Abstract—With the wide spread of digital document use in administrations, fabrication and use of forged documents have become a serious problem. This paper presents a study and classification of the most important works on image and document forgery detection. The classification is based on documents type, forgery type, detection method, validation dataset, evaluation metrics and obtained results. Most of existing forgery detection works are dealing with images and few of them analyze administrative documents and go deeper to analyze their contents.

Keywords—Document forgery, Copy-move forgery, Splicing, imputation, forgery detection methods, Digital image forgery.

I. INTRODUCTION

Administrative documents are forms created to establish an identity, right or authorization. And therefore, falsification of documents or identity is severely punishable by law. This concerns identity and authorization documents such as passports, identity cards and driving licenses. Fraudsters use these false documents to commit offences generally, like travelling using fake passport or visa, or to forge diplomas to get a job. Moreover, digitalization or digital transformation has created new communication and optimization tools for business and administration management. Due to new technologies, it is easy to digitize documents using a scanner and save them in pdf format or images. The new tendency of governments is to use digital documents instead of hard ones to optimize many administrative procedures.

Unfortunately, nowadays document images tampering has become easier with the use of sophisticated tools with recent advances in technology and multimedia. Anyone can use available and low cost professional image forgery tools easily to modify images, such that it cannot be distinguished from authentic ones with the naked eye. Image forgery detection is categorized into two main types: active and passive methods. The active methods are concerned with digital signatures or watermarking. They depend on previous information taken from the original image. Though, these methods are not used for all kind of documents because they need special equipment to embed watermark or a signature like particular cameras. Alternatively, passive methods are used to detect forgery without previous inserted information [1]. These methods can treat two main types of image forgery: Copy-move tampering (CMF) and image splicing tampering, where copy-move forgery is the most generally adapted by forgers. Many researchers have been interested to copy-move forgery and there exist several methods introduced in this field. CMF is the way of copying a part of an image and pasting it into another region on the same image, while splicing is combining multiple regions of different images to create a forged image [1], [2], [3]. There exist two main categories of techniques used to detect CMF: Block-based and key-point based methods. Where each of these techniques involve a feature extraction phase and a matching process.

This report presents main existent works related to image and document forgery detection and introduces their methods, results and discussion. The aim of this report is to point the main challenges of this research field and to compare the proposed methods and discuss their advantages and limits.

II. DIGITAL IMAGE FORGERY DETECTION METHODS

After the tremendous development in communication technologies in last recent years, digital image forgery detection has become a centre of interest for many scientific researchers trying to secure many administrative and business activities. Indeed, scientific research is now aware of the proposition of several techniques for the detection of falsified documents, especially passive methods.

Image forgery detection is concerned with detecting manipulated images or verifying their authenticity. It is divided into two main categories: Active and passive.

A. Passive methods

Passive forgery detection techniques do not need any signature or watermark to detect forgery but rather by analysing the statistical distortion they leave behind after forgery although the detection of digital image falsification in this case is considered more difficult. This technique has become widely used because it does not need prior information about the image. It depends on the hypothesis that any modification in the image may change its consistency or statistics property [4].

1) Copy-move forgery detection (CMFD)

Most of the research in the image forgery detection field is concentrated on copy-move forgery. In this section we explain CMFD and the common workflow of CMFD techniques.

The copy-move process is based on the idea of taking a part or parts of the image and pasting it on other sides of the same image. Because texture and color of these regions are similar, blending them into the background becomes easier.

In documents forgery, CMF is generally used to hide or add information, see Fig. 1.

![Fig. 1. A: Authentic image B: Forged image.](image-url)
CMFD process starts generally with a pre-processing step to enhance image features. The images can then be converted into grayscale colors and divided into blocks. After pre-processing, a feature extraction step is used to collect information representing the characteristics of the regions of interest in the image. After feature extraction is performed a matching phase is used to elicit similar features in the image. Finally, it is possible to show and identify the potential falsified regions in the image by visualising the results of the CMFD process [5].

CMFD techniques are organized into two main types, block-based and keypoint-based:

a) Block-based method: This method depends on dividing the image into blocks of different shapes, including squares and circles that can be non-overlapping or overlapping to be used afterwards in the preprocessing stage. Then, two main steps are performed to detect forgery:

- Features are first extracted from these blocks and compared to determine their level of similarity.
  
  i. Feature extraction step

  There exists many techniques for features extraction in block-based methods. We can cite for example:
  - Discrete Cosine Transform (DCT) which is one of the most widely used techniques in CMFD. It is based on frequency transform and known for its robustness against noise addition and JPEG compression [5].
  - Texture and intensity based features used in images that contain certain patterns or textures, for example we mention pictures that contain landscapes characterised by containing a certain density and smoothness, such as grass, trees, ground and sky [5].

  ii. Matching step

  To find similar blocks, the matching process is used to compare the features for each block and then match them to determine the manipulated area. Here is some of matching techniques for block-based methods:
  - Sorting: Sorting is a way that order the features, and it is commonly used in the matching process of block-based approaches. The sorting techniques include : KD-Tree, Lexicographical, and Radix [5].
  - Euclidean distance: Euclidean distance is measuring the distance between two points or two vectors in the Euclidean space. After arranging the calculated distances, the similar blocks are identified, and then the suspected regions are distinguished in the image [5].

iii. The main existing works:

In 2015, Beste Ustuboglu et al. [6] presented a technique to detect copy-move forgery using color moments. First they divided the image into circle blocks. Then, they extracted feature vectors from the blocks using three-color moments. Afterwards, the feature vector matrix has to be sorted lexicographically. To create a dataset, they used images from Google image search then they create fake images by duplicating some regions in the image and putting it within the same image. They found that the proposed method had high accuracy and false positive ratio with 0.9981 and 0.0205 respectively.

In 2017, using histogram of orientated gradient, Mahale Vivek Hilal et al. [7] presented an algorithm to detect copy-move forgery. In their methodology they started with a preprocessing step: first they convert images into grayscale, then to find out the intensity direction, they measure the gradient of image and after that they apply the Gaussian filter. Afterwards, they passed to feature extraction phase: In this step they divide the image into overlapping blocks of fixed size. After the image is divided into blocks, the Histogram of Oriented Gradient (HOG) is calculated for each block to find descriptor features. Then, a matching step is performed to identify the forged regions. They used the Euclidean distance with a threshold value to get the decision. As for the dataset, they used a public dataset called COMOFOD. They tested their approach on three different experimentations using three different dataset sizes. They got as best result a false acceptance rate of 0.82 and false rejection rate of 0.17 in the case of taking 70 original images and 70 forged.

In 2018, using discrete cosine transform, Mohammed Hazim Alkawaz et al. [8] presented a method for copy-move forgery detection. Using block-based detection approach with different block sizes, this work aims to study the effect of block size on its effectiveness in detecting forged areas in terms of FP and FN. They presented a process for the framework that starts with an RGB image then they convert it to a grayscale. After that, they partitioned the image into overlapping blocks between 4 × 4 and 8 × 8 pixels, then for each block they computed the 2D DCT coefficient and rearranged it into feature vector using zigzag scanning. With a lexicographic sorting, all blocks should be sorted then matching blocks is carried out to find duplicated blocks with Euclidean distance. For the implementation they used CoMoFoD dataset.

In 2018, Badal Soni et al. [9] proposed a technique that uses Speeded Up Robust Features (SURF) for block-based feature extraction, and for matching it uses Features from Accelerated Segment Test (FAST) key point method. First, they begin with a preprocessing stage where they convert the image into grayscale domain, then they divide it into n × n overlapping blocks. Then to extract features, they extract SURF descriptors from each block. Afterwards, they pass to matching process using FAST features points to concatenate neighbouring blocks. Thereafter, the extracted features have to be matched using 2NN matching procedure. Finally, they terminate by removing outliers if they exist. To evaluate the performance of their method, they used three different versions of the MICC dataset. They realize that the proposed technique is robust against rotation and scaling attacks. Also, they tested the proposed system performance by measuring TPR, FPR and execution time of the algorithm in seconds and they obtained the following results for the MICC-F220 dataset: 97.4%, 8.6% and 9.2 seconds respectively, the MICC-F2000 dataset: 94.5%, 9.8% and 28.6 seconds and the MICC-F8 multi dataset: 83.84%, 12.64% and 11.2 seconds.

In 2019, Tingge Zhu et al. [10] proposed a method based on LBP residue classes (LBPRC) and color regions (CR). The frame work of the proposed algorithm detects and identifies suspected tampered areas. First, the image has to be divided into overlapping blocks. Afterwards, for each block they compute LBPRC and CR to search then for similar blocks in the same LBPRC and CR. In this stage, the suspicious regions are extracted from these matching pairs. Finally, depending on a given threshold, they locate the forged regions.
To test the performance of their method, they used two databases: the CMH database and the CoMoFoD_small_v2 database. They employed recall, precision and F1 (a trade between precision and recall), and they achieve respectively 93.65%, 97.98% and 96.58% using the CoMoFoD_small_v2 database.

b) Keypoint-based method: Keypoint-based method is non block-based. Key point features are extracted from the distinct area such as edges and corners. Each feature is represented by a set of descriptors. Then, Descriptors and features are collected to be classified and then matched to identify duplicated regions in the image.

i. Feature extraction techniques

There are three categories for feature extraction of key-points methods, which are:
- Scale Invariant Feature Transform (SIFT).
- Speed Up Robust Features (SURF).
- Harris Corner Detector

Where, SIFT is frequently used in key point-based approach. Due to the effectiveness and the stability of this technique, it has been strongly used in the CMFD.

ii. Matching techniques

- Nearest neighbour is one of the similarity measurement methods used. It is used to measure the similarity between two specific points in a vector space by calculating the distance between these two points. We say that there is a similarity when the distance does not exceed a certain threshold.
- Clustering technique is a technique that combines similar objects together and puts them into groups [5].

iii. The main existent works

In 2010, Xu Bo et al. [11] proposed a method for copy-move forgery detection using SURF key point to find duplicate regions in the image. The main point of using this algorithm is to produce fast results compared to other key point feature extraction techniques. First, they extract the interest points to assign a unique orientation by using the Haar wavelet. In a second step, they extract square regions around the interest points using SURF descriptors. To determine the duplication between two images, they used the Euclidean distance for all feature descriptors. In the experiments, they used the Uncompressed Color Images Database (UCID) edited. They tested robustness against scaling, rotation, blurring and noise. They found that the proposed method can accurately detect duplicate areas and can also resist to the impact of noise, scaling and rotation.

In 2018, Hesham A.Alberry et al. [1] presented a copy move forgery detection method in which they introduce a fast technique that optimizes SIFT and fuzzy C-means (FCM) clustering. The technology is based on the SIFT algorithm for feature extraction. Fuzzy C-mean Clustering method is used to reduce the time complexity of SIFT algorithm. First, the key points are extracted by SIFT method. Then, these key points are used to extract the feature descriptor. Afterwards, they passed to a matching stage followed by a clustering algorithm to cluster the key points. For the experimental step, they used 573 pictures. They used the MICC-220 as a dataset plus their own data. They evaluated their method by measuring TPR, FPR and time complexity. To obtain the best results, three main parameters are used in FCM algorithm which are: the number of clusters, the maximum of clusters to create and the minimum amount of improvement. Their results depends on the datasets that are used, they noticed that the TPR of the MICC-220 is superior to the one obtained from their dataset, also the former exhibits a lower time complexity. Perhaps, that is due to the professional forged images used and the high number of images with high resolution in their dataset as compared to the MICC-220 dataset.

c) Other: Within existing algorithms, most of them are focusing on block-based and keypoint-based methods or both of them. Below, we survey other recently presented works using other detection methods.

In 2017, Junlin Ouyang et al. [12] proposed a new method using convolutional neural networks to detect copy-move forgery. Using a small sample of training data, they slightly modify the network architecture taken from an existing database of trained models such as ImageNet. To accomplish their work, they built their handcraft dataset that contained about 10000 images, also they used both the OXFORD and the UCID datasets. Subsequently, the Convolutional neural network CNN network was initialized while fine-tuning some of the parameters. Eventually, they can attain results by imputing test images into the obtained trained model. For the results, they achieved good performance on both the Oxford and the UCID datasets with 2.32% and 2.43% test error respectively. However, they got very poor performance for the handcraft database with 42% test error due to the random tampering operation.

For a deeper study on the CMFD techniques see [13]. S.Teerakanok et al. presented a review and analysis of CMFD. In addition, they proposed a new CMFD framework that considered CMFD techniques as a single framework and no longer divided into block-based and key-point based techniques.

2) Splicing forgery: Splicing is combining different elements from multiple images into a single image to create a fake one see Fig. 2. The tampering traces cannot be seen and it can be hardly tracked even if no post-processing is done [14]. It can be detected by looking for the effect of Splicing on the image statistics, by noticing the degrees of light on the image, or by searching the boundaries of the extraneous region [3]. Recently, some methods have been presented to detect image splicing forgery.

Splicing Imitation

Fig. 2. Splicing & Imitation forgery.
In 2013, using both techniques Discrete cosine transform (DCT) and Local Binary Pattern (LBP), Amani A.Alahmadi et al. [15] presented a new method to detect Splicing forgery. First, they divided the input image into overlapping blocks. Then for each block, they computed LBP and transformed it into frequency domain using 2D DCT. Finally, they used standard deviation to extract features and for the classification they used SVM.

For the input image they worked in chromatic channel. They used CASIA databases and Columbia Uncompressed Image Splicing Detection Evaluation Dataset. To evaluate the performance of the proposed method, they calculated the accuracy which reached to 97%.

Most of the methods have been proposed to detect splicing or CM forgery, however, in 2017, Chandhany Shyan et al. [16] proposed a method that aimed to detect both splicing and CM forgery using the same dataset. This method combines block discrete cosine transform (DCT) and Zernike moments, they used a process combining two main steps: finding image forgery using SVM classifier and classification of the output to either of the forgery types.

The proposed method extracted the features of a color image based on developed threshold method. First they used DCT to transform non-overlapping blocks of an image into matrices from which the discriminative features for forgery detection are extracted using an enhanced threshold method. Before that, to minimize the effect caused by the diversity of the image content, they deployed a pre-processing step.

For copy-move forgery detection they used a feature extraction technique. Afterwards, they used the Patch Match Algorithm implementing three steps: initialisation, propagation and random search. After the feature matching process they used a post-processing step to increase the possibility of detecting forgery in a proper manner without being exposed to a false alarm of Copy-move forgery detection.

They used in their experimentation the CASIA dataset. CASIA v1.0 consists of 1721 images between authentic and tampered images using splicing. However, CASIA v2.0 is the largest, it contains 12614 color images between authentic and tampered. The experimental results showed the effectiveness of the proposed method, as it gave a good accuracy rate of 99.50% at threshold $T = 8$ in the Splicing forgery type, but in Copy-move type it gave 87.50%, which is an evidence of the proposed method.

The database was constructed using text document and images, the text includes different language characters like English character “e” and Arabic character “Djim”. They used also benchmarked image like Peppers, Lena and Baboon. The results showed high accuracy according to the experiments. Where, the lowest accuracy they got is 79.71% and the highest one is 99.36% for different language characters and different CNN architectures. While, the highest accuracy rate for images is 99.95% using Lena image. On the other hand, the SVM classification system showed good performance with high accuracy (accuracy=99.97) for Peppers image.

In 2017, Francisco Cruz et al. [20] proposed a method where their aim was to detect tampered regions using a direct modification without any post-processing. Their method was based on the idea that the background of the forged image would not be coherent and consistent and the counterfeit region would appear different from the other intact neighbouring regions. They used in their experiments a handmade dataset of 200 documents, each of which contains at least one forgery operation. Thus, they collected 481 forgery instances with different types of forgery (copy-move, imitation and region cuts). They used SVM as classifier for their experiments with a cross-validation. For the results, they showed that they were able to detect the forged regions with 7.38% and with 0.05% of false positive ratio.

In 2017, H. Benhamza et al. [21] proposed a method to detect administrative digital documents forgery based on analytic study of scanned documents. In order to determine that, they calculate the similarity of the image document according to the three basic components of the document: background texture, text and stamp or signature. Hence, they divided the image into non overlapped blocks with different sizes. Then, they calculated the mean and the standard deviation of each block to calculate the homogeneity of the image. Using these measurements they extract a features vector. They used SVM machine learning technique on a
handmade dataset and the best accuracy they obtained was 85.24%.

In 2018, Shruti Ranjan et al. [22] presented a method for digital image forgery. They enhanced the quality of the images using histogram equalization. Afterwards, they removed noise using a median filter and segmented images using K-means clustering. They extracted features using the Gray Level Co-occurrence Matrix (GLCM), which is a matrix used to analyse the texture with a set of statistical measurements. The classifier first used was the linear SVM then they used Artificial Neural Network (ANN) classifier which showed good results compared to that given by linear SVM (ANN accuracy = 96.4%).

Some methods have been proposed for image and document forgery detection based on multispectral image analysis. Multispectral cameras can capture extra information such as ultraviolet, visible, infrared and thermal ranges, which can help to detect if there exist a manipulation in images.

For example, Muhammad Jaleed Khan et al. proposed in [23] a method based on Fuzzy C-means Clustering (FCM) where they used the public available UWA Writing Inks Database. Also, Yue Zheng et al. presented in [24] a data-device hash for image forgery detection. This new device used to identify the forged areas in the image and can identify the camera source as well. They used an adjusted CASIA database in this work which is a pictures combination taken from the CASIA ITDE v1.0 and the CASIA ITDE v2.0 databases. The proposed method shows a high tamper detection rate (TDR) of 95.42%. It has also proven to be highly accurate in determining the type of camera with which the picture was taken, where, it has reached an accuracy of 99%.

### B. Active methods

Active forgery detection techniques, are considered as an image protection tool such as watermarking and digital signatures. In these methods, a known authentication code is placed in the image before transmission, and its credibility is then examined by the receiver. The negative point is its limitation, as only pre-processed images can be identified, but the main positive side is that it is more certain and more reliable than passive forgery detection techniques [4], [25].

Steganography is an active method, some works have used it for image authentication and integrity verification. It is a mean of confidential communication between a sender and a receiver. As the way this technology works is based on the idea of the sender inserting a secret message contained within a digital image called the cover image, and then after it reaches the receiver, he can extract the secret message from the image.

In 2009, Abbas Cheddad et al. [26] proposed a technique that prevents digital documents from falsification. The aim of this work was proposing new approach that is motivated by existing techniques that display security weaknesses. Using different techniques, such as the use of wavelet transform, for the purpose of developing a secret message for digital documents encryption.

In 2014, Ahmed Pahlavan Tafti et al. [27] proposed a method that uses cellular automata (CA) for the system implementation in image forgery detection, where they proposed two methods. The first scenario is about using cellular automata and Lower Upper Decomposition and the second scenario using CA and Singular Value Decomposition. Their aim of proposing this method was to prevent digital images from tampering by including an encrypted and unpredictable key into the image. For the first scenario: They have to obtain the corresponding matrix of the original image then they performed lower-upper (LU) decomposition to obtain L and U matrices. Afterwards, a statistical information has to be computed to get an Array list format. After that, they used cellular automata with a XOR local rule to embed the secret code into the LSB of each first eight pixels of the input image. The results is an image that contains the cipher key to detect image forgery. For the second scenario: They used an RGB type instead of a gray scale type that was used in the first scenario. First, they obtained the red, blue, and green matrices of input image. Afterwards, they computed the Eigen-values and the Eigen-vectors of the red and the green channels to create a feature vector (key) that was then embedded into the blue matrix. They created their own dataset using official digital document, medical images and portrait in gray scale and RGB types in png and jpeg format. The results of the proposed method were analysed using different mechanisms, such as: True and False Alert, time consumption and performance and visual quality.

Other works were focusing on protecting the copyright of the image ownership. To realise that, they used watermarking techniques.

In 2018, using the blind and non-blind watermarking technique, Dayand G.Savaka et al. [28] proposed a hybrid method that combines the two techniques. First of all, they included the blind technique in the internal watermarking. While for the external watermarking, they used the non-blind technique. To achieve that, they followed two processes. First, for the embedding process they have to embed the secret watermark into the internal cover image using DWT with the help of blind watermarking technique, and this would yield the internal watermark. Afterwards, they embed it into the external cover image using DWT with non-blind watermarking to get the Hybrid watermarked image. For watermark extraction, they have to apply the reverse operation using a secret key to extract the secret watermark. To evaluate the performance of this technique, they have used similarity measurement such as: the correlation, structural similarity (SSIM) and PSNR between the original watermark and the extracted one. The results showed that this approach is proven to be robust against noise.

### III. Discussion

In the following table TABLE I, we present a summery and a classification of the most important existing works of forgery detection. Classification is based on the used features extraction technique, the used databases, the training method, the performance measurements and the obtained results.

Most of works are on image forgery detection, for document forgery detection, we consider the documents as images. Where, particular characters are used to detect forgery such as “e” character for English and “Djim” character for Arabic (the detected characters are processed as images).

Among the 21 analysed document works, only one [19] dealt with Arabic language and no related works specific to
administrative documents that are characterised by containing text, logos, stamps and signatures.

SVM is the most machine learning technique used for forgery detection for its accuracy and because it performs well on datasets with limited number of samples. Nevertheless, recent works such as [12] use deep learning.

CASIA, COMOFOD and UCID image databases are the most used sets in this field. While, for document images there exist no existing sets yet as far as we know.

DCT and SURF are the most used techniques for feature extraction.

For performance measurements: TPR, FPR, Recall and accuracy are used to evaluate the precision of forgery detection methods.

### TABLE I. Summary of the used methods in image and document forgery detection

<table>
<thead>
<tr>
<th>Forgery detection type</th>
<th>Forgery method</th>
<th>Author(s)</th>
<th>Techniques</th>
<th>File type</th>
<th>Dataset(s)</th>
<th>Evaluation metrics</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMF</td>
<td>Beute et al. [6]</td>
<td>Colour Moments</td>
<td>Image</td>
<td>handmade</td>
<td>accuracy and false positive rate</td>
<td>0.9981 and 0.0205</td>
<td></td>
</tr>
<tr>
<td>CMF</td>
<td>Mahale et al. [7]</td>
<td>histogram of oriented gradient (HOG)</td>
<td>Image</td>
<td>COMOFOD</td>
<td>False accepted rate (FRR), False rejected rate (FRR)</td>
<td>0.82 FRR, 0.17 FPR</td>
<td></td>
</tr>
<tr>
<td>Passive</td>
<td>M. Harim et al. [8]</td>
<td>DCT</td>
<td>Image</td>
<td>CoMoFoD</td>
<td>FN/FP precision and recall</td>
<td>precision=0.52%, recall=97.89%</td>
<td></td>
</tr>
<tr>
<td>Passive</td>
<td>Xu Bo et al. [11]</td>
<td>SURF</td>
<td>Image</td>
<td>UCID</td>
<td>Scaling, Rotation, Blurring, Noise</td>
<td>97.4%, 8.6% and 9.2 sec</td>
<td></td>
</tr>
<tr>
<td>Passive</td>
<td>Bailal et al. [9]</td>
<td>SURF and FAST</td>
<td>Image</td>
<td>MICC-F220, MICC-F2000 and MICC-8mult</td>
<td>TPR, FPR and execution time</td>
<td>97.4%, 8.6% and 9.2 sec</td>
<td></td>
</tr>
<tr>
<td>Splicing</td>
<td>Tingge et al. [10]</td>
<td>LBPRC and CR</td>
<td>Image</td>
<td>CMH and CoMoFoD</td>
<td>recall, precision and F1</td>
<td>93.65%, 97.98% and 96.58%</td>
<td></td>
</tr>
<tr>
<td>Splicing</td>
<td>Ibrahim et al. [11]</td>
<td>SIFT, Fuzzy C-means clustering</td>
<td>Image</td>
<td>MICC-220 and handmade</td>
<td>FPR, FRR and time complexity</td>
<td>MICC-220 (FRR=0.99%, FPR=0.09% TPR=16min), handmade(TPR=71.69%, FPR=10.83% TPR=1h 15min)</td>
<td></td>
</tr>
<tr>
<td>Imitation</td>
<td>Justin et al. [12]</td>
<td>CNN</td>
<td>Image</td>
<td>handmade, OXFORD and UCID</td>
<td>Error rate</td>
<td>2.32%, 2.43% and 42%</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Ameni et al. [13]</td>
<td>DCT, LBP and SVM</td>
<td>Image</td>
<td>CASIA and Columbia</td>
<td>accuracy</td>
<td>97%</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Chalapathy et al. [16]</td>
<td>DCT, zernike moments and SVM</td>
<td>Image</td>
<td>CASIA</td>
<td>accuracy</td>
<td>99.5% (splicing), 87.5% (CMF)</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>Roman et al. [17]</td>
<td>Hu invariant moment, Euclidian distance</td>
<td>Document</td>
<td>handmade</td>
<td>recall and precision</td>
<td>recall=0.77, precision=0.82</td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>J. Benezet et al. [18]</td>
<td>branch-and-bound, Gaussian distribution and Bayesian formulation</td>
<td>Document</td>
<td>handmade</td>
<td>accuracy</td>
<td>99.5%</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>M. Tsai et al. [19]</td>
<td>SVM and CNN</td>
<td>Image</td>
<td>Document and handmade and benchmarked image</td>
<td>accuracy</td>
<td>99.36% for documents and 99.97% for images</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Francisco et al. [20]</td>
<td>SVM</td>
<td>Document</td>
<td>handmade</td>
<td>TPR and FPR</td>
<td>7.38% forged patches 0.05% FP ratio</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>H. Righetto et al. [21]</td>
<td>SVM</td>
<td>Document</td>
<td>handmade</td>
<td>accuracy</td>
<td>85.24%</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Shrivastava et al. [22]</td>
<td>K-means clustering, SVM and ANN</td>
<td>Document</td>
<td>handmade</td>
<td>accuracy</td>
<td>96.4%</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Muhammad et al. [23]</td>
<td>Fuzzy C-means</td>
<td>Document</td>
<td>UWA Writing Marks</td>
<td>accuracy</td>
<td>76%</td>
<td></td>
</tr>
<tr>
<td>Active</td>
<td>Yue et al. [24]</td>
<td>SURF, DCT</td>
<td>Image</td>
<td>the modified CASIA</td>
<td>TPR, TDR</td>
<td>7.5%, 95.42%</td>
<td></td>
</tr>
</tbody>
</table>

### IV. CONCLUSION

In this paper, we introduced image forgery detection, its methods and tools. We showed the most used techniques for feature extraction and training stages and we presented the most used datasets and the performance measurements for evaluation. Hence, we found that a few works are dealing with Arabic documents and only one which treated it in the same way as other languages.

This paper is considered as a survey to start a work on detecting forgery in Arabic administrative documents by analysing them and preparing a training image dataset.

### REFERENCES


