A PRELIMINARY MINI PROJECT REPORT ON

“Image Forgery Detection”

SUBMITTED TOWARDS PARTIAL FULFILLMENT OF THE REQUIREMENTS OF INTERNAL EVALUATION-2 FOR SUBJECT: **COMPUTER VISION** (SEMESTER: 7)

(B.Tech, Div: B)

Academic Year: 2023-24

Submitted by:

Shreyash Kharde – BTCOB102
Ishwar Deore – BTCOB147
Dattatray Pandharmise – BTCOB141
Sugam Phirke – BTCOB152

Under the Guidance of:

Prof. Anil Pawar

DEPARTMENT OF COMPUTER ENGINEERING,
PIMPRI CHINCHWAD COLLEGE OF ENGINEERING,
PUNE

Abstract:

With the advent of increasing globalization in the world, the internet has paved various new ways for people to communicate their thoughts or ideas with the world. In the early 2000s, the world saw a rise in social media platforms. This indeed made communication easier and more interactive. It attracted people! It became a common platform for everyone to communicate on daily-basis. This collectively shaped the world into more connected and interdependent place.

Besides this, great amount of data is also generated from these social media activities every second. As the data increased with time, its vulnerability to get altered also increased. Primary data types like photos and videos are no longer reliable because they can be easily duped with tools like GNU Gimp, Adobe Photoshop, and other image and video editing applications. Such manipulated data is a major source of false information and is frequently utilised in malevolent ways, including to instigate mobs and spread false propaganda. The legitimacy must be confirmed before any action, based on a dubious image, is taken. Over years, to regain the faith in the image data and detect such doctored data, various methods have been implemented, and are still under development. In this paper, we shall aim at performing analysis on the feature extraction of images using the Thepade's Sorted Block Truncation Code (SBTC) Technique and Bernsen Local Thresholding Technique.

Introduction:

With the mobile manufacturing industry becoming more competitive, every provider company is attempting to provide the best in segment phones at a low price. Over the last few decades, this has resulted in an increase in cell phone users all over the world. . In 2022, the total figure of smartphone holders in the world have reached 6.648 billion, which corresponds to 83.32% of the current world population. As a result, data generation has become simple, and data is being generated at a much faster pace than ever before. As of April 2022, estimates say that there are over 5 billion people on the internet, who create 1.7 megabytes of data per second, on average. Tampered, altered, and fraudulent content is used and spread inappropriately over multimedia through many platforms. As the modification tools are easily available, it is challenging to accurately authenticate the multimedia content, especially images. Therefore, it has become imperative to develop a methodology or tool that can effectively recognize image forgery.

Image forgery is commonly divided in two types: Copy-Move forgery and Image splicing. In Copy-Move forgery, a compound picture is formed by cutting some object from image and adding it to same image, while Image splicing deals with composite pictures formed by cutting some object(s) from image and adding it to some another image. It is clearly evident that it is relatively difficult to detect image splicing. Retouching is also a type of image forgery which adjusts the colour, sharpness, brightness, noise, contrast, etc. It is done mainly to hide the differences in texture features (between the background and the incident image segment) occurred after forgery has been performed. Morphing, another kind of image forgery technique, smoothly changes an image to a different image through seamless transition between two images.

Many methods are and are being implemented for detecting the image splicing. They are divided in two types: Active/non-Blind and Passive/Blind techniques. The sole difference between both the techniques is that the former one depends on the prior information of the image such as a watermark or any signature at time of acquisition, the later one works by analysing content and statistics of image. As availability of such features is a major deterrent for Active techniques, Passive techniques have evolved a lot since last few decades.

After an image is forged, some irregularities are observed between the original segment and the doctored portion of the image. These irregularities can also be considered to create feature vectors for

detecting the forged images. The irregularities in texture pattern are easily detectable in the segmented images. Image segmentation is a technique for breaking up a digital image into smaller groupings called image segments, which reduces the complexity of the image and permits each picture segment to be subjected to further processing or analysis. Technically, segmentation is the process of giving labels to pixels in an image in order to distinguish between objects, persons, or other significant aspects. Image Thresholding is the simplest method of segmentation. It is a way to create a binary image from a grayscale or full-colour image. This is typically done in order to separate desired object or foreground pixels from background pixels, which aids in forgery detection. In this paper we work with the Bernsen Local thresholding technique to find the segmented images.

The remainder of the paper is structured as follows: Section 2 provides a thorough examination of existing techniques for image forgery detection. The proposed methodology will be described in Section 3. Section 4 comprises of detailing the experimental environment. Section 5 holds discussions about the results of the experimentation. Section 5 brings the paper to a conclusion.

Literature Review:

[1] A unique splicing picture forgery detection approach working with DCT and LBP is recommended in this research. The chromatic component of the picture was separated to overlapped blocks and the LBP code of every block is translated in to the DCT Domain. Following that, the standard deviations of coefficients of DCT, for all blocks, are calculated and utilized as features. For classification, the Support Vector Machine was used. The experimental findings reveal that the suggested chromatic channel characteristics outperform those of other colour channels. The suggested technique consistently outperforms the CASIA TIDE V1.0, Columbia and CASIA TIDE V2.0 datasets, with accuracies of 97%, 96.6% and 97.5% respectively.

[2] This work proposes a Markov-based method for detecting picture splicing in the DCT and DWT domains. The enlarged Markov features in the DCT domain and the Markov features in the DWT domain, which were produced using the transition probability matrices, make up the suggested feature vector. The latter was designed to define the dependence among coefficients of wavelet across locations, orientations, and scales the former was established to get the relation between the DCT coefficients. To manage a large number of produced features, the SVM-RFE feature selection technique is used. The last step is to use SVM as the classifier to identify picture splicing by making the use of the final dimensionality reduced feature vector. According to authors, experimental findings show that the suggested strategy can outperform many other approaches.

[3] In this study, Rao and Ni offer a revolutionary deep Convolutional Neural Network(CNN) based picture forgery detection method. In order to effectively suppress the influence of complex picture contents and hasten network convergence, the weights at the first layer of the network are initialised with the 30 fundamental high-pass filters employed in the Spatial Rich Model (SRM) for image steganography. The CNN model is used in this technique as a local patch descriptor, and it is pre-trained using labelled patch samples that were painstakingly created using only the fabricated borders in altered pictures. After extracting dense features from the test pictures using the pre-trained CNN, the ultimate discriminative features for SVM classification are created by combining the extracted features. Numerous tests using a variety of publicly available datasets were conducted, showing that the suggested CNN-based system performs better than existing state-of-the-art image forgery detection techniques.

[4] Two techniques to identify and pinpoint picture manipulation are discussed in this research. The paper provides two techniques for spotting and classifying fake images. In the first technique, the authors describe an end-to-end system based on the Radon transform and Deep Learning to identify and pinpoint these digital changes. In the second, authors characterise tampered patches by integrating

resampling features based on Probability-maps (p-maps) and Long Short-Term Memory (LSTM)-based modelling. The tests demonstrated that both LSTM-based networks and Convolutional Neural Networks (CNNs) are efficient at utilising resampling characteristics to identify tampered areas.

[5] This research suggests a scalable multi-texture representation for the identification of fake images. According to experimental findings, the complementing discriminative strength of distinct texture descriptors enables the multi-texture representation to more effectively capture small texture differences. The four texture descriptors LBP, LPQ, BGP and BSIF were considered in the study. The chrominance subbands Cb and Cr of the YCbCr colour space are broken down using SPT into many scales and orientation subbands. Each sub band is used to extract texture characteristics using four texture descriptors. The feature vector is created by concatenating the texture features from every subband. By selecting the most discriminating features, the ReliefF technique reduces the high dimensionality of this composite multi-texture representation to a subset. For the purpose of detecting forgeries, the chosen characteristics are input into a Random Forest classifier.

On common datasets, including Columbia, CASIA V1.0 and CASIA V2.0, authors thoroughly evaluated the performance of individual texture descriptors and multi-texture representation. The representation of multi-texture, as compared to just using each descriptor separately, increases detection accuracy, according to experimental data. Additionally, testing results proved that the multi-texture representation's compact representation led to greater detection accuracy.

[6] One of the best techniques for picture tampering detection and image steganalysis has been proven to be the Markov model. Almost all Markov model-based methods for detecting image tampering (in the BDCT or DWT domains) interpret the picture as a 1-D causal signal. As a result, the conventional model only shows state interdependence between nearby states in certain directions. In order to properly represent the 2-D picture and account for additional information, a 2-D noncausal Markov model is presented in this study. Each state in the proposed model concurrently relies on its surrounding states. This model cannot be solved directly analytically, therefore the researchers have divided it into four 2-D causal sub-models and solved them one at a time. The present state for each causal sub-model is dependent on its adjacent states, often known as a Markovian property for 2-D signals. The state transition probability matrix, state parameters, and prior probabilities of each state all contribute to the description of these causal sub-models. All of these model parameters are viewed as classification features with discriminative properties. The suggested model was tested in both the BDCT and DMWT domains, and it has proven its generalisation and effectiveness in both the domains. The suggested noncausal Markov model outperforms various other existing techniques, according to the results.

[7] On the basis of SIFT features, a unique approach for supporting picture forensics investigation has been put out. It is capable of accurately identifying the geometric transformation used to carry out such tampering and determining if a specific region has been replicated, given a suspect photo. With regard to a variety of operational scenarios, such as composite processing and multiple cloning, the given approach demonstrates effectiveness. The main goal of the research was to figure out how to improve the detection phase in the case of a cloned picture patch with a very uniform texture in which prominent key-points are not recovered by SIFT-like approaches. Future research will integrate with other forensics methods used locally on flat areas. An image segmentation technique can also be used to prolong the clustering phase.

[8] In this research, an image splicing detection approach based on SVD is implemented and tested. SVD was used to extract features from an image dataset in the spatial domain and DCT. When compared to the separate approaches(SVD and SVD-DCT), the findings showed that the combined approach (SVD + SVD-DCT) gives the highest detection rate. But, because their performance is less than 80%, the total results were unsatisfactory. According to authors, the disparity between steganography and splicing processes is most likely to be responsible.

[9] This work describes a unique fusion-based methodology for detecting image tampering using an adaptive mix of keypoint-based and block-based methods. For each image, the proposed scheme can find an appropriate initial size of regions and split the image into smooth and keypoints areas. The suggested solution detects forgeries from both smooth and non-smooth regions while lowering computation costs by applying distinct algorithms to these two types of regions. The threshold used to identify forgeries in smooth sections has a significant impact on the results.

Proposed Model:

The fundamental concept behind this approach is to combine the features extracted from Thepade's SBTC and Bernsen thresholding technique to form a feature vector and then investigate its behaviour in relation to various Machine learning algorithms and their ensembles. Subsections A and B elaborate Thepade's SBTC and Bernsen thresholding technique respectively.

A. Thepade's Sorted Block Truncation Code (SBTC) Technique:

This global feature extraction technique takes images as input. The R, G, B colour channels are extracted from the input image for each pixel and flattened to a one dimensional array. This array is then sorted in ascending order. To generate the resultant N-ary feature vectors, (here in our studies, we will assume $N \in \{2,\ldots,10\}$), split the obtained array in approximately equal N parts. Later to it, N vectors for each channel [$R_1, R_2, \ldots, R_N; G_1, G_2, \ldots, G_N; B_1, B_2, \ldots, B_N$] are generated by calculating the mean of each of these N parts.

Let us assume that the size of input image is "w×h" pixels. Hence, the size of the flattened and sorted 1-D array will be "w*h". So, for w*h values and N-ary, the previously formed 1-D array will be split into N different arrays, each of size "(w*h)/N", and averages of each of these N arrays will form the feature vectors. This can be generalized in formulae as follows:

$$R_i = \frac{N}{(w \times h)} \sum_{\frac{((i-1)\times w\times h)}{N}+1}^{\frac{(i\times w\times h)}{N}} sortedRED$$

$$G_i = \frac{N}{(w \times h)} \sum_{\frac{((i-1)\times w\times h)}{N}+1}^{\frac{(i\times w\times h)}{N}} sortedGREEN$$

$$B_i = \frac{N}{(w \times h)} \sum_{\frac{((i-1)\times w\times h)}{N}+1}^{\frac{(i\times w\times h)}{N}} sortedBLUE$$

B. Bernsen Local Thresholding Technique[10]:

This localized method specifies a dynamic threshold for each pixel based on the minimum and maximum intensities in the neighbourhood surrounding the pixel. The threshold is derived by calculating the minimum and maximum values in a w×w neighbourhood. The threshold value is then simply calculated as the average of these two values, as follows:

$$th = \frac{minN + maxN}{2}$$

Parameters used:

$minN$ = minimum intensity in neighbourhood
$maxN$ = maximum intensity in neighbourhood

The value is used as long as the local contrast is above a predefined limit, c_{min}. Local contrast (l_c) is defined as $l_c = (maxN - minN)$. If $l_c < c_{min}$, then the pixel is assumed to belong to a single class and are by default set to the background.

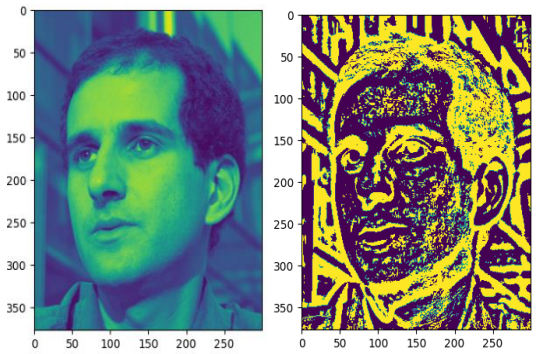


Figure 1: Implementation of Bernsen Thresholding method to produce a segmented image. The image on right is the input grayscale image while one on the left is segmented. (w=7 and c_{min} = 100)

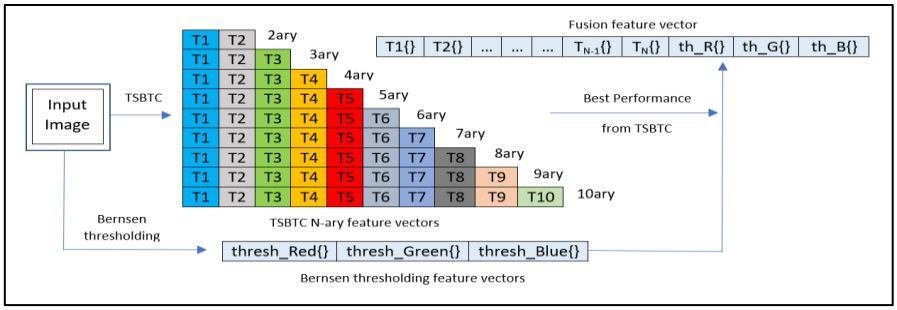


Figure 2: Training Phase of Proposed Model

EXPERIMENTATION ENVIRONMENT

A. Machine learning algorithms:

A classifier in machine learning is an algorithm that automatically orders or categorizes data into one or more of a set of "classes". The classifiers used in this paper to study the feature vectors are as follows:

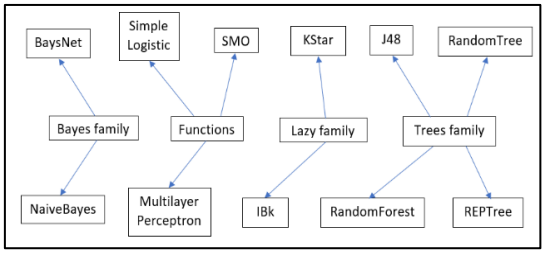


Figure 3: Individual classifiers used for training

B. Ensembles:

Ensemble methods are a type of machine learning technique that integrates multiple base models to create a single optimal prediction model. The ensembles used in this paper to study the feature vectors are as follows:

Sr. No.	Ensembles
1	RandomForest(RF) + RandomTree(RT) + Multilayer Perceptron(MP)
2	RandomForest(RF) + RandomTree(RT) + REPTree
3	IBk + Multilayer Perceptron(MP) + RandomForest(RF)
4	RandomForest(RF) + RandomTree(RT) + IBk
5	Random Forest(RF) + Random Tree (RT)+ IBk + KStar + J48

TABLE I: LIST OF ENSEMBLES USED FOR ANALYSIS

C. Datasets:

The architecture is tested using the WEKA (Waikato Environment for Knowledge Analysis) tool on following 2 datasets:

1) *MICC-F220*
2) *MICC-F2000*

Dataset	Composition	Sizes of Images	Size of Tampered Region
MICC-F220 [17]	It comprises of 220 pictures divided into 110 spliced pictures and 110 original pictures.	Between 722 × 480 and 800 × 600 pixels	The region accounts for 1.2% of the whole picture.

TABLE II: INFORMATION OF DATASET MICC F220

Dataset	Composition	Sizes of Images	Size of Tampered Region
MICC-F2000 [17]	It comprises of 2000 pictures divided into 700 spliced pictures and 1300 original pictures.	2048 × 1536 pixels	The tampered region accounts for 1.12% of the whole image.

TABLE III: INFORMATION OF DATASET MICC F2000

Figure 4(a): Samples from MICC-F220 Dataset. The left one is original while the right one is tampered.

Figure 4(b): Samples from MICC-F220 Dataset. The left one is original while the right one is tampered.

Figure 5(a): Samples from MICC-F2000 Dataset. The left one is original while the right one is tampered.

Figure 5(b): Samples from MICC-F2000 Dataset. The left one is original while the right one is tampered.

D. Evaluation Metrics:

The analysis is based on the performance metrics which consists of accuracy (in percentage) and the weighted F-Score.

1) Accuracy:

Accuracy is a useful measurement for evaluating classifier performance on any dataset. It is defined as the percentage of accurate classification made by our algorithm.

$$Accuracy = \frac{Number\ of\ correct\ classification}{Total\ number\ of\ instances}$$

If classification is to be performed within two classes only, i.e., for binary categorization(here, original and tampered), accuracy can also be expressed as:

$$Accuracy = \frac{t_p + t_n}{t_p + t_n + f_p + f_n}$$

where, t_p is number of True Positives, t_n the number of True Negatives, f_p the number of False Positives and f_n the number of False Negatives.

(t_p+t_n) denotes the total number of correctly classified instances, while (f_p+f_n) denotes the total number of incorrectly classified instances.

2) Weighted F-Measure:

Precision and Recall are used to construct the F-Score (also known as the F-Measure). The computation looks like this:

$$Precision = \frac{t_p}{t_p + f_p}$$

$$Recall = \frac{t_p}{t_p + f_n}$$

$$F - Score = \frac{2 * Precision * Recall}{Precision + Recall}$$

Precision is the ratio of instances correctly classified as positive out of all the instances the algorithm classified as positive, while recall is the defined as the fraction of instances correctly categorised as positive out of all the positive instances. A weighted average of the f-scores from each category, weighted by the proportion of number of instances in each of the category, results in the weighted f-score.

Results and Discussions:

The testing process entails examining the performance metrics generated by the different techniques outlined in Section 3, for each dataset, individually. Later, we shall demonstrate that the proposed fusion approach produces superior outcomes.

1) Analysis on MICC-F220:

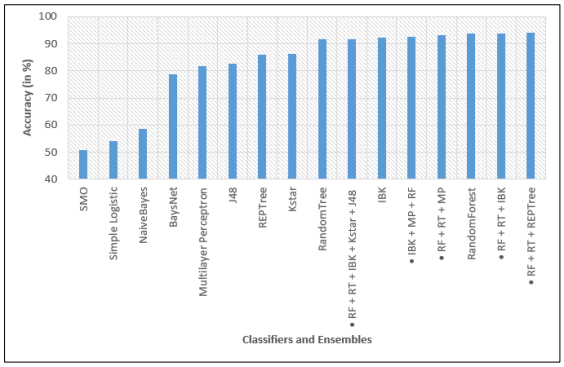
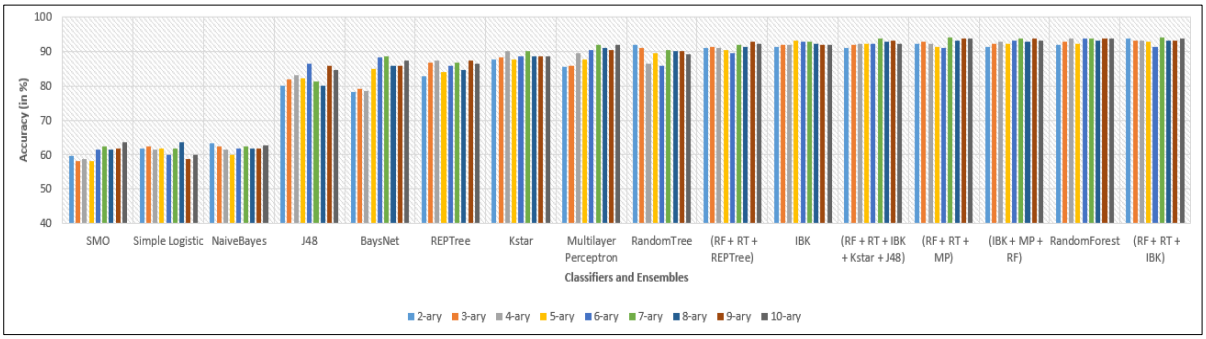


Figure 6: Comparison of Accuracies for different classifiers and ensembles for MICC-F220 using Bernsen Thresholding.

The accuracy-based comparative evaluation using 11 classifiers viz. SMO, Simple Logistic, NaiveBayes, BaysNet, Multilayer Perceptron, J48, REPTree, KStar, RandomTree, IBk, RandomForest and 5 ensembles(as mentioned in Section 4.B) was performed on MICC-F220 dataset using the Weka tool, after applying both techniques(Bernsen thresholding and TSBTC N-ary) individually. Figure 6 and 7 depicts the results for Bernsen thresholding and TSBTC N-ary techniques respectively.
For single classifiers, RandomForest gives same maximum accuracy in both the techniques, which is 93.6364%. Ensemble – (RP+RT+REPTree) gives overall maximum accuracy for Bernsen thresholding technique i.e., 94.0909%. Both the ensembles – (RF+RT+IBk) and (RF+RT+MP) also give overall maximum accuracy of 94.0909% for TSBTC N-ary technique.

The F-Measure was also examined separately for both procedures, and it revealed the same trend as accuracy. When individual classifiers were trained on MICC-F220, RandomForest achieved the highest F-Score of 0.936 for both Bernsen thresholding and the TSBTC N-ary approaches . Ensemble - (RP+RT+REPTree) yields the highest overall F-Score for the Bernsen thresholding approach, 0.941. Both ensembles (RF+RT+IBk) and (RF+RT+MP) provide the same maximum F-Score of 0.941 for the TSBTC 7-ary vector also.

Figure 8 represents the performance appraise of feature level fusion of local features of Bernsen thresholding and global features of TSBTC 7-ary for considered classifiers and ensembles. The findings show that the proposed



methodology of fusion gives highest accuracy of 94.5455% for both the single classifier – RandomForest and

Figure 7: Comparison between accuracies obtained from various different classifiers and ensembles on MICC-F220 using TSBTC N-ary feature vectors.

ensemble – (RF+RT+MP) on MICC-F220. Similarly, analysis of Figure 9 shows that F-Measure for proposed methodology was also highest i.e., 0.945 for both the single classifier – RandomForest and ensemble – (RF+RT+MP) on MICC-F220.

1) Analysis on MICC-F2000:

Similar analysis was also performed on MICC-F2000 dataset, using 10 classifiers viz. NaiveBayes, Simple Logistic, Multilayer Perceptron, BaysNet, REPTree, J48, KStar, RandomTree, IBk, RandomForest and 5 ensembles (as mentioned in Section 4.B).

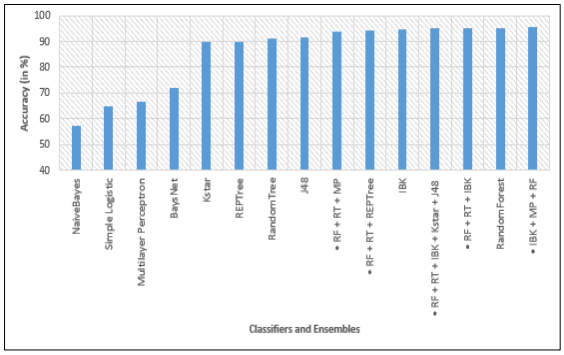
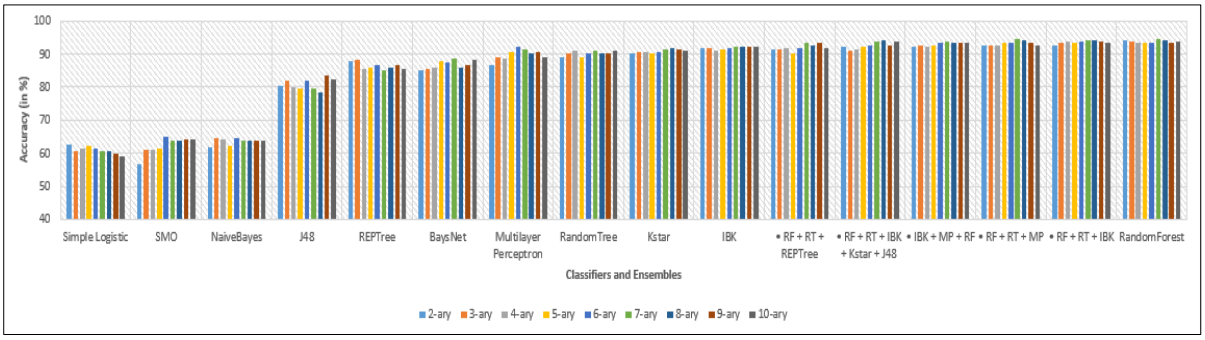


Figure 10: Comparison of Accuracies for different classifiers and ensembles for MICC-F2000 using Bernsen Thresholding.

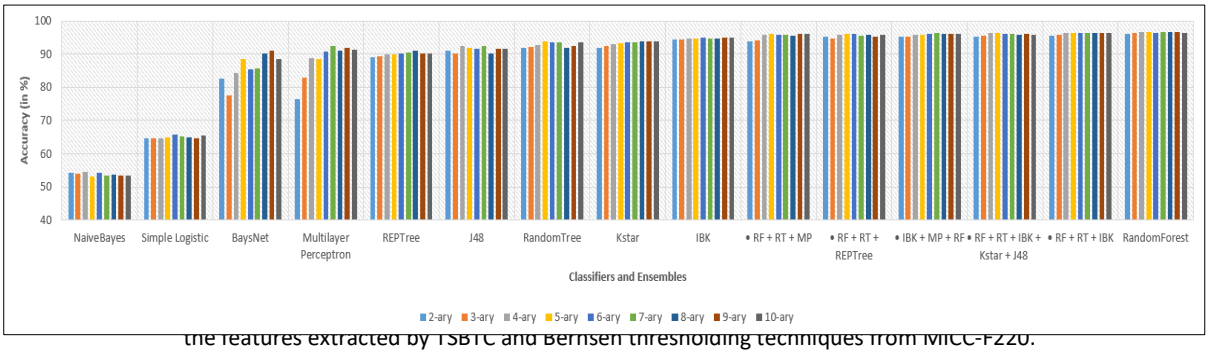
that in single classifiers, RandomForest gives highest accuracy of 95.2%, while ensemble (IBk+MP+RF) gives increased accuracy of 95.4%.

Figure 11 represents the accuracies obtained from TSBTC N-ary feature vectors for single classifiers as well as ensembles. Here, single classifier – RandomForest was found to give higher accuracy than any ensemble used for studies. Ensemble (RF+RT+IBk) gave accuracy of 96.55%, while RandomForest yielded 96.75% accuracy.

Bernsen local thresholding technique gave highest F-Measure of 0.952 for RandomForest and 0.954 for ensemble (IBk+MP+RF). For TSBTC 9-ary, Ensemble (RF+RT+IBk) gave F-score of 0.966 while TSBTC 8-ary and 9-ary



both gave highest F-scores of 0.968 for individual classifier RandomForest.



the features extracted by TSBTC and Bernsen thresholding techniques from MICC-F220.

Figures 12 and 13 depicts the performance appraise of feature level fusion of local features extracted using Bernsen thresholding technique and global features extracted using the TSBTC N-ary technique. It was observed that a single classifier, RandomForest, consistently outperformed every ensemble under consideration. RandomForest gave an increased accuracy of 96.85% and f-score of 0.969 for proposed method on dataset MICC-2000

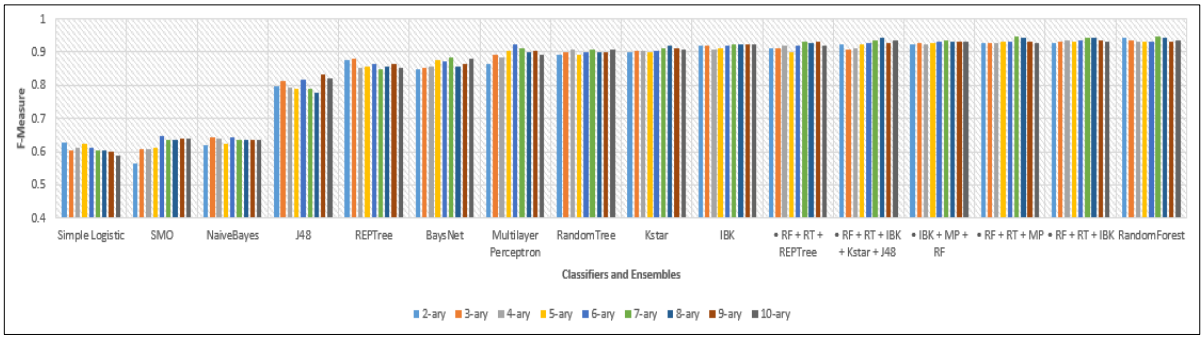


Figure 12: Comparison of percentage accuracy for various classifiers and ensembles trained on feature vector generated by fusing the features extracted by TSBTC and Bernsen thresholding techniques from MICC-F2000.

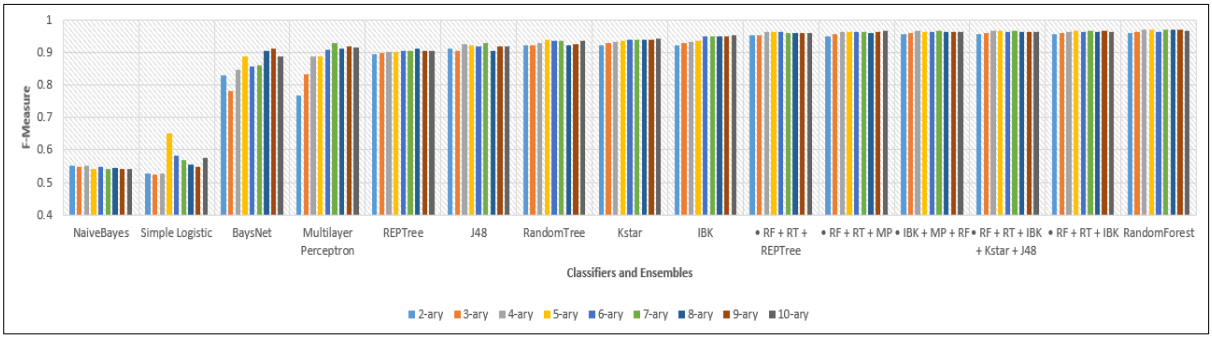


Figure 13: Comparison of F-Measures for various classifiers and ensembles trained on feature vector generated by fusing the features extracted by TSBTC and Bernsen thresholding techniques from MICC-F2000.

Conclusion:

With the rapid advancement of cutting-edge image modification technologies, the creation of counterfeit visuals that are imperceptible to the unaided human eye has become an increasingly prevalent concern. Therefore, there is an urgent need for the development of a technique capable of swiftly and accurately identifying concealed forgeries within an image.

In response to this imperative, this paper introduces a novel approach that leverages the fusion of features extracted through two distinct methods: Bernsen thresholding and the TSBTC N-ary technique. This innovative methodology is designed to significantly enhance the detectability of tampered images, thereby addressing the burgeoning challenge of image authenticity verification.

The essence of this research lies in the synergistic application of Bernsen thresholding and the TSBTC N-ary techniques, both of which contribute their unique strengths to the overall objective of improved forgery detection. By combining these approaches, the proposed methodology has exhibited superior performance in rigorous testing scenarios, particularly when assessed against established and conventional methods.

In concrete terms, this approach has demonstrated its efficacy and potential on diverse datasets, including but not limited to MICC-F220 and MICC-F2000. The comparative analysis against traditional methods underscores the distinctive advantages of the newly proposed technique in terms of precision and speed when identifying concealed image manipulations.

Figures 14 and 15 illustrate the improved efficiency of performance metrics consisting of accuracy and F-Measure:

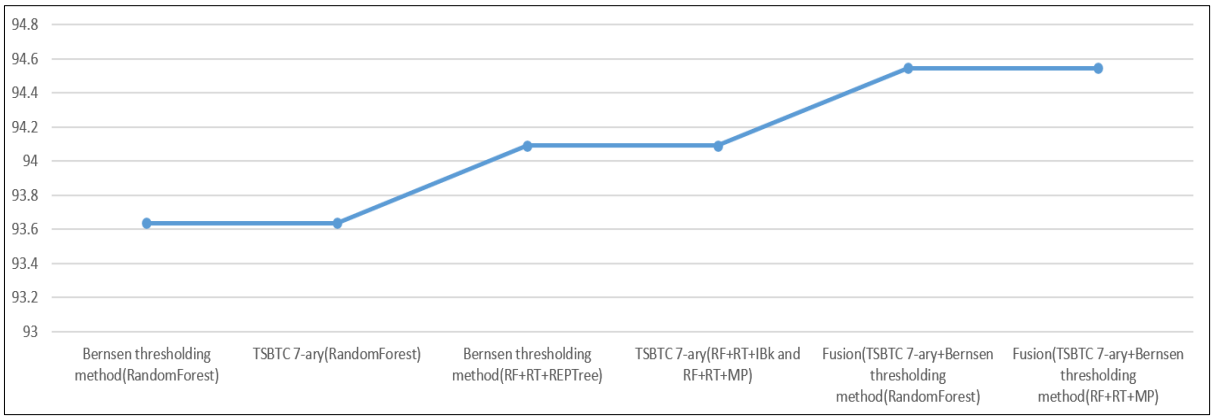


Figure 14: Demonstration of better results being yielded from the proposed model than the traditional individual methods on dataset MICC-F220. Fusion (TSBTC 7-ary + Bernsen thresholding method) trained on ensemble (RandomForest + RandomTree + Multilayer Perceptron) yields 94.5455% accuracy.

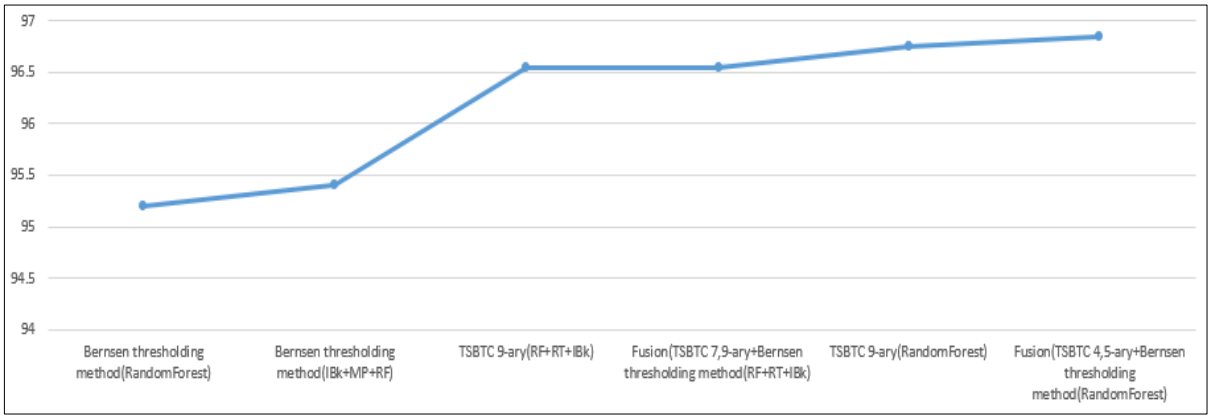


Figure 15: Demonstration of better results being yielded from the proposed model than the traditional individual methods on dataset MICC-F2000. Fusion (TSBTC 4/5-ary + Bernsen thresholding method) trained on classifier - RandomForest yields 96.85% accuracy.

The proposed method was trained using various machine learning classifiers and their ensembles in WEKA tool. For MICC-F220, overall best performance was attained by Fusion of TSBTC 7-ary vector and the vectors obtained from Bernsen thresholding, 94.5455%. While F-Measure for same was found to be 0.945, which was again the highest. For MICC-F2000, overall best performance was attained by Fusion of TSBTC 4/5-ary vector and the vectors obtained from Bernsen thresholding, 96.85%. Similarly, F-Measure was found to be 0.969, which was again the highest.

Further combinations of fusing various other methods for improving the detection of spliced images would be interesting to study and are left for future work.

References:

[1] A. A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad and G. Bebis, "Splicing image forgery detection based on DCT and Local Binary Pattern," 2013 IEEE Global Conference on Signal and Information Processing, 2013, pp. 253-256, doi: 10.1109/GlobalSIP.2013.6736863.

[2] Zhongwei He, Wei Lu, Wei Sun, Jiwu Huang, Digital image splicing detection based on Markov features in DCT and DWT domain, Pattern Recognition, Volume 45, Issue 12, 2012, Pages 4292-4299, ISSN 0031-3203,
https://doi.org/10.1016/j.patcog.2012.05.014

[3] Rao, Y., & Ni, J. (2016). A deep learning approach to detection of splicing and copy-move forgeries in images. *2016 IEEE International Workshop on Information Forensics and Security (WIFS)*, 1-6.

[4] Bunk, J., Bappy, J. H., Mohammed, T. M., Nataraj, L., Flenner, A., Manjunath, B. S., ... & Peterson, L. (2017, July). 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).

[5] Vidyadharan, Divya & Thampi, Sabu. (2017). Digital image forgery detection using compact multi-texture representation. Journal of Intelligent & Fuzzy Systems. 32. 3177-3188. 10.3233/JIFS-169261.

[6] Xudong Zhao, Shilin Wang, Shenghong Li, and Jianhua Li. 2015. Passive Image-Splicing Detection by a 2-D Noncausal Markov Model. IEEE Trans. Cir. and Sys. for Video Technol. 25, 2 (Feb. 2015), 185–199. https://doi.org/10.1109/TCSVT.2014.2347513

[7] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo and G. Serra, "A SIFT-Based Forensic Method for Copy–Move Attack Detection and Transformation Recovery," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 3, pp. 1099-1110, Sept. 2011, doi: 10.1109/TIFS.2011.2129512.

[8] Moghaddasi, Zahra & Jalab, Hamid & Md. Noor, Rafidah. (2014). SVD-based image splicing detection. 27-30. 10.1109/ICIMU.2014.7066598.

[9] J. Zheng, Y. Liu, J. Ren, T. Zhu, Y. Yan, and H. Yang, “Fusion of block and keypoints based approaches for effective copy-move image forgery detection,” Multidimensional Systems and Signal Processing, pp. 1-17, 2016

[10] Bernsen, J.: ‘Dynamic thresholding of gray-level images’. Proc. 8th Int. Conf. on Pattern Recognition, Paris, 1986, pp. 1251–1255

[11] Badre, S. R., and S. D. Thepade. 2016. Novel video content summarization using thepade’s sorted n-ary block truncation coding. Procedia Computer Science-79:474–82. doi:10.1016/j.procs.2016.03.061.

[12] Bhondve, R. K., S. D. Thepade, and R. Mathews. 2015. Performance assessment of color spaces in multimodal biometric identification with Iris and palmprint using Thepade’s sorted ternary block truncation coding. International Journal of Integrated Computer Applications and Research (IJICAR). rb.gy/e89wlp

[13] Thepade, S., R. Das, and S. Ghosh. 2015. Novel technique in block truncation coding based feature extraction for content based image identification. Transactions on Computational Science XXV:55–76.

[14] Thepade, S. D., S. Sange, R. Das, and S. Luniya. 2018. Enhanced image classification with feature level fusion of niblack thresholding and Thepade's sorted N-ary block truncation coding using ensemble of machine learning algorithms. IEEE Punecon, Pune, India.

[15] Thepade, S. D., and Y. Bafna. 2018. Improving the performance of machine learning classifiers for image category identification using feature level fusion of otsu segmentation augmented with Thepade's N-ary sorted block truncation coding. 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), Pune, India

[16] Thepade, S., and S. Badre. 2016. Performance comparison of color spaces in novel video content summarization using thepade's sorted n-ary block truncation coding. International Conference & Workshop on Electronics & Telecommunication Engineering (ICWET 2016), Mumbai, India

[17] I. Amerini, L. Ballan, R. Caldelli, A. Del Bimbo, G. Serra. "A SIFT-based forensic method for copy-move attack detection and transformation recovery", IEEE Transactions on Information Forensics and Security, vol. 6, issue 3, pp. 1099-1110, 2011.