Digital Forgery Detection of Official Document Images in Compressed Domain

Abdulbasit Darem[1*], Asma A. Alhashmi[2*], Mohammed Javed[3#], A. B. AbuBaker[4#],

* Northern Border University, Saudi Arabia
Indian Institute of Information Technology, Allahabad, U.P -211012, India

Abstract
With the proliferation of a large number of digital tools and techniques in recent years, it becomes a challenge to tackle the crimes in the digital world like forgery or duplication of official documents. Forgery detection is a very difficult task in case of digital images if the source image is unavailable. Moreover, the problem becomes much more complex when it has to be detected directly in the compressed domain. Most of the existing forgery detection techniques are unable to work directly with the compressed digital image and fail to detect forgery within the compressed image. Therefore, this research paper aims to demonstrate two unsupervised algorithms for forgery detection - Copy-Move and Copy-Paste based forged scenarios - directly in the JPEG compressed domain.

Key words:
Forgery Detection, Copy-Move, Copy-Paste, JPEG Compression, Discrete Cosine Transform (DCT).

1. Introduction

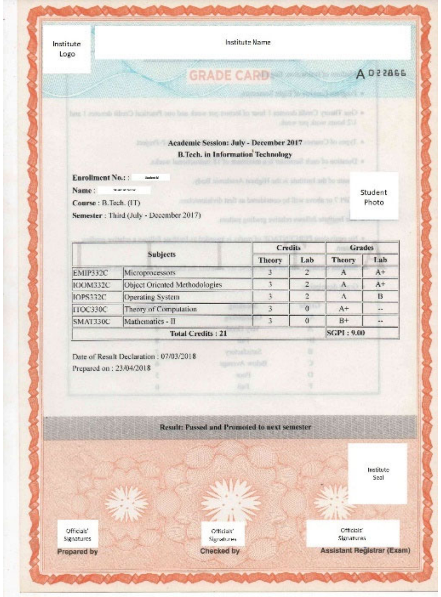
Digital forgery detection has been a problem of great interest for many decades. However, with the progress of digital tools and technology, availability of the internet and social media platforms, forgery detection has become much more challenging than ever before. Recently, the crime of forging official documents to get jobs, university admission, promotions are observed to be rapidly increasing at an alarming rate. Therefore, the issue of forgery detection in digital images is now a cybercrime and has become an important research issue in the field of cybersecurity. In the literature, many researchers have defined various types of digital forgeries and have reported different approaches to address them [1]-[7]. Therefore, developing counter technology for automatic detection of digital forgeries is also very important. In Big Data era, a huge volume of articles, images, videos, official documents are being produced in various forms on a daily basis. This huge volume of data is generated, archived and communicated in the compressed form (generally images/videos) in order to facilitate efficient storage and transfer. Performing any operation with such type of data would require the usage of repetitive compression and decompression operations, which is not advisable when large data is involved. Specifically, the compressed data is increasing for the simple reasons of the efficiency of storage and transmission. Particularly for the image data, JPEG (Joint Photographic Experts Group) is one of the most used image compression formats [8] in the internet world. Due to this, many official documents are being compressed into this format. Like normal images are compressed, forged digital images are also compressed and made available in the internet world. Therefore, forgery detection directly in the compressed domain is a potential research problem. In this research paper, we propose a forgery detection technique for forged documents that are in JPEG compressed form. With the help of the existing sophisticated digital technology, a lot of documents are getting forged every day for various purposes. The official documents are considered to be the unique, personal and very important assets for an individual or an organization. Therefore, forgery detection in official documents is one of the significant and useful problems. There are different official documents like identity documents, degree certificates, university transcripts, photographs, official letters, asset documents, and so on which need to be protected from forgeries. One such example of our interest in this research paper is the official university/institute grade card, as shown in Fig. 1. A variety of significant details are included in the student's grade card like student name, photo, grades, signatures, institution information, and other details. Usually, the forgery in this type of documents happens by replacing the person’s photo or name with person’s photo or name of another person. The signatures in the document can also be forged. It may also happen that the same person may replace the low grades with high grades of different subjects. However, in doing this, the forging person takes the utmost care to hide all the forged details. Therefore, this paper will address various forgeries issues in such official documents to uncover the forgeries.

2. Related Literature

Digital forgery detection is a well-explored research field, where numerous methods have been proposed for addressing different kinds of forgery problems [1]-[7]. The existing digital forgery detection methods can be broadly

Manuscript received December 5, 2020
Manuscript revised December 25, 2020
https://doi.org/10.22937/IJCSNS.2020.20.12.12

classified into two main groups, active methods and passive/blind methods [3][7][9]. Active methods use some hiding techniques (pre-embedded information) at the time of image creation. These techniques use steganography or digital signatures and watermarking for easy comparison with the original one for forgery detection. They are very accurate in finding image tampering. Whereas passive methods include statistical features or some inherent attributes/patterns in the image for determining the forgeries. For finding tampered images, different hidden patterns or traces are used which can be divided into three different categories as detailed in [3]. Some traces occur during image acquisition, other traces left at the time of image storage, and some other traces left during image editing.



Institute Logo

Institute Name

GRADE CARD

A 022866

Academic Session: July - December 2017

B.Tech. in Information Technology

Enrollment No.: :

Name :

Course : B.Tech. (IT)

Semester : Third (July - December 2017)

Student Photo

Subjects		Credits		Grades	
		Theory	Lab	Theory	Lab
EMIP332C	Microprocessors	3	2	A	A+
IOOM332C	Object Oriented Methodologies	3	2	A	A+
IOPS332C	Operating System	3	2	A	B
ITOC330C	Theory of Computation	3	0	A+	--
SMAT330C	Mathematics - II	3	0	B+	--
Total Credits : 21				SGPI : 9.00	

Date of Result Declaration : 07/03/2018

Prepared on : 23/04/2018

Result: Passed and Promoted to next semester

Institute Seal

Officials' Signatures

Prepared by

Officials' Signatures

Checked by

Officials' Signatures

Assistant Registrar (Exam)

Fig. 1 A sample example of an official University/Institute grade card that can be used for carrying out different forgeries.

Generally, digital images are communicated and archived in the compressed form, and JPEG is the most used compression algorithm. There are other ways where they compress the image again after applying some kind of forgery [10][11]. This research paper is specifically focused on forgery detection with only JPEG compressed document images. JPEG is a sequential compression algorithm that compresses the image by dividing the pixel image into 8×8 blocks and then applying a Discrete Cosine Transform (DCT) over them [12]. Compression leaves different patterns at each subsequent step. The first one is called the Quantization Error (QE) [12]. This occurs when the 8×8 DCT block gets divided by the standard quantization table. The second one is Rounding Error (RE) which occurs during the dequantization step. Truncation Errors (TE) also occurs in the compression processes. Generally, QE is more than the RE and TE [12]. The compression patterns in the forged image is very similar to the original image compression patterns. However, they may have some inconsistencies in lighting, shadows, perspective, and so on. These variations can be detected by proper analysis and serve as a significant clue to identify and locate the forgery[3].

There are numerous ways for tampering the pixel-based decompressed version of the JPEG compressed image. One approach is splicing the different portions of the different images also called Copy-Paste [7][21]. Another one is applying the resampling (such as resize, rotation, stretching) operations upon the forged image. The main aim of the pixel-based techniques is just to identify the forged images and ensure their authenticity. They used statistical features introduced at the pixel level. Unlike the active approaches, here any prior knowledge of the original image is not required. Warbhe and Dharaskar [14] proposed the format-based image forgery detection technique, and Ansari et. al. [13] proposed the detection of Copy-Move forgery. Here they extracted the features from the DCT coefficients. These DCT coefficients are sorted in the lexicographical order, and then the similar blocks are detected, and the forged regions are identified based on the similarity index. Forgery detection based on DCT coefficients analysis is reported in [7]. Another approach based on using a Double JPEG compression pattern is reported in [15]. However, this research work proposes an approach to detect digital forgeries directly in the JPEG compressed version of the document image.

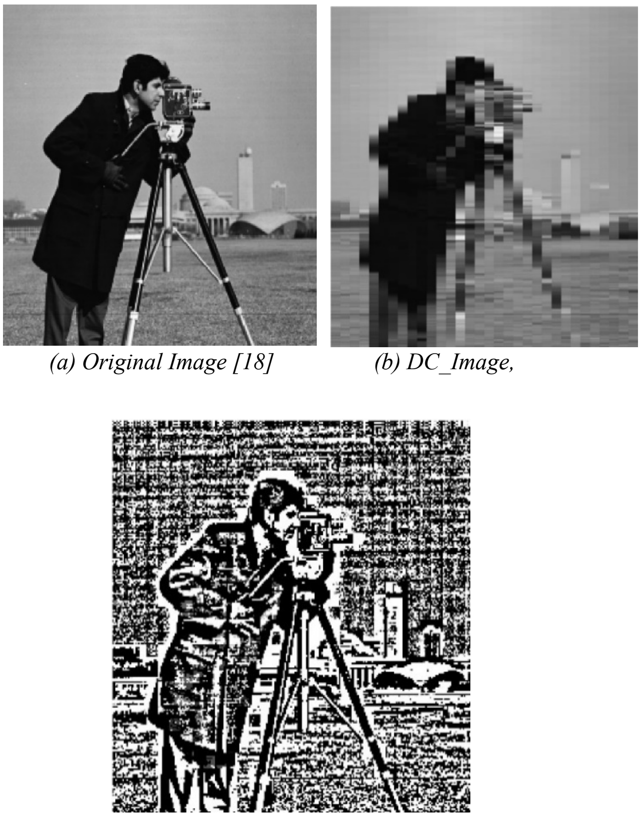
Kumar and Nagori [5] reported a few key-points based approaches like SIFT, SURF, ORB, BRISK in their research work. They used a two-step technique for detecting and describing the local interest points. The first step is to perform the localization, and in the second step, the interest points are described. During detection, each descriptor is matched with another one, and all the matched points are used to detect the duplicate points. Since these key-point features are invariant to different geometrical transformations, the robust performance is achieved even in different challenges like rotation, scaling, illumination, invariant perspective transformations. Thakur and Jindal [16] proposed another forgery detection algorithm. They first convert the input image into grayscale. This image is used to perform adaptive over-segmentation with the help of the Discrete Wavelet Transform (DWT). Hilal et al. [6] proposed HoG (Histogram of Gradients) based technique for image forgery delectation. The Copy-Move forgery detection technique is proposed in [17]. This approach is accomplished by hybridizing both the block-based DCT technique and a key-point based SURF technique. Here it first performs the DCT operation upon the forged image with the goal of enhancing the detection rate of the image, and then it applies the SURF for detecting the tampered areas in the image.

Brief Review on JPEG

In DCT, a finite sequence of data points is expressed in terms of a sum of cosine functions having a different oscillating frequency. In JPEG Compression [12], the pixel image is segmented in 8×8 non-overlapping blocks. Using *Eq. 1*, DCT operation is performed on each block to convert that into the form of 64 DCT coefficients. A typical 8×8 pixel is shown in the below matrix (denoted as PB) in Fig. 3. The corresponding DCT blocks with only DC value and with only AC values are shown with respective matrices (DB and AB). This information is very useful to understand the underline details of the proposed methods in the below sections.

$$F_{uv} = \frac{c_u c_v}{4} \sum_{i=1}^{7} \sum_{j=1}^{7} f(i,j) cos(\frac{(2m+1)u\pi}{16}) cos(\frac{(2n+1)v\pi}{16})$$

$$Where, c_u, c_v = \begin{cases} \frac{1}{\sqrt{2}} & for\ u,v = 0 \\ 1 & otherwise \end{cases} \quad 0 \leq \text{u, v} \leq 7 \qquad \textit{Eq. (1)}$$



(a) Original Image [18]

(b) DC_Image,

(c) AC_Image

Fig. 2 A typical sample image and reproduced images

$$\boldsymbol{PB} = \begin{bmatrix} 156 & 159 & 158 & 155 & 158 & 156 & 159 & 158 \\ 160 & 154 & 157 & 158 & 157 & 159 & 158 & 158 \\ 156 & 159 & 158 & 155 & 158 & 156 & 159 & 158 \\ 160 & 154 & 157 & 158 & 157 & 159 & 158 & 158 \\ 156 & 153 & 155 & 159 & 159 & 155 & 156 & 155 \\ 155 & 155 & 155 & 157 & 156 & 159 & 152 & 158 \\ 156 & 153 & 157 & 156 & 153 & 155 & 154 & 155 \\ 159 & 159 & 156 & 158 & 156 & 159 & 157 & 161 \end{bmatrix}$$

$$\boldsymbol{DB} = \begin{bmatrix} 1254 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\boldsymbol{AB} = \begin{bmatrix} 0 & -1 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & -1 & 0 & 0 & -1 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 & -1 & -1 & -1 & -1 \\ -1 & 0 & -1 & -1 & 0 & -1 & 0 & -1 \\ 0 & -1 & 0 & 0 & 0 & 0 & -1 & 0 \\ -1 & 0 & 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -1 & -1 & -1 & -1 & -1 \\ -1 & 0 & -1 & -1 & -1 & -1 & -1 & 0 \end{bmatrix}$$

Fig. 3 A typical 8×8-pixel matrix (denoted as PB).

3. Proposed Methods

The JPEG compression algorithm transforms the pixel image into the DCT form by repetitively convolving the 8 × 8 DCT operation on each 8 × 8 non-overlapping pixel blocks. This DCT operation is the basic building process for transforming the whole image. This process converts the whole image into a non-overlapping 8 × 8 DCT block. These DCT coefficients are called to be the compressed representation of the document. Based on the type of pixel values the DCT operation produces different coefficient values. Each DCT block consists of one DC value and 63 AC coefficients. In a typical DCT block, the DC value signifies the amount of content that block contains. Similarly, the AC coefficients also give significant information about the frequency levels of the pixels contained in that block. To understand the contents of any document directly in the compressed domain these coefficients are very much useful and sufficient. In this work, these coefficients are used as features for forgery detection and its location. A typical sample image in the pixel domain is shown in Fig. 2 (a). From the compressed representation of this figure, two other figures have been reproduced from its compressed version. One is reproduced by extracting only one DC value from each 8 × 8 DCT block, and it is called a DC_Image as shown in Fig. 2(b). Similarly, the second one is called the AC_Image as shown in Fig. 2 (c), which is reproduced by taking AC coefficients alone from each block. For each of these images, one 8×8 block of their numerical values is shown respectively in Fig. 3. They are 8 × 8-pixel blocks (PB), and its DC coefficients block (DB) and AC coefficients block (AB). Here, the DC_Image is showing some blur/no smooth effect at the borders, because it does not have an AC Coefficient. Similarly, the AC_Image is also showing the mesh-like/no shade appearance which is because of the absence of DC value. The overall observation is that from each block the DC and AC coefficients are carrying significant information of the pixel image contents. Although the forgery detection is very challenging in the pixel domain itself, based on this information from the DCT blocks, an attempt has been made for detecting the forgery in official documents directly in the JPEG compressed domain. Two types of methods are proposed in this paper. One method is to address the Copy-Move forgery detection, and another one is to address the Copy-Paste forgery detection directly in the JPEG compressed domain.

Usually, the forgery in official marks cards happens by copying the high grades of different subjects to replace the other subjects of low grades in the same marks sheet. For example, the mathematics subject grade D may be replaced by the science subject grade A+. This is a kind of Copy-Move forgery where they copy some portion of the same image and move it to another place [3]. In this scenario, it is clear that the forged document contains at least two similar contents within that image. There might be a possibility that the same grade/marks would be replaced by many other subjects' grades/marks. Depending on the amount of forgery many similar patches can be located more than two times in a forged document. In other words, the coefficient values of those regions would be similar. Another type of forgery happens by copying some grades, symbols/stamps, or signatures from one document and pasting them on the other document. This is called Copy-Paste forgery. Unlike the Copy-Move forgery, the pasted content may not present two times. Since this pasted content is from another image, definitely it contains different compression patterns in it. This patch may not be perfectly matched with the document on which it pasted. For solving these two types of forgeries two different approaches have been proposed respectively.

3.1 An approach for Copy-Move forgery detection

The Copy-Move detection approach is based on developing a template with the help of the 8×8 DCT block coefficients. Generally, after performing the forgery, the images are compressed with high quality/low-quality factors and perform some post-processing on the forged patch to cover the details of forgery. Based on this assumption, an approach is proposed for detecting the Copy-Move forgery. The block diagram of the proposed method is shown in Fig. 4. We first extract the DCT coefficients for the compressed stream of the document image. This extracted image is in the form n number of small 8×8 DCT blocks. After observing the certain blocks in the forged image, it has been noted that similar patches are having the same values in their respective DCT blocks. With this understanding, each 8 × 8 DCT block is considered as one individual template. Each template would be matched with all other templates once. In this matching process, the respective coefficient values are matched with the coefficient values in the other block. The same templates produce a high similarity score based on this similarity value.

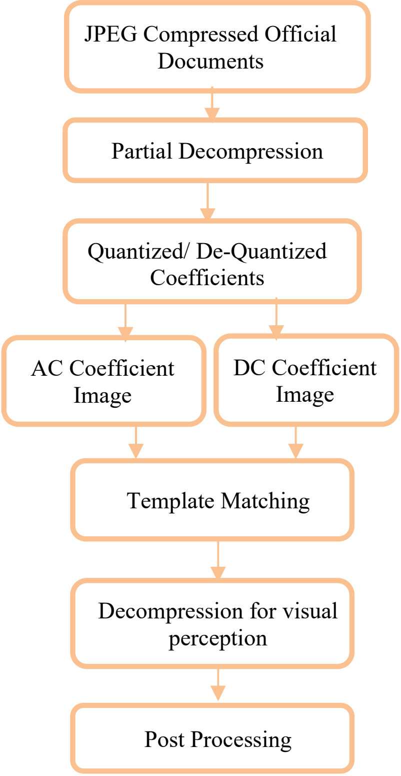

JPEG Compressed Official Documents
Partial Decompression
Quantized/ De-Quantized Coefficients
AC Coefficient Image
DC Coefficient Image
Template Matching
Decompression for visual perception
Post Processing

Fig. 4 The block diagram of the proposed method for Copy-Move forgery detection in official grade cards.

3.2 An approach for Copy-Paste forgery detection

In the Copy-Paste forgery detection, since the forged regions are not from the same image, the above template matching based method is not a suitable technique for detecting Copy-Paste forgery. In the literature, many researchers have used the double compression patterns as the feature for forgery detection [1]-[5]. The block diagram of proposed method is shown in Fig. 5. The compressed image is generated from the DCT compressed stream. We have tested the generated images by taking two types of information from 8x8 coefficient blocks. One is just by extracting only the AC coefficients. The other one is by extracting the DC coefficients. To address the Copy-Paste forgery, we have used the approach proposed in [21] which used the Averaged Sum of Absolute Difference (ASAD) technique as shown in Equation 2. This has been done in the pixel domain based on the assumption that the forged image is compressed with high quality in the second time after performing some forgery. The two versions of the images have been generated based on the Equation 2. Here we go from left to right and top to bottom select the 512 x 512 block. The first quantization "q1i" is applied to this block called to be "C1i". Similarly, the second quantization "q2i" step is applied to the same block to get the "C2i". This second image is subtracted from the first image. Due to this subtraction, the un-forged regions are mitigated and some clues like bright dots have been highlighted at the position of forgery in the document. Here also the morphological post-processing techniques have been applied to further highlight these details.

$$v_{asad}(i) = \frac{1}{512\times512}\sum_{n=1}^{512\times512}|c_{2i}(n) - c_{1i}(n)\,| \quad \textit{Eq. (2)}$$

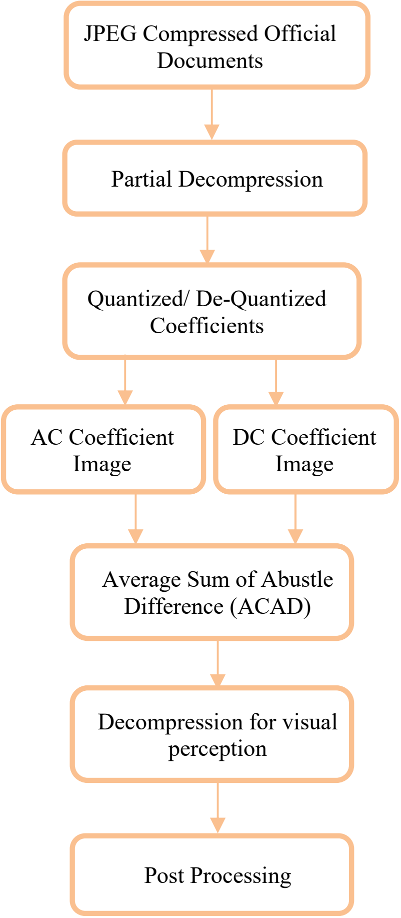

JPEG Compressed Official Documents
Partial Decompression
Quantized/ De-Quantized Coefficients
AC Coefficient Image
DC Coefficient Image
Average Sum of Abustle Difference (ACAD)
Decompression for visual perception
Post Processing

Fig. 5 The block diagram of the proposed method for Copy-Paste forgery detection in official grade cards.

4. Results and Analyses

The proposed models have been tested on two datasets which include both official document images and normal scenery images. The first dataset is CoMoFoD database [20]. It consists of 260 forged image sets with two types of images sizes. The first size is 512x512, and the other one is 3000x2000. The images are categorized into 5 different groups based on the different manipulations (translation, rotation, scaling, combination, and distortion). The second dataset is Official Marks Card Dataset (OMCD) which is created by authors. OMCD dataset contains 300 JPEG compressed official marks cards. OMCD dataset created with various kinds of forgeries that come under both Copy-Move and Copy-Paste detection techniques like moving or replacing names, grades, photos, signatures, etc...

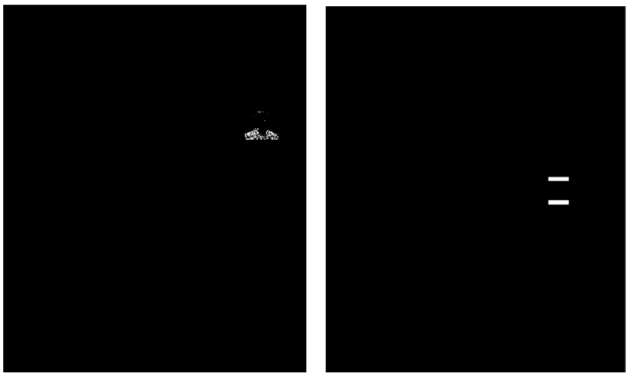
The performance and accuracy of the proposed model are evaluated by Precision, Recall, and F Measure variables. The precision is defined as the fraction of true instances among the total detected instances. Similarly, the recall is the total amount of relevant instances that were actually detected. F Measure represents the total test accuracy. The formulas of these variables are shown in Equation 3.

$$\boldsymbol{Recall} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FP}}\ ;\ \boldsymbol{Precision} = \frac{\boldsymbol{TP}}{\boldsymbol{TP+FN}}\ ; \qquad \textit{Eq.}\ (3)$$

$$\boldsymbol{F} = \boldsymbol{2} \times \frac{\boldsymbol{Precision} \times \boldsymbol{Recall}}{\boldsymbol{Precision+Recall}}$$

All the results of the proposed model are tabulated in Table1, Table 2, and Table 3. Table1 and Table 2 show the results of various analyses like quantized and unquantized DCT coefficients compared to different coefficients. Table1 shows the performance of the proposed methods tested on the standard datasets CoMoFoD and Table 2 shows the results on OMCD dataset. The output images of the proposed approaches are shown in Fig. *6*, where (a) shows a sample of output image of student-image forgery in grade card using Copy-Paste approach and (b)) shows a sample of output image of student-grades forgery in grade card using Copy-Move approach. The CoMoFoD dataset contains only the Copy-Move forge images therefore we created OMCD dataset of official document and tested both Copy-Move and copy pest method. Since Copy-Paste technique works using only DC values, the experiments were carried out only using DC coefficients for Copy-Paste method which is shown in Table 2. The results of the proposed model are compared in Table 3 with different other models that are existed in the literature.

In the 8 × 8 DCT block, DC value carries lots of information. For template matching, we used three types of matching. One is based on matching with just one DC value within two DCT blocks alone, and the second one is using AC coefficients, and the third one is just by using the DC value along with three positions (01, 11, 10) of the AC coefficients. The same three kinds of matching are applied for both quantized and unquantized DCT coefficients also. During template matching, we found that, matching one DC value is faster than matching the whole block. But in the whole comparison process, it's true that most of the DC values would be the same if it contains similar large background. Sometime this may lead to being easily matched with some other DC value in another DCT block but at the same time, we cannot decide that both of these blocks are forged. This would be the same case even if we take the other AC coefficients into the matching process.



(a) (b)

Fig. 6: The sample output images of forgery detection in JPEG compressed domain

Table1. The results of the proposed model tested on CoMoFoD dataset continuing only Copy-Move forge images

Type of Operation	Precision (%)	Recall (%)	F Measure (%)	Speed (sec)
Quantized (AC Coefficients, Copy move)	91.45	92.28	91.86	102
Quantized (DC Coefficients, Copy move)	95.95	94.52	95.22	78
Unquantized (AC Coefficients, Copy move)	87.13	86.34	86.73	127
Unquantized (DC Coefficients, Copy move)	96.31	90.18	93.14	89

Table 2. The results of the proposed model tested on OMCD dataset

Type of Operation	Precision (%)	Recall (%)	F Measure (%)	Speed (sec)
Quantized (AC Coefficients, Copy move)	83.45	90.01	86.60	267
Quantized (DC Coefficients, Copy move)	89.95	93.78	91.82	130
Unquantized (AC Coefficients, Copy move)	80.13	90.29	84.90	261
Unquantized (DC Coefficients, Copy move)	86.31	87.59	86.94	136
DC coefficient image, Copy Paste)	80.45	89.05	84.53	70

Table 3. The proposed method with other methods

Type of Operation	Precision (%)	Recall (%)	F Measure (%)
Muhammad Bilal [19] (using CoMoFoD dataset)	95.98	91.24	93.54
Abhishek Thakur [16] (using CoMoFoD dataset)	97.25	100	98.53
Nan Zhu [15] (using CASIA TIDEv 2.0 dataset)	94.08	80.48	86.75
Proposed method using OMCD dataset (JPEG compressed domain, Copy-Move)	95.95	94.52	95.22
Proposed method using OMCD dataset (JPEG compressed domain, Copy-Paste)	80.45	89.05	84.53

5. Conclusion

This paper proposed two approaches for detecting forgery in official documents directly in the JPEG compressed domain. The DCT coefficients have been extracted from the compressed representation. The DC and AC coefficients have been used as a template. Template matching has been used to identify and locate the forgery regions. Some templates have been used as the forgery regions (for Copy-Move). Whereas, for locating the Copy-Paste forgery, the subtraction method has been used. Extensive experiments have been conducted to reach the satisfactory level of performance.

Acknowledgment

The authors gratefully acknowledge the approval and the support of this research study by grant no. SAT-2018-3-9-F-7974 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

References

[1] Bilal, Muhammad, et al. "Single and Multiple Copy–Move Forgery Detection and Localization in Digital Images Based on the Sparsely Encoded Distinctive Features and DBSCAN Clustering." *Arabian Journal for Science and Engineering* (2019): 1-18.

[2] Soni, Badal, Pradip K. Das, and Dalton Meitei Thounaojam. "Geometric transformation invariant block-based copy-move forgery detection using fast and efficient hybrid local features." *Journal of information security and applications* 45(2019): 44-51.

[3] Lin, et al. "Recent advances in passive digital image security forensics: A brief review." *Engineering* 4.1 (2018): 29-39

[4] Hassan, Alsadig Bashir, and Yahia A. Fadlalla. "A survey on techniques of detecting identity documents

forgery." *2017 Sudan Conference on Computer Science and Information Technology (SCCSIT)*. IEEE, 2017.pp. 1–5.

[5] Kumar, Sunil, and Swati Nagori. "Key-point based copy-move forgery detection in digital images." *Journal of Statistics and Management Systems* 20.4 (2017): 611-621.

[6] Hilal, Mahale Vivek, Pravin Yannawar, and Ashok T. Gaikwad. "Image inconsistency detection using histogram of orientated gradient (HOG)." *2017 1st Inte. Conference on Intelligent Systems and Information Management (ICISIM)*.IEEE,2017.pp. 22–25.

[7] Lin, Zhouchen, et al. "Fast, automatic and fine-grained tampered JPEG image detection via DCT coefficient analysis." *Pattern Recognition* 42.11(2009):2492-2501.

[8] Wu, Shaobao, et al. "Localizing JPEG Image Forgeries via SIFT and DCT Coefficient Analysis." *2019 IEEE 19th International Conference on Communication Technology (ICCT)*. IEEE, 2019. pp. 1635–1638.

[9] Gurunlu, Bilgehan, and Serkan Ozturk. "A Survey on Photo Forgery Detection Methods." *ITM Web of Conferences*. Vol. 22. EDP Sciences, 2018., p. 01055.

[10] Galvan, Fausto, et al. "First quantization matrix estimation from double compressed JPEG images." *IEEE Transactions on Information Forensics and Security* 9.8 (2014): 1299-1310.

[11] Yu, Liyang, et al. "An improved parameter estimation scheme for image modification detection based on DCT coefficient analysis." *Forensic science international* 259 (2016): 200-209.

[12] Mukhopadhyay, Jayanta. *Image and video processing in the compressed domain*. CRC Press, 2011..

[13] Ansari, Mohd Dilshad, Satya Prakash Ghrera, and Vipin Tyagi. "Pixel-based image forgery detection: A review." *IETE journal of education* 55.1 (2014): 40-46.

[14] Warbhe, Anil Dada, and R. V. Dharaskar. "Survey on Pixel and Format Based Image Forgery Detection Techniques." *Recent Trends in Computing (NCRTC), MPGI National Multi Conference*. 2012., pp. 7–8.

[15] Zhu, Nan, Junge Shen, and Xiaotong Niu. "Double JPEG Compression Detection Based on Noise-Free DCT Coefficients Mixture Histogram Model." *Symmetry* 11.9 (2019): 1119.

[16] Thakur, Abhishek, and Neeru Jindal. "Image forensics using color illumination, block and key point-based approach." *Multimedia Tools and Applications* 77.19 (2018): 26033-26053.

[17] Ojeniyi, Joseph A., et al. "Hybridized Technique for Copy-Move Forgery Detection Using Discrete Cosine Transform and Speeded-Up Robust Feature Techniques." *International Journal of Image, Graphics and Signal Processing* 10.4 (2018): 22.

[18] Gonzalez, Rafael C. "Richard E. Woods Digital Image Processing, Pearson." (2018).

[19] Bilal, Muhammad, et al. "A robust technique for copy-move forgery detection from small and extremely smooth tampered regions based on the DHE-SURF features and mDBSCAN clustering." *Australian Journal of Forensic Sciences* (2020): 1-24.

[20] Tralic, Dijana, et al. "CoMoFoD—New database for copy-move forgery detection." *Proceedings ELMAR-2013*. IEEE, 2013., pp. 49-54.

[21] Li, Xiang-hua, et al. "Passive detection of copy-paste forgery between JPEG images." *Journal of Central South University* 19.10 (2012): 2839-2851.

Dr. Abdulbasit Darem is an Assistant Professor at Northern Border University Saudi Arabia. He participated in many conferences and published more than 18 research papers in reputed international Journals and Conferences. He is working currently in five research projects funded by NBU university and MOH, KSA. His areas of research interest are Cybersecurity, Human Computer Interaction, E-government, Web Engineering and Cloud Computing.

Dr. Asma A. Alhashmi is an Assistant Professor at Northern Border University Saudi Arabia. She participated in many conferences and published more than 18 research papers in reputed international Journals and Conferences. She is working currently in five research projects /funded by NBU university and MOH, KSA. Her research interests are Cybersecurity, E-government, Human Computer Interaction, Web Engineering and Cloud Computing.

Dr. Mohammed Javed is currently working as assistant professor in Dept. Of IT, Indian institute of information technology, Allahabad, India. His research interests are in image processing, pattern recognition, data compression and cybersecurity. He has published more than 30 research papers in various international journals and conferences.

Dr. A. B. AbuBaker is an assistant professor in applied science department (mathematics) of Indian institute of information technology Allahabad, India. He has published more than 10 research papers in various international journals and conferences. His research interests are in functional analysis, linear algebra and its applications.