Transactions on Machine Learning and Artificial Intelligence - Vol. 10, No. 5
Publication Date: September, 25, 2022
DOI:10.14738/tmlai.105.13126.
Gornale, S. S., Patil, G., & Benne, R. (2022) Document Image Forgery Detection Using RGB Color Channel. Transactions on Machine Learning and Artificial Intelligence, 10(5). 01-14.

SOCIETY FOR SCIENCE AND EDUCATION

Document Image Forgery Detection Using RGB Color Channel

Shivanand S. Gornale
Department of Computer Science
Rani Channamma University, Belagavi

Gayatri Patil
Department of Computer Science
Rani Channamma University, Belagavi

Rajkumar Benne
Government First Grade College, Bhalki

ABSTRACT

Using advanced digital technologies and photo editing software, document images, such as typed and handwritten documents, can be manipulated in a variety of ways. The most common method of document forgery is adding or removing information. As a result of the changes made to document images, there is misinformation and misbelief in document images. Forgery detection with multiple forgery operations is challenging issue. As a result, special consideration is given in this work to the ten-class problem, in which a text can be altered using multiple forgery types. The characteristics are computed using RGB color components and GLCM texture descriptors. The method is effective for distinguishing between genuine and forged document images. A classification rate of 95.8% for forged handwritten documents and 93.11% for forged printed document images are obtained respectively. The obtained results are promising and competitive with state-of- art techniques reported in the literature.

Keywords: Document forgery, GLCM Features, RGB color Channels, Support Vector Machine, Ten class classification.

INTRODUCTION

As we live in today's digital world, the use of document images in our lives is increasing day by day. Everything is going paperless in today's digital age. However, many important documents are still written on paper like. Certificates, receipts, official documents, property papers and other items are common examples. These documents are insecure because they lack the necessary security features [1]. At the same time the manipulation of these documents also increasing day by day. These document manipulations are known as document tampering, and they are simple to carry out with inexpensive devices such as scanners, printers, using advanced digital technologies and photo editing software. Typically, the document to be manipulated is scanned first, and then the scanned image of the original document is easily manipulated. As a result, typed and handwritten papers' text can be altered. For example, the information of a property document can be manipulated to facilitate an unauthorized transaction, and the date on a flight ticket can be changed to get access to airport terminals

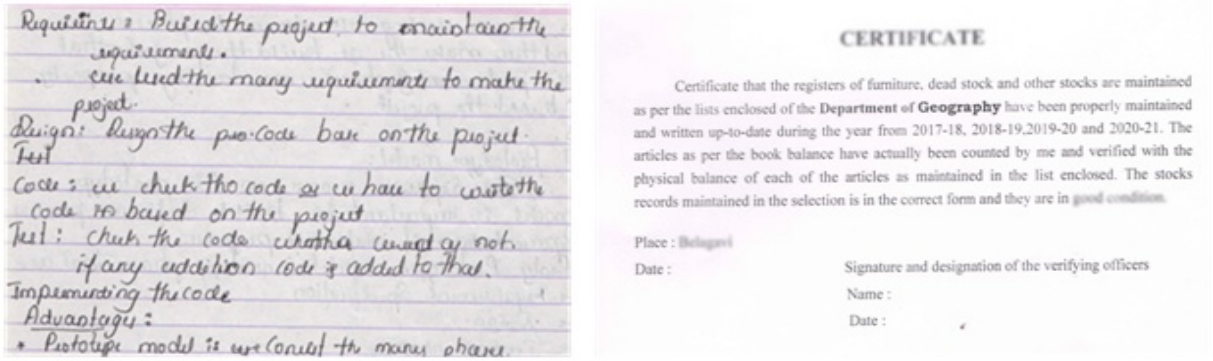
while avoiding security checks. Handwritten documents, such as fake suicide notes, answer scripts, and certificates, are also utilized to generate falsified documents [2]. Hence, digital images are becoming more susceptible to forgery, and trust in digital images has eroded.

Forgeries are a very old problem in human kind. Detection of forged videos and images is not a new topic in computer vision and image processing; yet, it is a new problem in study [3, 4]. In comparison to video and images, however, fraud recognition in document images, including printed and handwritten document images, is relatively recent. [5]. This is due to the fact that document images are frequently used as authenticated proof evidence in judicial system for any crime scene investigation. Furthermore, we, the general public, genuinely think that the information in newspapers and on the internet is truthful and authenticated [6]. If the information of these records is modified, it causes misleading information and sends the wrong message to community. As a result, it is necessary to automatically verify the authenticity and decency of the documents without requiring manual involvement.

In the digital domain, document forensics evolved to eliminate the need for specialized devices and trained personnel to evaluate the authenticity of documents being analyzed. Document forensics technology, which is primarily concerned with identifying the origin of a document or detecting forgery, has improved rapidly in the last decade. To carry out the necessary studies, this technology employs commodity scanners and a computer. The analyses can be performed automatically or semi-automatically, lowering costs while increasing convenience. Even though, document forensics faces significant challenges that limit its growth. Currently, the techniques are limited to textual documents such as handwritten and printed documents [7].

In order to create fake or forged documents, forgers usually use copy-paste and insertion operations to tamper original content. Copy and paste operations [2] involve copying the content from the same or a different document to paste at target words, while in insertion; the words are altered by using software tools, adding characters to appropriate places according to their needs. There are methods to find a solution in the literature [8, 9] if the document comprises forged words with simple operations. In reality, noise, document age, paper quality, ink use in handwriting, and other factors can cause document degradation. When a document contains forged words in contrast to the words affected by the various degradations, the approaches fail to detect the forged words [10, 11].

To address these issues, we have created a forged document dataset. The figure. 1(a) and 1(b) are the examples of forged handwritten and printed document images respectively. On our custom created dataset we use multiple forgery operations to generate forged words. For example, the forged word created by noise operation one can perform copy paste operation, which is called as copy paste + noise class. In the similar way forgery operations are created such as insertion + blur, insertion + noise, copy paste + blur, insertion + copy paste along with simple copy paste, insertion alone, noise and blur alone. Hence this results in 10 different forgery classes as shown in figure. 2.



(a) (b)

Figure. 1 (a). Example of Forged Handwritten Document image and (b). Example of Forged Printed Document image

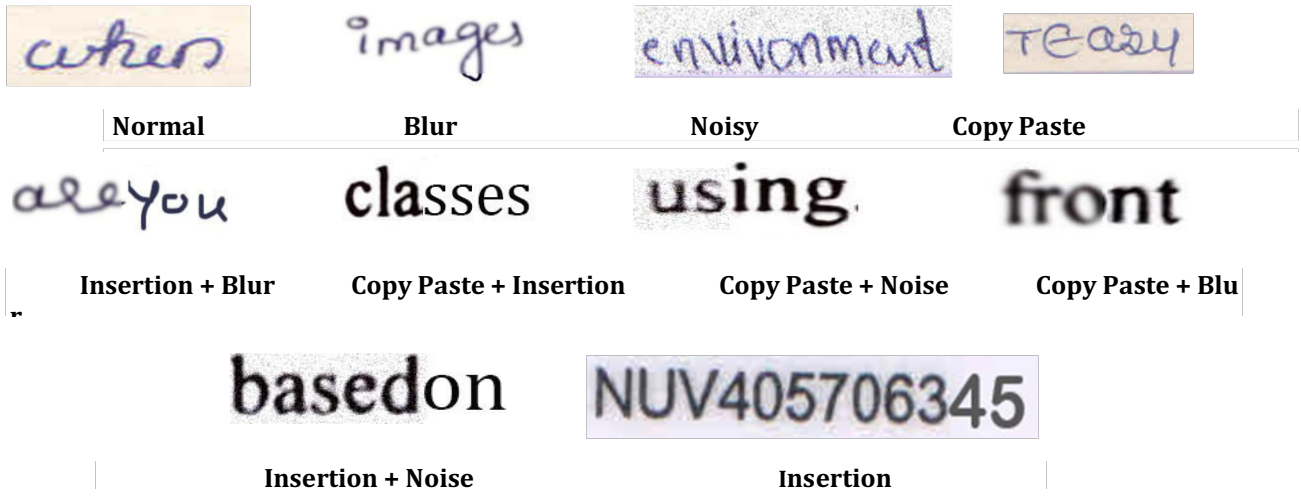


Figure. 2 Example of Ten Different forgery types on handwritten and printed text images.

RELATED WORK

Forgery detection in document images can be performed using a variety of methods and these methods can be classified into two categories: those which are focused on printed document images and those which are focused on handwritten document images. Few researchers address both printed and handwritten images of documents for forgery detection.

Myna et al. [12] (2007) developed a DWT-based image forgery detection approach that first finds the matching blocks before using phase correlation to detect the copied portions. Their technique has a flaw in that it produces very poor results when the duplicated region is significantly rotated or resized. Tsai and Liu [13] (2013) analyzed the Chinese printed source to find the source of printers using different texture feature extraction methods such as gray-level co-occurrence matrix (GLCM) and discrete wavelet transform (DWT). In addition, the authors investigate the best feature subset by employing feature selection techniques and

URL: http://dx.doi.org/10.14738/tmlai.105.13126

employing support vector machine (SVM) to identify the source model of the documents. Bertrand et al. [14] (2013) suggested a method for detecting forgeries in documents based on inherent properties at the character level. Outlier character detection in a discriminant feature space and detection of related characters are the foundations of the suggested method. For each character, a feature set is computed and categorized depending on the distance between characters in the same class. Gorai et al. [15] (2016) undertook handwriting examinations to detect forged documents, handwritten image was divided into three RGB channels, as well as the texture characteristics of the grayscale image, were compared using the histogram matching method. Megahed et al. [16] (2017) proposed an approach for identifying handwritten forgery in text by using computer vision to detect different ink. The features are derived from the red, green, and blue channels. Distance measurements between each pair of feature vectors were also computed using the Root Mean Square Error. Shivakumara et al.'s [17] (2018) proposed a fusion operation and a color space approach for detecting forged IMEI (International Mobile Equipment Identity). An approach based on connected component analysis was used to detect final forged IMEI numbers. Tests were conducted on images of IMEI numbers, but not on images of handwritten text. This may mean that the method is not suitable for detecting counterfeit in handwritten images of text. Khan et al. [18] (2018) introduce a forgery detection system based on fuzzy clustering in document pictures. The proposed features are ineffective for documents with poor quality or that have been tampered with by several processes Kundu et al. [2] (2019) proposed forgery detection method where, Noisy and blurred text were added to the normal images to get forged images. The challenge is a classification problem with four classes. The method uses spectral density and variations as features to distinguish between falsified text classes. Despite the fact that the methods address the issues of noise and blur, their application is limited to images altered by single actions rather than numerous actions. Munish et al [1] (2020) have suggested a classifier-based model for identifying the source printer and categorizing the forged document as belonging to one of the printer classes. The Speeded Up Robust Features, Oriented Fast Rotated, and BRIEF feature descriptors are extracted and classification is done using Naive Bayes, k-NN, random forest, and various combinations of these classifiers have been tested. The proposed model is capable of efficiently classifying the questioned documents into their respective printer class.

It is observed from the preceding work that many researchers study have focused on detecting forgery in printed and handwritten document images, raising the following challenges and issues:

- Forgery detection in low resolution images
- Words altered by multiple forgery operations
- Identification of forged words rather than source printer identification
- Multiple forgery detection in both typed and handwritten document images

To address the above - mentioned challenges and issues, the authors developed a ten-class classification problem in handwritten and printed document images containing text that varies in different writing styles and is affected by multiple forgery operations, as described in section Dataset.

PROPOSED METHODOLOGY

The proposed methodology consist the major steps are preprocessing, dividing the image into blocks, feature extraction and comparing the texture similarity obtained features. The figure .3 represents the graphical flow diagram for the proposed algorithm. The key issue of detecting forgery in both printed and handwritten documents in noise and blur environment is to discovering the distinctive pattern for the forged character. It is true that, one can expect some regular pattern when we perform single or multiple forgery operations on text. The color intensity of inks used in handwriting is not uniform and is affected by a variety of factors [19], including pen pressure, ink type and friction between the pen and the paper. When documents are thoroughly examined and inks for each object are compared, these differences emerge. Taking these observations into consideration, the proposed methodology extract RGB color channels and texture feature to solve the ten-class problem.

Pre-processing

It is necessary to pre-process an image in order to better understand it. This may improve some of the image's key features. In this work, pre-processing is done on a color document image that is resized to 100X100 for proper document analysis.

Feature Extraction

The original and forged document scans are used as input in this study to detect original and forged images. We propose dividing each color input image into R, G, and B components in order to investigate local variations in detail, as this aids in extracting minute changes in the content. We believe that examining local differences in R, G, and B of the input images will aid us in extracting the difference, which shows forgeries produced by certain processes. Gray-Level Co-Occurrence Matrix (GLCM) features such as contrast, homogeneity, and energy are estimated to extract the differences. Exploring R, G, and B color components and extracting GLCM characteristics based on these color channels from input images to discriminate between real and counterfeit document images is the key contribution here.

URL: http://dx.doi.org/10.14738/tmlai.105.13126

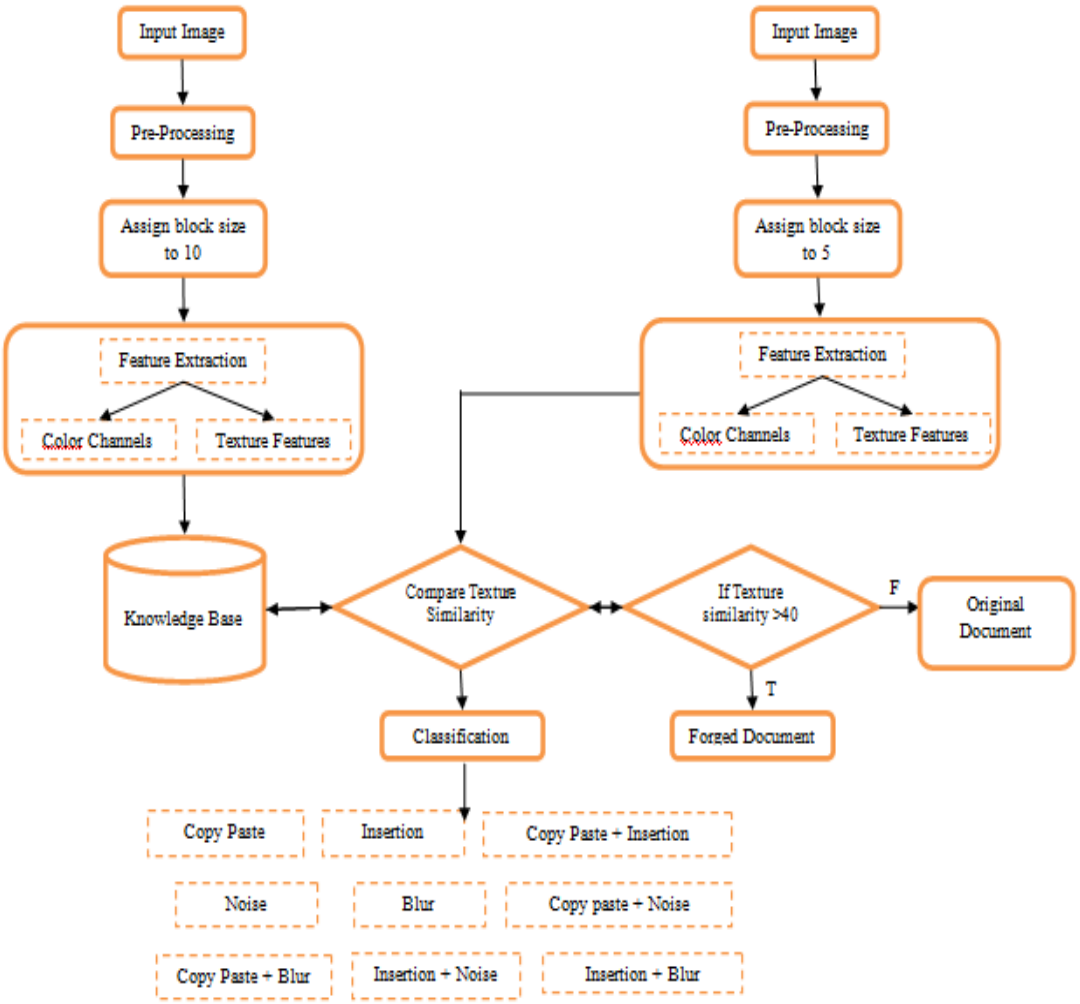


Figure 3. Proposed Block Diagram

We extract nine features for each object in order to identify individual characteristics of words as Feature vector F= {Hr.Hg,Hb, Cr.Cg,Cb, Er.Eg,Eb}. First three features {Hr.Hg,Hb} are computed as Homogeneity of red , green and blue intensity values respectively as represented in eq.(1). The second three features {Cr.Cg,Cb} are computed as contrast of red , green and blue intensity values respectively as represented in eq.(2) and last three features {Er.Eg,Eb} are computed as Energy of red , green and blue intensity values respectively as represented in eq.(3).

Gray-Level Co-Occurrence Matrix (GLCM)

The GLCM algorithm is used to extract the input image's textural information. For obtaining the 2nd order statistics of image textures, GLCM simulations are frequently used. To analyze the GLCMs over a given image region, the frequency of co-occurring intensity correlations is computed. [20]. The GLCM algorithm determines whether a pixel with intensity i occurs horizontally, vertically, or diagonally to a pixel with intensity j [21]. GLCM is most commonly used in analysis of image texture. Homogeneity, energy and contrast are some commonly used statistical values derived from the co-occurrence matrix.

Homogeneity

Inverse difference moment is also called homogeneity. It is used to estimate the image of homogeneity because it acknowledges a significant value for smaller grey tone contrast in pair elements as represented in eq. (1). As a result of the closeness of diagonal components, it is more complicated in the GLCM. If all the components in the image are identical, the value is the highest. The degree of homogeneity decreases if contrast increases while vitality stays constant [22].

Homogeneity H= $\sum i \sum j \frac{1}{1+(i-j)^2} P_{(i,j)}$ (1)

Contrast

Contrast is a GLCM differential moment that is used to assess the spatial frequency of an image as represented in eq.2. An adjacent collection of pixels is measured by their contrast, or the difference between their minimum and maximum values. In simple terms, it's a way to describe the number of local differences among images. The sharpness of the image is reflected in contrast. Contrast plays a major role in how the visual effect is perceived; the higher the contrast, the more clearly the visual impact. [22]

Contrast $C = \sum i \sum j \ (i - j)^2 \ P_{ij}$ (2)

Energy

The Energy Textural Uniformity, or angular second moment, is measured by energy and is defined as pixel pair repetitions as defined in eq.3 [22] The total of the squares of the elements in the GLCM, which can quantify textural regularity, is energy (E).

Enegry $E = \sum i \sum j \ P_{ij}^2$ (3)

Classification

To carry out this experiment, an image dataset of 950 handwritten and printed forged documents were used. The documents were classified into ten classes: Copy Paste, Copy Paste + Insertion, Copy Paste+ Noise, Copy Paste +Blur, Insertion, Insertion + Noise, Insertion + Blur, Blur, Noise and Normal. The feature vector is computed by extracting RGB color component based GLCM texture features such as Homogeneity, Contrast and Energy. This feature vector is considered as a single feature vector to classify different forgery operations. The experiment utilized a variety of classification techniques, however the findings were insufficient. Hence the classification is carried out using Support Vector Machine (SVM) for better results and to improve the accuracy rate.

Support Vector Machine (SVM)

SVM is primarily used in classification. It employs high-dimensional recognition methods to prevent computational complexity. SVM classification is primarily based on the concept of decision making, which defines the decision boundaries. A decision plane distinguishes between a group of objects with different class memberships and a group of objects with different class relationships. SVM generates a set of vectors known as "support vectors" that easily identify separators, allowing for a wide separation of classes and objects [23]. To classify the original and forgery detection, the Multi-Class Vector Machine (MC-SVM) classifier is used. The MC-SVM classifier also improves the detection of forgery. The classification of image frames is performed using test and training values [24].

URL: http://dx.doi.org/10.14738/tmlai.105.13126

The algorithm for proposed method is given as follows

Input: Forged Handwritten/Printed Document Image
Output: Identification and Classification of handwritten/Printed Forged Document Image.

Algorithm1: Document Feature Extraction

Step1: Read the document
Step2: Resize the document to 100x100
Step3: Assign the block size to 10
Step4: Extract the color and texture features [R, G, B Channel & Contrast, Homogeneity and Energy Texture Features]
Step4: Store it to Knowledge base

Algorithm2: Document Checking

Step1: Read the document
Step2: Resize the document to 100x100
Step3: Assign the block size to 5
Step4: Examine the texture similarity with knowledge base
Step5: If Texture Similarity > 40 then
Display ('Forged Document');
Else
Display ('Original Document');
Step6: Classification of Obtained Features using SVM classifier.
Step7: Stop

IMPLEMENTATION RESULTS

The experiment is carried out on our custom created dataset which consist of 950 forged document images (500 forged handwritten and 450 forged printed document images) of 10 different classes multiple forgery operation. The detail description about the dataset is discussed in dataset section. Using digital image processing techniques, a unique method for detecting fraudulent documents is provided. The source of data is a scanned document. The input image is then divided using the block size, and nine features based on RGB color components are retrieved for each block of image. Three GLCM features were computed for each color channel: contrast, homogeneity, and energy. The computed features were added to the knowledge base, and the default threshold value to 40 has been set throughout the testing phase when comparing the features. If the texture similarity is more than the given threshold value, the document image is classified as forged, otherwise it is considered to as original.

Dataset

From the literature review it has been found that the standard datasets available include images with minimal forgery actions such as noise, blur, copy paste, and insertion, but they do not comprise handwritten or printed documents with multiple forgery actions. To address the issue, a new custom dataset containing 950 forged document images that consist of 500 handwritten document images and 450 printed document images with10 different forgery classes is created such as: Normal, Copy Paste, Noise, Blur, insertion, Insertion + Blur, Insertion + Noise, Copy Paste + Blur, Copy Paste + Noise and Copy Paste + Insertion. Initially, the handwritten and printed documents were scanned using LajerJet M1136 MFP scanner with 200 dpi and then forgery operation is performed on each single image as described in Table 1. Each

class of forged handwritten document images consist of 50 images and each class of forged printed document image consist of 45 images.

The detailed description of 10 different classes discussed in Table 1. The table gives a detailed idea about single and multiple forgery operations. The single forgery operations such as copy paste, insertion, noise and blur affects the whole word. Whereas, the multiple forgery operation performed on text results in half portion of word is affected by one forgery operation and rest half portion is affected by another forgery operation. From figure.2. single and multiple forgery operations performed on text can be noticeable.

Table 1. Ten Class Problems

Forgery Type	**Description**
Class 1: Normal Words	Original words
Class 2: Copy- Paste	Words forged by copy-paste operation
Class 3: Noise	Creating Forged words by adding noise to the normal words
Class 4: Blur	Creating forged words by adding blur to the normal words
Class 5: Insertion	Create forged words by inserting characters.
Class 6: Insertion + Blur	Creating forged words by insertion and blur operation
Class 7: Insertion +Noise	Creating forged words by insertion and noise operation
Class8: Copy-Paste + Blur	Creating forged words by copy paste and blur operations
Class 9: Copy Paste+ Noise	Creating forged words by copy paste and noise operations
Class10:CopyPaste+Insertion	Creating forged words by copy paste and insertion operations

Table 2 and Table 3 report the quantitative classification results of the proposed method based on RGB Color channels and texture features extracted from forged handwritten and forged printed documents images using SVM classifier. Tables 2 and 3 show that values found diagonally in the table are deemed accurate categorization, but values found off-diagonally are considered misclassification.

URL: http://dx.doi.org/10.14738/tmlai.105.13126

Table 2. Confusion Matrix for Proposed Method on Forged Handwritten Document Images Using SVM Classifier

	BLUR	CP	NRM	CP+BLR	CP+INS	CP+NS	INS+BLR	INS	INS+NS	NOISE
BLUR	**49**	0	0	0	0	0	0	0	0	1
CP	0	**48**	1	0	0	0	0	0	0	0
NRM	0	1	**49**	0	0	0	2	1	1	0
CP+BLR	0	0	0	**50**	0	1	0	0	1	0
CP+INS	1	0	0	0	**47**	0	2	0	0	0
CP+NS	0	0	0	0	1	**49**	0	1	0	1
INS+BLR	0	1	0	0	0	0	**45**	0	0	0
INS	0	0	0	0	0	0	0	**47**	0	1
INS+NS	0	0	0	0	0	0	1	0	**48**	0
NOISE	0	0	0	0	2	0	0	1	0	**47**

Table 3. Confusion Matrix for Proposed Method on Forged Printed Document Images Using SVM Classifier

	BLUR	NRM	CP	INS+BLR	CP+BLR	CP+INS	CP+NS	INS	INS+NS	NOISE
BLUR	**44**	0	2	0	0	0	0	1	1	0
NRM	0	**44**	0	0	0	0	0	1	0	0
CP	0	0	**38**	0	0	0	0	0	0	0
INS+BLR	0	1	0	**43**	2	0	2	0	0	0
CP+BLR	0	0	2	0	**42**	1	0	1	0	0
CP+INS	1	0	1	0	0	**44**	0	2	1	0
CP+NS	0	0	1	1	0	0	**41**	0	0	2
INS	0	0	1	0	1	0	0	**37**	0	0
INS+NS	0	0	0	0	0	0	0	2	**43**	0
NOISE	0	0	0	1	0	0	2	1	0	**43**

The class Abbreviations used in Table 2 and table 3 are: BLUR: Blur, CP+NS: Copy Pate + Noise, INS+NS: Insertion + Noise, NOISE: Noise, CP+BLR: Copy Paste + Blur, NRM: Normal, CP: Copy Paste, CP+INS: Copy Paste + Insertion, INS+BLUR: Insertion + Blur, INS: Insertion.

Table 4 shows the accuracy rate of GLCM texture features based on RGB color channels on forged handwritten and printed document images using Support Vector Machine Classifier, which is 95.8% and 93.11%, respectively. The performance of proposed methodology is evaluated in terms of metrics, such as Precision, F_Score, Recall, and Accuracy as represented in eq. (4) to eq. (7) respectively. The figure.4 represents the graphical representation of classification performance of RGB channel based GLCM texture features.

$$Precision = \frac{TruePositive}{TruePositive+FalsePositive} \quad (4)$$

$$F_Score = \frac{2*Precision*Recall}{Precision+Recall} \quad (5)$$

$$Recall = \frac{TruePositive}{TruePositive+FalseNegative} * 100 \quad (6)$$

$$Accuracy = \frac{Total\ No.of\ correctly\ classified\ images}{total\ no.of\ test\ images}\ X\ 100 \quad (7)$$

Table 4. The performance analysis of feature set on Forged handwritten and Printed Document images (in %).

FEATURE SET	CLASSIFIER	FORGED HANDWRITTEN DOCUMENTS				FORGED PRINTED DOCUMENTS			
		Precision	Recall	F-Score	Accuracy	Precision	Recall	F-Score	Accuracy
GLCM texture feature based on RGB channels	SVM	0.9502	0.9621	0.9678	**95.8%**	0.9343	0.9487	0.9291	**93.11%**

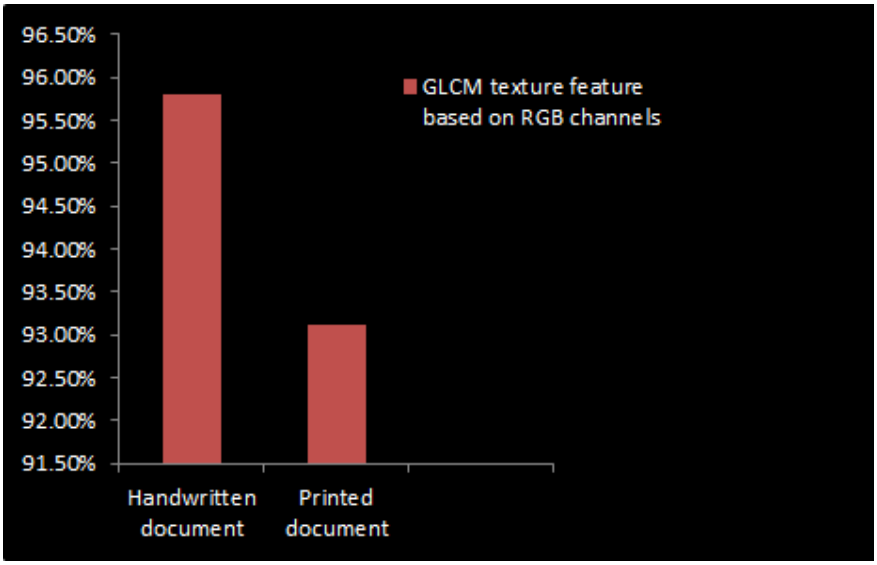


Figure. 4. Graphical representation of classification performance

Statistical test of significance

To determine whether or not the experimental outcomes are statistically significant, a statistical test of significance is performed. It is a method of comparing obtained results to a predetermined data assertion. At a significance level of 5%, the Chi-Square Test is utilized to validate the statistical inference in this study.

A chi-square statistic is a calculation that compares a model to actual data. The following are the null hypothesis, alternative hypothesis, and degrees of freedom in this test:

- **Null Hypothesis (H_0):** The proposed methodology's conclusions and the overall number of forged document images have a strong correlation.
- **Alternative Hypothesis (H_1):** The proposed methodology's conclusions have no strong correlation with the overall quantity of forged document images.
- **Degree of Freedom (df)** =9, the critical value of χ^2 with df=9 at a 5% significance level is 16.92. (Taken from the chi-square table.)

URL: http://dx.doi.org/10.14738/tmlai.105.13126

If χ^2<16.92, Accept H_0 and Reject H_1, else vice versa

The performance evaluation of Chi-Square examination on total forged document images and proposed method for classification are shown in Table 5. Chi-Square Statistics are computed using Eq. (8).

$$\text{Chi} - \text{Square}\ (x^2) = \sum \frac{(O_o - E_e)^2}{E_e} = 3.337 \qquad (8)$$

The determined value of the Chi Square statistic is less than the critical value from the chi square table. As a result, the Null Hypothesis H_0 is accepted and the alternative hypothesis H_1 is rejected. It demonstrates that the proposed method and the observations provided by the total number of forged document images have a significant relationship

Table 5. Chi-Square Test Performance Analysis on Total Forged Document Images and Proposed Classification

FORGERY TYPES	FORGED DOCUMENTS TI	PROPOSED METHOD PI	TOTAL (TI + PI)	EXPECTED VALUES (EE)	OBSERVED VALUES (OO)	$x^2 = \sum \frac{(O_o - E_e)^2}{E_e}$
Blur	95	93	188	96	91	0.260
CopyPaste	95	93	188	96	91	0.260
Normal	95	86	181	93	87	0.387
CopyPaste+Blur	95	92	187	96	90	0.375
CopyPaste+Insertion	95	91	186	95	90	0.263
CopyPaste+Noise	95	90	185	95	89	0.378
Insertion+Blur	95	88	183	94	88	0.382
Insertion	95	84	179	92	86	0.391
Insertion+Noise	95	91	186	95	90	0.263
Noise	95	90	185	95	89	0.378
Total	∑Ti = 950	∑Pi =898	$\sum(T_i + P_i) = \mathbf{1848}$			x^2=3.337

CONCLUSION

We suggested a method for detecting and classifying forged handwritten and printed document images in this study. The proposed method investigates the extraction of RGB Color channel based GLCM texture features from document images containing words affected by ten different types of forgery operations. Document images are very vulnerable to undesirable distortions created by scanners while scanning papers, as well as forgery-related distortion, which can overlap with distortion in normal images and reduce image quality. The authors used methodologies that provide an effective strategy for better understanding and analyzing handwritten and printed document images to address these challenges. The method achieves an accuracy rate of 95.8% on forged handwritten document images and 93.11% on forged printed document images when using the Support vector machine classifier.

ACKNOWLEDGEMENT

We would like to express our gratitude to all students at Rani Channamma University, Belagavi, Karnataka, India, who provided us with samples of handwritten and printed documents as part of this research.

References

1. Kumar, M., Gupta, S., and Mohan, N." A computational approach for printed document forensics using SURF and ORB features". Soft Computing. A Fusion of Foundations, Methodologies and Applications, Springer doi:10.1007/s00500-020-04733-x ,2020
2. S. Kundu, P. Shivakumara, A. Grouver, U. Pal, T. Lu and M. Blumenstein," A New Forged Handwriting Detection Method Based on Fourier Spectral Density and Variation", In Proc. Of Autorité de contrôle prudentiel et de résolution (ACPR) pp 136-150, 2019
3. L. Su, C. Li, Y. Lai and J. Yang, "A Fast Forgery Detection Algorithm Based on Exponential-Fourier Moments for Video Region Duplication," in IEEE Transactions on Multimedia, vol. 20, no. 4, pp. 825-840, doi: 10.1109/TMM.2017.2760098, April 2018.
4. L. D'Amiano, D. Cozzolino, G. Poggi and L. Verdoliva, "A PatchMatchBased Dense-Field Algorithm for Video Copy–Move Detection and Localization," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 29, no. 3, pp. 669-682, doi: 10.1109/TCSVT.2018.2804768, March 2019
5. HanyFarid "Image Forgery Detection: A Survey" IEEE Signal Processing Magazine March 2009
6. B. Sarma, G. Nandi," A Study on Digital Image Forgery Detection", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 11, ISSN: 2277 128X, November 2014
7. Shang, S., Memon, N., and Kong, X. "Detecting documents forged by printing and copying". EURASIP Journal on Advances in Signal Processing, 2014(1). doi:10.1186/1687-6180-2014-140 ,2014
8. Z. Luo, F. Shafait and A. Mian, "Localized forgery detection in hyperspectral document images," 2015 13th International Conference on Document Analysis and Recognition (ICDAR), Tunis, Tunisia, pp. 496- 500, doi: 10.1109/ICDAR.2015.7333811, 2015
9. M. J. Khan, A. Yousaf, K. Khurshid, A. Abbas and F. Shafait, "Automated Forgery Detection in Multispectral Document Images Using Fuzzy Clustering," 13th IAPR International Workshop on Document Analysis Systems (DAS), Vienna, Austria, 2018, pp. 393-398, doi: 10.1109/DAS.2018.26, 2018
10. R. d. S. Barboza, R. D. Lins and D. M. d. Jesus, "A Color-Based Model to Determine the Age of Documents for Forensic Purposes," 12th International Conference on Document Analysis and Recognition, Washington, DC, USA, 2013, pp. 1350-1354, doi: 10.1109/ICDAR.2013.273, 2013
11. L. Nandanwar. et al. "A New Method for Detecting Altered Text in Document Image". In: Lu Y., Vincent N., Yuen P.C., Zheng WS., Cheriet F., Suen C.Y. (eds) Pattern Recognition and Artificial Intelligence. ICPRAI 2020. Lecture Notes in Computer Science, vol 12068. Springer, Cham. https://doi.org/10.1007/978-3-030-59830-3_8, 2020
12. Myna, A. N., Venkateshmurthy, M. G., and Patil, C. G. "Detection of region duplication forgery in digital images using wavelets and log-polar mapping". In International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007) (Vol. 3, pp. 371-377). IEEE,2007
13. M. Tsai and J. Liu, "Digital forensics for printed source identification," 2013 IEEE International Symposium on Circuits and Systems (ISCAS), pp. 2347-2350, doi: 10.1109/ISCAS.2013.6572349,2013
14. R. Bertrand, P. Gomez-Krämer, O. R. Terrades, P. Franco and J. Ogier, "A System Based on Intrinsic Features for Fraudulent Document Detection," 2013 12th International Conference on Document Analysis and Recognition, 2013, pp. 106-110, doi: 10.1109/ICDAR.2013.29.
15. A. Gorai, R. Pal and P. Gupta, "Document fraud detection by ink analysis using texture features and histogram matching," 2016 International Joint Conference on Neural Networks (IJCNN), 2016, pp. 4512-4517, doi: 10.1109/IJCNN.2016.7727790.

16. A. Megahed, S. M. Fadl, Q. Han and Q. Li, "Handwriting forgery detection based on ink colour features," 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS), pp. 141-144, doi: 10.1109/ICSESS.2017.8342883, 2017.

17. Shivakumara P, Basavaraja V, Gowda H S, Guru D S, Pal U, Lu T, "A New RGB Based Fusion for Forged IMEI Number Detection in Mobile Images", 2018 16th International Conference on Frontiers in Handwriting Recognition (ICFHR), pp. 386-391, doi:10.1109/icfhr-2018.2018.00074

18. Khan M J, Yousaf A., Khurshid K., Abbas A., Shafait, F (2018) "Automated Forgery Detection in Multispectral Document Images Using Fuzzy Clustering", 13th IAPR International Workshop on Document Analysis Systems (DAS), pp. 393-398, doi:10.1109/das.2018.26

19. 13 H. Dasari and C. Bhagvati." Identification of non-black inks using hsv colour space", in Document Analysis and Recognition, 2007. ICDAR 2007. Ninth International Conference on, 2007, pp. 486-490.

20. Kanika, Dr. Vivek Thapar, and Er. Gurjit Kaur, "Image Blind Detection Using GLCM, ABC and Voting Classification Method", International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 8, Issue 7, July 2021.

21. Gulivindala, Suresh and Rao, Chanamallu. (2016). "Copy Move Forgery Detection Using GLCM Based Statistical Features". International Journal on Cybernetics & Informatics. 5. 165-171. 10.5121/ijci.2016.5419.

22. Shanthi, G. & Velanganny, Cyril. (2018). "A Novel Approach for Efficient Forgery Image Detection Using Hybrid Feature Extraction and Classification", International Journal of Engineering and Technology (UAE). Pp 215-219. doi:10.14419/ijet. v7i3.27.17879.

23. Palanivel. N, Arthi.Z, Deepika.G and Latha.S," Image forgery detection using support vector machine", International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 03 | Mar 2019

24. Clara Shanthi. G, V. Cyril Raj,"An Efficient Forgery Image Detection Method using Hybrid Feature Extraction and Multiclass SVM", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-2S2, July 2019.