liu. "SMDAF: A novel keypoint based method for copy-move forgery detection." IET Image Processing 16, no. 13 (2022): 3589-3602.

[12] Tahaoglu, Gul, Guzin Ulutas, Beste Ustubioglu, Mustafa Ulutas, and Vasif V. Nabiyev. "Ciratefi based copy move forgery detection on digital images." Multimedia Tools and Applications 81, no. 16 (2022): 22867-22902.

[13] Mehta, Rachna, Karan Aggarwal, Deepika Koundal, Adi Alhudhaif, and Kemal Polat. "Markov features based DTCWS algorithm for online image forgery detection using ensemble classifier in the pandemic." Expert Systems with Applications 185 (2021): 115630.

[14] Siddiqi, Muhammad Hameed, Khurshed Asghar, Umar Draz, Amjad Ali, Madallah Alruwaili, Yousef Alhwaiti, Saad Alanazi, and M. M. Kamruzzaman. "Image splicing-based forgery detection using discrete wavelet transform and edge weighted local binary patterns." Security and Communication Networks 2021 (2021): 1-10.

[15] Amerini, Irene, Lamberto Ballan, Roberto Caldelli, Alberto Del Bimbo, and Giuseppe Serra. "A sift-based forensic method for copy–move attack detection and transformation recovery." IEEE transactions on information forensics and security 6, no. 3 (2011): 1099-1110.

[16] Badre, Shalakha R., and Sudeep D. Thepade. "Novel video content summarization using Thepade's sorted n-ary block truncation coding." Procedia Computer Science 79 (2016): 474-482.

[17] Otsu, Nobuyuki. "A threshold selection method from gray-level histograms." IEEE transactions on systems, man, and cybernetics 9, no. 1 (1979): 62-66.

[18] Sasaki, Yutaka. "The truth of the F-measure". University of Manchester. Available online: http://www.flowdx.com/F-measure-YS-26Oct07. pdf (accessed on 20 October 2022).

[19] Thepade, Sudeep D., and Piyush R. Chaudhari. "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, no. 2 (2021): 154-170.

[20] Thakur, Rahul, and Rajesh Rohilla. "Recent advances in digital image manipulation detection techniques: A brief review." Forensic science international 312 (2020): 110311.

[21] Walia, Savita, Krishan Kumar, Munish Kumar, and Xiao-Zhi Gao. "Fusion of handcrafted and deep features for forgery detection in digital images." IEEE Access 9 (2021): 99742-99755.

## Author Biographies

**Dr Sudeep D. Thepade** is a Professor in the Computer Engineering Department at Pimpri Chinchwad College of Engineering, affiliated with Savitribai Phule Pune University, Pune, Maharashtra, India. He completed his PhD in 2011. He has over 400 research papers to his credit published in International/ National Conferences and Journals. His domain of interest is Image Processing, Image Retrieval, Video Analysis, Video Visual Data Summarization, Biometrics and Biometric Liveness Detection. He is a member of the International Association of Engineers (IAENG) and the International Association of Computer Science and Information Technology (IACSIT). He has served as a Technical Program Committee member and Reviewer for Several International Conferences and Journals.

**Sanjit Wakilnarayan Jha** is pursuing his Bachelor of Technology (B.Tech.) degree in Computer Engineering from Pimpri Chinchwad College of Engineering, Maharashtra, India. His research areas are Data Science and Analytics, Image Processing, Machine Learning and Deep Learning.