Digital administrative documents forgery detection using One-class SVM

Agti Sana
Computer science department
Université Mohamed Khider - Biskra
sana.agti@yahoo.com

Drid Abou Bakr Seddik
LESIA Laboratory
Université Mohamed Khider - Biskra
drid.abs@univ-biskra.dz

Djeffal Abdelhamid
LESIA Laboratory
Université Mohamed Khider - Biskra
a.djeffal@univ-biskra.dz

***Abstract*—In everyday life, we rely on digital documents in almost every transaction. And with the widespread use of these documents in all jurisdictions, a new crime has emerged. This is the forgery of documents using a scanner, and advanced tools for images editing that allow a simple user to alter a digital document and change its content. To prevent such a crime and to fight against fraudsters who are constantly developing new methods, many researchers have tried to develop automatic methods for fraud detection using image processing techniques and machine learning. Most of these works use the binary classification to classify documents as authentic or forged and need to use samples of the two classes together for training.**

In this work we propose a method to detect digital administrative documents forgery in cases where only authentic documents are available. The proposed method extracts background, text and stamp characteristics and build a decision model using One-class SVM. The obtained model was tested on a set of generated administrative documents using several kernel functions and parameters. Results show a high recognition rate, thus proof the effectiveness of our model.

***Index Terms*—Digital administrative document, Administrative document forgery, Machine learning, Image editing tools, One-class SVM.**

I. Introduction

Nowadays, due to the advancement of digital technology, processing software and editing tools, an image can be easily manipulated and modified. It is very difficult for humans to visually identify whether the image has been modified or not. There is a rapid increase in digitally manipulated counterfeits in the mainstream media and on the Internet. This trend indicates serious vulnerabilities and diminishes the credibility of digital images.

While these digital documents are widely used in our lives, especially in the official and commercial environment, many types of forgery have begun to appear with different techniques. These techniques are classified into three general categories: copy / move, counterfeiting and image editing [17] and mainly made on data, documents, checks, images and videos.

The forged documents are generated to illegally obtain short-term or long-term benefits. This poses a serious threat to the nation's various sectors especially juridic, economic and security.

Therefore, developing techniques to verify the integrity and authenticity of digital images is very important, especially considering that images are presented as legal evidence, information, medical documents, financial documents, or administrative documents. In this sense, the detection of image forgery is one of the main objectives of documents credibility.

Several research attempts to find a solution to the document forgery problem by constructing and proposing models, approaches and techniques for detecting forgery from documents, using a series of extracted features from a document image such as line alignments, characters in English language letters and also with some pixel properties [12], [18], [2], [5], [13].

Due to the unavailability of a public dataset for the experimentation purposes, especially the administrative documents, a considerable size of data samples must be collected for the experimental purposes.

These samples may include conference certificates, official documents, birth certificates, or academic degrees. Generally it is too difficult to collect real forged documents to use them in the learning task, and only authentic documents are available.

In this work, we propose a method to solve the problem of recognizing forged digital administrative documents, by extracting the characteristics of a scanned document images, and then learn a One-class SVM model, which will be able to automatically detect forged documents.

The reminder of this work is organized as follows: In section II, a brief overview about the digital documents and their forgery is introduced Then, in section III, some of related works are sited, then we will present the One-class SVM method principals in section IV. Section V, contains a detailed description of the proposed method followed by the experiments and obtained results discussion in section VI. Then we will end this paper by a conclusion which contains a summarization and future prospects.

II. Administrative digital documents and their forgery

Administrative documents are official and has a standard form. They are edited to establish a right, an identity (identity card, residence permit), a quality (certificate of nationality) or grant an authorization (all documents that issue permits) certificate of registration of a vehicle or driver's license, marriage certificate, etc.

A digital document has the characteristic of being on an electronic medium, of being perceptible via digital technology, it can be an image, a sound file, a set of data organized in file, an electronic writing,...etc. [6]. It is considered as a computer file (and thus represented at the base by a sequence of 0 and 1) whose content, structured according to the specifications of a file format, represents information understandable by a human and/or a computer. The forgery of a digital document is the modification of one or more of its components as the validity date, mentions of identity or on the photograph [10].

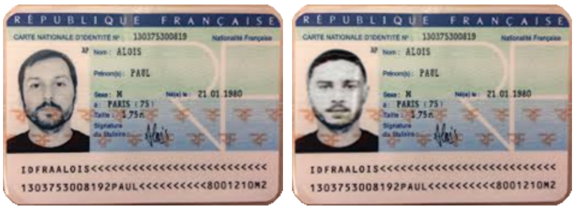
A. Forgery methods

There are many methods for making images or documents. However, in this section, we will present only the commonly used methods to falsify an authentic document. There are three types of forgery:

1) *Photo forgery:* Consist of the Id photo replacement.
2) *Text forgery:* Editing the document text in order to convert its meaning or change some of its informations.
3) *Stamp/signature forgery:* Consists of copying the existing stamp or signature into an authentic document in the forged document. [3].

Digital images are easy to manipulate and modify due to the availability of powerful image processing and editing software. There are many types of image forgery:

- **Copy and paste:** In this technique, it must cover part of the image to add or delete information. In the Copy-Move image technique, a part of the same image is copied and pasted into another part of that image itself. In a copy attack, the intention is to hide something in the original image with another part of the same image [17].



(a) (b)

Fig. 1. Copy-paste forgery example.(a) original image (b) forged image.

- **Image Splicing:** It is an image composition technology by combining image fragments from the same images or different images using available digital tools such as Photoshop.
  Falsifying the image involves composing or fusing two or more images that significantly alter the original image to produce a forged image. In the case where images with a different background are merged, it becomes very difficult to create the borders. Detection of splicing is a difficult problem by which composite regions are studied by a variety of methods. Abrupt changes between the different areas that are combined and their backgrounds provide valuable traces for detecting splicing in the image considered [11].
- **Image retouch:** In digital image editing, the images are less modified. This improves some features of the image. The image is made to reduce or improve certain characteristics of the image. Retouching may require rotating, scaling, or stretching an image before combining it with another image. This is a very common type of image change and is often advertised. Cloning of the part of the image is also very common in image editing. The detection is very difficult because there is no radical change in the different parts of the image [11].
- **Imitation**
  The fraudster adds or replaces information by trying to find the same font properties of a document. As a result, the final forged digital document contains words with different font type, font size, misalignment, etc. [14].
- **State of the lighting:** This type of fake can be done easily by splicing together two different images. Often, the spliced images come from different scenes and have different lightning conditions and so it is very difficult for the image forging to match the exact lightning state of one image with the other. Such variation in lighting conditions can be used to identify quenching in the image. Many times, the splicing of the image is done with such precision that it is obviously impossible to identify different lightning conditions in the combined image. Since the direction of the light source can be estimated for different objects / people in an image, inconsistencies in the sense of illumination can be used as evidence of numerical alteration. [11] .
- **Cropping:**
  Cropping is a technique for cutting borders or removing a peripheral portion of an image. Generally, this type of operation is used to delete the border information that is not very important for the display or to adapt it to a use other than that for which it was made, or to modify its format [3].

III. Related works

A large number of researches in the literature was proposed to deal with the image forgery problem. However, only a few of them are related to the document forgery texts. In what follows, we will cite some of those works, and try to classify them according to the methods, techniques and features they have followed.

Gebhardt et al. [8] have proposed a system for detecting differences in the edges of printed characters. They created a dataset with 1200 document images by 7 inkjet printers and 13 different laser printers. Then they recorded the characteristics of each printer to clarify the properties of the edges of the letters and then look for different letters to distinguish them in the document to show the suspicious letters. The whole process they used was divided into two main stages: the first stage is the extraction of features, and the second is the detection of anomalies.

Christoph H et al. [4] proposed in 2010 a classification system to analyze the printing technique used to print a document. Each letter of the document is classified using a carrier vector machine that has been trained to distinguish laser impressions from inkjet. A color-coded visualization helps the user to interpret the classification results by letter. The proposed approach was used to detect fraud using a letter classification of the printing technique. It is based on the fact that each printer has its own visual characteristics in printed characters, especially in the border areas of the letters. From the distribution of gray levels in this image area, a decision can be made for each letter in the document about the type of printer created it. The method does not require specific hardware but can work with a standard consumer imaging device such as a scanner or digital camera.

Shize Shang et al. [16] proposed in 2014 a method for distinguishing documents produced by laser printers, inkjet printers and electrostatic copiers. The approach makes it possible to distinguish the documents produced by these sources according to the characters of the document. The use of separate characters can also detect and locate forgery of documents created using different types of tools.

Romai Bertrand et al. [14] introduced in 2012 a method that can automatically detect manufacturing based on the characteristics of certain character-level documents. This method is based on the detection of aberrant characters in a discriminant feature space and the detection of strictly similar characters. They calculated a set of characteristics for all the characters. Then they ranked the character so false or true based on a distance between characters of the same class. The method uses intrinsic document functions. It is based on two forgery techniques for the detection of a fraudulent character: "Copy and Move" and "imitation".

Beusekom et al. [9] proposed in 2010 an approach to examine the intrinsic characteristics of documents for the security of optical documents, the purpose was to automatically detect lines of text manipulated or inserted in a document by inspecting their alignment (left, right or center) with respect to other lines of the document text. This is an additional feature in order to develop a powerful toolbox for automatic document inspection. They used the extracted lines of text and alignment margins. The statistics on the distances between the lines of text and the margins of alignment serve to identify the lines that could have been forged.

Fadi H. et al. [7] proposed in 2015 a new method to detect the manufacture of text in scanned documents, it involves two steps. The first one undergoes four process, which are used to pre-process and extract the document characteristics for the next step. The second step, contains the fifth process, it aims to extract the edge gradient to find the difference between original and forged text. The final process is the coloring and location of suspicious pixels.

Ramzi M. Abed [1] proposed in 2015 a new technique for detecting altered scanned documents. This technique is based on identification of the used scanner by the meaning of its intrinsic characteristics. The proposed system begins by extracting, from a scanned document, all the letters "e" in the document, as it is the most common letter in the English language (their system has been proposed for English documents). Then, the system extracts a set of features from each character group "e", and then forms a feature vector for them by dividing the scanned document tested into blocks. A different set of features is extracted for each of these blocks. Each of these feature vectors was then separately tested and categorized using the Support Vector Machine (SVM) classifier, which ultimately decides whether the scanned document image being tested is authentic or altered.

H. Benhamza et al. [3] proposed in 2017 a method for the detection of forged administrative digital documents using binary support vector machines. The aim of the work was to study the nature of scanned images and the methods used for their forgery, then to propose techniques allowing the detection of forged documents based on rules obtained through machine learning.

To conclude, the previous works are based on the following topics: tamper-proofing and detection techniques by extracting different characteristics of the document based on printer footprint, paper, scanner, characters, or pixel properties.

Although, many of these techniques are very promising and innovative. However, they all have some limitations, such as unsupported oriental languages (as Arabic, Chinese, etc.), and low accuracy when dealing with documents which have submitted only a little forgery, also the restriction on a particular language (English), or conviction of a document from a single character.

IV. One class SVM

In binary and multiclass support vector machines (SVM), we always have positive examples and other negatives, i.e. examples and counterexamples. Such information is not available in all application cases. Sometimes it is very expensive, if not impossible, to find counterexamples that really represent the negative class.

Take the example of recognition of a particular category of parts by a robot in a factory, it is easy to have sufficient examples of this piece, but it is difficult to have examples of all the different parts. In such cases, it is desirable to have a decision model that recognizes as many possible examples of this category and rejects all others. This problem is often called novelty detection, since the decision model knows a set of examples and detects all that is new (strange).

For the one class SVM classification, it is assumed that only the data of the target class is available. The goal is to find a boundary that separates the examples of the target class from the rest of the space, in other words, a boundary around the target class that accepts as many target examples as possible. This boundary is represented by a positive decision function inside the class and negative outside. Figure 2 represents, in two dimensions, a case of separation of a class from any other class.

To solve this problem, the single-class SVM technique uses the same binary model with an extra trick; the origin of the space is considered to be the only instance of the negative class. the problem lies, therefore, in finding a hyperplane that separates the examples of the target class from the origin, and which maximizes the margin between the two [15].

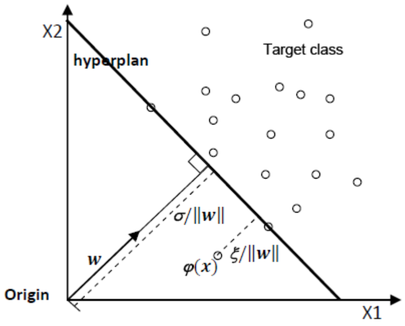


Fig. 2. One class SVM at maximum margin.

The problem is modeled by the primal problem of quadratic programming as following: Let $X = \{x_1, x_2, ..., x_n\}$ be our data set, in order to define the domain of novelty, we have to learn an optimal hyperplane which can can separate the data samples from the origin such that the margin is maximized. This optimization problem is formulated as follows:

$$max_{w,b}(\frac{|b|}{\|w^2\|})$$

subject to:

$$y_i(w^T\phi(x_i) - b) \geq 0,\ i = 1, 2, ..., N$$

Where ϕ is a transformation from the input space to the feature space and $w^T\phi(x) - b = 0$ is equation of the hyperplane. After using Lagrangian and some transformations, we get the following dual problem:

$$min_\alpha \sum_{i,j} \alpha_i\alpha_j k(x_i x_j) - \sum_i (x_i x_j)$$

subject to.

$$0 \leq \alpha_i \leq \frac{1}{\nu N}$$
$$\sum_i \alpha_i = 1$$

Where $k(x_i x_j)$ is the used kernel function and parameter $\nu \in [0, 1]$ allows to control training errors [15].

V. Proposed Method

Our proposed forgery detection system undergoes two main steps, training and use, see Fig. 3. However, these two steps depends on a vector which contains the image's characteristics, and constructed in the preprocessing step as following:

A. Preprocessing

- Acquisition of a digital document and converting into gray-scale and then filtering it by a median filter to reduce noise.
- Extract background characteristics by:
  1) Divide the image into blocks of the same size,
  2) Calculate the average and frequent color of each block,
  3) Calculate the average and frequent color of the image's background,
- Detect the stamp area in the image and calculate its information by :
  1) Determine the stamp area by detecting the blue or red color in the color image,
  2) Convert the selected stamp area to grayscale,
  3) Calculate the first and second frequent color in the stamp area to determine the background color of the stamp as the second most common color,
  4) Calculate the average color of the stamp area,
- Detect the text area and calculate its information by:
  1) Delimitation of the text area by detecting the color of the image text,
  2) Cut text into image blocks representing syllables or words delimited by detected empty lines and columns,
  3) Calculate the first frequent color of each block and the second one as the background color
  4) Calculate the average color of each block,
- Combine all previous obtained information to build the features vector,
- Apply the previous steps on all scanned documents to build a features database for authentic documents,
- Train the One-class SVM model based on built features,
- Construction of a decision model and its test,
- Use of built model for the detection of forged documents.

N.B. Text analysis step makes possible to check the homogeneity of the text color, because its intensity represents an important factor, which affects the coherence and the homogeneity of words in the text. We noticed that the original words and characters intensity is very different from their intensity when added by an image or text processing tools. This is because the color of the original characters is influenced by the characteristics of the printer and scanner used in their creation.

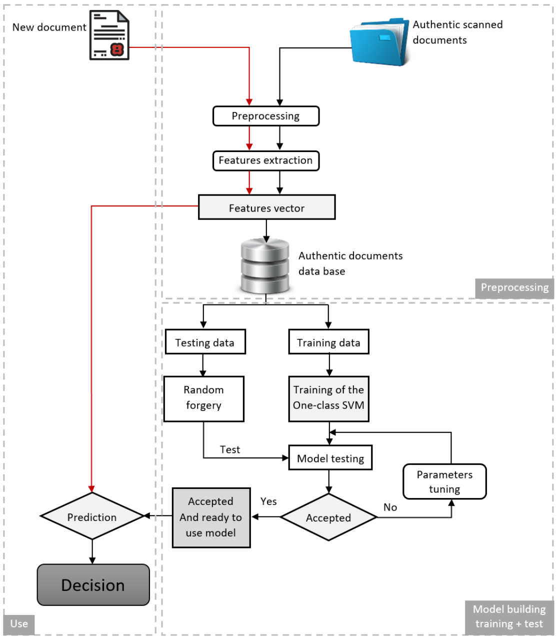


Fig. 3. Design of the model construction phase.

The obtained vector is composed of the characteristics acquired from the three main parts of an administrative document, the background, the stamp and the text.

a) Characteristics extracted from the background:

- The average and frequent color of each block in the image.
- The average and frequent color of the background of the image.

b) Characteristics extracted from the stamp:

- The first frequent color of the stamp area (the color of the stamp background)
- The second frequent color of the stamp area (the color of the stamp).
- The average color of the stamp area.

c) Characteristics extracted from the text:

- The first and second frequent color of each word / character in the image.
- The average color of each word / character.

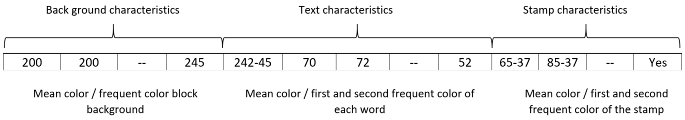

Back ground characteristics
Text characteristics
Stamp characteristics
200
200
--
245
242-45
70
72
--
52
65-37
85-37
--
Yes
Mean color / frequent color block background
Mean color / first and second frequent color of each word
Mean color / first and second frequent color of the stamp

Fig. 4. Features vector of a document.

We built our data base from all vectors constructed by repeating the previous process with the acquired images. We forged some of these images before constructing the corresponding vector in the purpose to use them only in the testing step.

B. Training phase

In this phase, the system learns from the training data whose membership is known in advance (authentic). The obtained model is then tested on the test data to verify its validity. The model that detects forged documents among authentic ones at higher rate will be adopted and used later in the use phase.

C. Use phase

In the use phase, we must go through all the previous steps except the learning step where we start to import an administrative document and extract all its features to build a feature vector. Finally, the registered template is used to decide the authenticity of the document.

VI. Experiments and Results

To test the effectiveness and performance of our proposed method, we passed it throw three tests, with different parameters and attributes. We used WEKA 3.8 software with the package 'libsvm' and One-class SVM as SVM type with a 10-Cross validation test option.

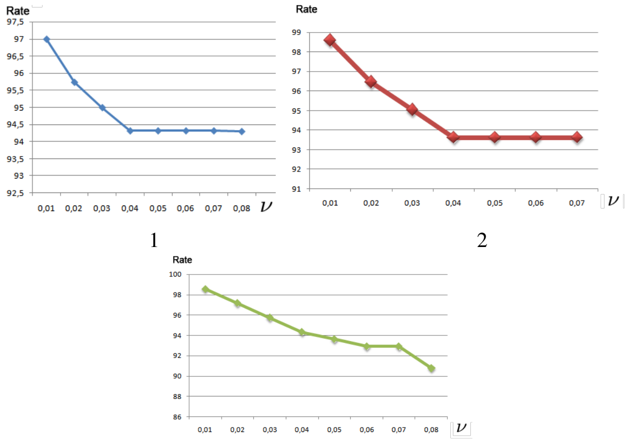
To the best of our knowledge, general public dataset for document forgery detection doesn't exist. That is due mainly to confidential nature of documents and their inclusion of sensitive information. For these reasons, we constructed our test database by scanning 141 administrative documents including invitations, certificates and reports. We tested our methods in three experiments representing cases of dividing images into 3x3, 4x4 and 5x5 blocs.

The obtained results according to kernel type in each experiment are given in the following table.

Kernel type	1^{st} experiment (3x3)	2^{nd} experiment (4x4)	3^{rd} experim
Linear	95.74	98.58	97.8
Polynomial	97.87	98.58	98.5
Radial basis function	94	43.26	86.5

TABLE 1
Obtained Recognition rate of three experiments for three kernel types

The influence of parameter ν on recognition rate is shown in the following figure:



1

2

3

Fig. 5. The effect of the ν value on the recognition rate

VII. Discussion of Results

The results presented on table 1 show that the best recognition rate is obtained using polynomial kernel and a subdivision of images into more than 3x3 blocs. The superiority of the polynomial kernel is due to the geometric form of features vectors of authentic documents in original space. Also, the superiority of 4x4 and 5x5 blocs subdivisions is due to that a small number of blocks gives blocks of large dimensions which reduces the importance of small details.

The influence of parameter ν on recognition rate represented in figure 5 shows that a small value (0.01) gives better recognition rate in the three experiments and indicates that used samples can be well separated without need to allow important number of errors.

For comparison to other works, we can say that our method has the advantage to use only authentic documents for training and doesn't need to use forged documents that might be difficult to get with sufficient number.

Despite that we compared our proposed method to some others in literature based on used documents type for training and on obtained recognition rate . It was clear that our method overcomes those methods. The following table 2 shows comparison results.

Method	Used samples	Accuracy (%)
Cruz et al. [5]	Authentic and forged	89.65
Pun at al. [13]	Authentic and forged	91.56
Ramzi M. [1]	Authentic and forged	90
Benhamza et al. [3]	Authentic and forged	80
Our method	Forged	98.5

TABLE 2
COMPARISON WITH OTHER METHODS

Through all our experiments and results, we can say that our proposed method is very effective in detecting fraudulent documents. The results show it's ability to correctly identify more than 98% of documents using one class SVM, thereby speeding up the document verification process automatically.

VIII. Conclusion

With the increasing use of digital documents, their forgery has become one of the most well-known crimes. To overcome this crime, we have studied several related works and their methods and techniques for the detection of forged digital documents.

In order to fight against forgery and to cope with the spread of this crime, we have proposed a method based on automatic learning by the One-class SVM method by using some image's characteristics of the document concerning the background, the text, and the stamp.

To carry out our work, we extracted these characteristics from all available authentic administrative documents.

We recorded the extracted features in a database and used them to build a decision template to recognize forged documents from authentic ones.

To validate our proposed method, we have prepared a training database of 141 samples representing authentic administrative documents. The best recognition rates obtained on these data exceed 98%, which is encouraging and disproves the effectiveness of the proposed method over other existing methods.

For future work, we suggest some ideas that can improve our system such as:

- Try to process stamps and logos in documents with text to test all components of documents.
- Try to extract other features from the document to improve system performance.
- Work on the processing and analysis of properties in other administrative documents such as passports, identity cards, etc., to generalize the use of the system.

References

[1] Ramzi M. Abed. Scanned documents forgery detection based on source scanner identification. *American Journal of Information Science and Computer Engineering*, 2015.

[2] Hesham Ahmed Alberry, Abdelfatah Hegazy, and Gouda i Salama. A fast sift based method for copy move forgery detection. *Future Computing and Informatics Journal*, 2018.

[3] H. BENHAMZA and A. DJEFFAL. Détection des faux documents administratifs par machines à vecteurs supports. *Fifth International Conference on Image and Signal Processing and their Applications, University of Abdelhamid Ibn Badis, Mostaganem, Algeria*, 3rd - 4th December 2017.

[4] Lin Mei Christoph H. Lampert and Thomas M. Breuel. Printing technique classification for document counterfeit detection. *German Research Center for Artificial Intelligence (DFKI)*, 2010.

[5] Francisco Cruz, Nicolas Sidere, Mickaël Coustaty, Vincent Poulain D'Andecy, and Jean-Marc Ogier. Local binary patterns for document forgery detection. In *Document Analysis and Recognition (ICDAR), 2017 14th IAPR International Conference on*, volume 1, pages 1223–1228. IEEE, 2017.

[6] Michel Gorin. Le numérique: impact sur le cycle de vie du document. premier colloque ebsi-enssib du 13 au 15 octobre 2004, montréal (québec). *RESSI*, (1), 2005.

[7] Fadi H. Naser Hasan. *New Method to Detect Text Fabrication in Scanned Documents*. Master thesis, Gazza University, 2015.

[8] Faisal Shafait Johann Gebhardt, Markus Goldstein and Andreas Dengel. *Document Authentication using Printing Technique Features and Unsupervised Anomaly Detection*. German Research Center for Artificial Intelligence, School of Computer Science and Software Engineering, The University of Western Australia.

[9] Faisal Shafait Joost van Beusekom and Thomas M. Breuel. Document inspection using text-line alignment. *German Federal Ministry of Education and Research*, 2010.

[10] Aurélien langlade. Éléments de connaissance sur la fraude aux documents et à l'identité en 2014, annual report. 2015.

[11] VV Nath, GKS Gaharwar, and RD Gaharwar. *Comprehensive study of different types image forgeries*. IJSTM, 2015.

[12] Choudhary Shyam Prakash, Avinash Kumar, Sushila Maheshkar, and Vikas Maheshkar. An integrated method of copy-move and splicing for image forgery detection. *Multimedia Tools and Applications*, pages 1–25, 2018.

[13] Chi-Man Pun and Jim-Lee Chung. A two-stage localization for copy-move forgery detection. *Information Sciences*, 2018.

[14] Oriol Ramos Terradesy Romain Bertrand, Petra Gomez-Kramer. A system based on intrinsic features for fraudulent document detection. *Computer Vision Center, Universitat Autonoma de Barcelona*, 2012.

[15] Bernhard Scholkopf and Alexander J Smola. *Learning with kernels: support vector machines, regularization, optimization, and beyond*. MIT press, 2001.

[16] Shize Shang, Nasir Memon, and Xiangwei Kong. Detecting documents forged by printing and copying. *EURASIP Journal on Advances in Signal Processing*, 2014(1):140, 2014.

[17] Prof. Dr. Ajay A. Gurjar Snigdha K. Mankar. Image forgery types and their detection: A review. *International Journal of Advanced Research in Computer Science and Software Engineering*, 5(4), 2015.

[18] Nor Bakiah Abd Warif, Ainuddin Wahid Abdul Wahab, Mohd Yamani Idna Idris, Roziana Ramli, Rosli Salleh, Shahaboddin Shamshirband, and Kim-Kwang Raymond Choo. Copy-move forgery detection: survey, challenges and future directions. *Journal of Network and Computer Applications*, 75:259–278, 2016.