



HAL
open science

Crossing number features: from biometrics to printed character matching

Pauline Puteaux, Iuliia Tkachenko

► **To cite this version:**

Pauline Puteaux, Iuliia Tkachenko. Crossing number features: from biometrics to printed character matching. IWCDF 2021 - 3rd International Workshop on Computational Document Forensics, Sep 2021, Lausanne, Switzerland. pp.437-450, <10.1007/978-3-030-86198-8_31>. <hal-03335687>

HAL Id: hal-03335687

<https://hal.science/hal-03335687v1>

Submitted on 6 Sep 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



HAL Authorization

Crossing number features: from biometrics to printed character matching

Pauline Puteaux¹ and Iuliia Tkachenko²

¹ LIRMM, Université de Montpellier, CNRS, Montpellier, France
pauline.puteaux@lirmm.fr

² LIRIS, Université Lumière Lyon 2, CNRS, Lyon, France
iuliia.tkachenko@liris.cnrs.fr

Abstract. Nowadays, the security of both digital and hard-copy documents has become a real issue. As a solution, numerous integrity check approaches have been designed. The challenge lies in finding features which are robust to print-and-scan process. In this paper, we propose a new method of printed-and-scanned character matching based on the adaptation of biometrical features. After the binarization and the skeletonization of a character, feature points are extracted by computing crossing numbers. The feature point set can then be smoothed to make it more suitable for template matching. From various experimental results, we have shown that an accuracy of more than 95% is achieved for print-and-scan resolutions of 300 dpi and 600 dpi. We have also highlighted the feasibility of the proposed method in case of double print-and-scan operation. The comparison with a state-of-the-art method shows that the generalization of proposed matching method is possible while using different fonts.

Keywords: Printed document · Feature extraction · Print-and-scan process · Crossing numbers · Matching method.

1 Introduction

Due to the broad availability of professional image editing tools, cheap scanning devices and advancements of high-quality printing technologies, there is a high need in fast, reliable and cost-efficient document authentication techniques. The actual pandemic situation forces the people and the administrative centers to use digital copies of hard-copy documents. The official hard-copy documents have specific security elements that can be efficiently used for document authentication as moiré patterns, holograms, or specific inks [24]. Nevertheless, the digital copies of such documents can be easily tampered using some image editing tools (like Photoshop or Gimp) [2] or using some novel deep learning approaches [18,27,28]. That is why, there is a high need of designing efficient and robust solutions for printed-and-scanned document integrity check.

For described situations, we need to work with the documents in two formats (hard-copy and electronic soft-copy). This type of documents is called hybrid

documents [6]. For hybrid documents, the integrity check must work identically for both soft-copy and hard-copy documents. That means that if the document was printed and captured several times without tampering, the document integrity check should label this document as authentic.

One of the first hybrid protection system was presented in [25]. There was proposed to construct the hash digests for the text in electronic and printed documents. The technique based on the use of Optical Character Recognition (OCR) software and a classical cryptographic message authentication code gave a good performance. Later it was shown that the OCR software cannot give us stable results due to Print-and-Scan (P&S) process impact [8,22].

In this paper, we do not want to improve the accuracy and stability of OCR methods, we would like to find some features extracted from character skeletons that can be robust to P&S impact and used for character representation. These features are then matched with a template in order to identify a character. We consider this work as a first step for the construction of text fuzzy hash that can then easily be stored in a high capacity barcode and integrated to documents (or stored in a database) as a document representation.

The rest of the paper is organized as follows. We introduce the existing document authentication methods and the impact of P&S process to hard-copy and printed-and-scanned documents in Section 2. The proposed feature extraction method as well as the proposed matching methods are presented in Section 3. We show the experimental results in Section 4. Several future paths are discussed in Section 5. Finally, we conclude in Section 6.

2 Challenges of printed document protection

There exist several approaches for hard-copy document authentication. The first one is a forensics approach that aims at identifying the printer and scanner [4] that were used to produce a given hard-copy document and its scanned version. Here, some specific features are extracted from the printed characters according to different techniques as gray-level co-occurrence matrix [13,14], noise energy, contour roughness and average gradient of character edges [19]. These features are then classified using different machine learning methods (LDA, SVM, *etc.*) in order to identify the printer. In the last few years, some forensics methods based on deep learning appear [9,15]. In [15], authors presented human-interpretable extensions of forensics algorithms that can assist to human experts to understand the forensics results. This approach cannot be used for hybrid document authentication as we cannot control the printer and scanner used, and thus, the forensics features cannot ensure the authenticity of a hybrid document.

The second approach aims to add a specific copy-sensitive code to the document that is used to detect unauthorized duplication of the document [17,23]. These solutions take an advantage of the stochastic nature of Print-and-Scan (P&S) process. Nevertheless, these copy sensitive codes can only make the difference between first print and all other re-prints of the document. Thus, this approach cannot be also extended to hybrid document authentication. However, if such

code has a high storage capacity as [23], it could be used for document hash storage.

The third approach works with hybrid documents [6]. The contributors of this approach introduce the term of stability in the document processing domain. The main idea of this approach is to separate the document into primary elements as images [5], text [8], layout [7] and tables [1], and to represent these elements by stable features. These stable features are unchanged when the document is printed-and-scanned using different resolutions.

The text integrity check can be done by another approach that consists of the construction of document hash using the specific feature code extracted from each character [21]. The authors show that the proposed solution can resist to affine transformations, JPEG compression and low-level noise, but is not robust to median filtering. Specific features based on character skeleton can also be used for character recognition [12]. The authors reported the recognition results comparable with those obtained by the deep learning approach. In [22], the authors suggest to use the PCA for character feature extraction and a minimal euclidean distance for character recognition. The main problem of this approach is the extraction of correct bounding boxes and stable features as a P&S process impacts to the shape and color of the printed characters. In addition, this machine learning based method cannot be generalized, thus it is necessary to re-train the model for each font type.

The images after P&S process are affected by noises, blur and other changes [20,29]. Therefore, the P&S communication channel is always characterized by loss of information. The loss could be minimal and imperceptible by the naked eye, but it is significant for authentication test or integrity check.

When the soft-copy document is printed and scanned, some noise is added by the printer and the scanner. Therefore, if a hard-copy document was scanned and re-printed, it suffers from double impact of the P&S process. In general case, the document can be scanned and reprinted several times. Nevertheless, the most realistic situations are: 1) one P&S operation - when the soft-copy was printed and then scanned or captured with a camera by a person before sending to authority center; 2) double P&S - when the hard-copy was scanned and then reprinted by an authority center (or a person). That is why, in this paper, we work with characters printed once (P&S) or printed twice (double P&S).

3 Proposed method

When a hard-copy document is scanned several times, each time a slightly different document image is obtained [31] due to the optical characteristics of captured devices. The similar problem can be found in biometrics: we know that the enrolled fingerprint has several differences with the stored fingerprint template. In this work, we want to adapt the biometrical features for character feature extraction and matching with a template.

3.1 Pre-processing operations

The pre-processing steps of fingerprint matching process consists of binarization and thinning (or skeletonization) processes. As a P&S process impacts a lot to the character shape, we need to apply some morphological operations before the binarization step in order to fill the holes (appeared due to the inhomogeneous spread of ink during printing or quantization and compression operations during scanning). In this paper, we do not focus on the search of the best pre-processing operations, we use 1) the opening operation to correct possible errors of P&S process, 2) the classical Otsu's binarization method [16] and 3) the classical thinning method based on medial axis transform [11].

3.2 Feature extraction

The feature extraction is done from the skeleton image of a character, in digital (during the template construction phase) or printed-and-scanned form.

We analyze pixels of the binary image considering their neighborhood. Two pixel values are possible: 0 for black and 1 for white (the skeleton is represented by white pixels). In order to extract significant feature points, we compute the crossing numbers [30]. For each pixel, the associated crossing number is defined as half of the sum of differences between two adjacent pixel values. Depending on the value of its associated crossing number (CN), five pixel types can be defined, as presented in Fig. 1.

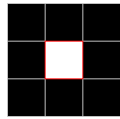
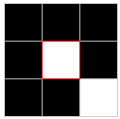
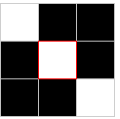
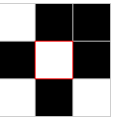
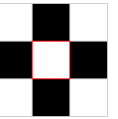
CN = 0	CN = 1	CN = 2	CN = 3	CN = 4
Isolated point	Ending point	Connective point	Bifurcation point	Crossing point
				

Fig. 1. Five pixel types as a function of their associated crossing number (the centered pixel framed in red is the pixel of interest).

In biometrics, only ending and bifurcation points are generally considered for minutia extraction from fingerprint. However, in the case of printed characters, it should be interesting to consider isolated and crossing points in addition. Indeed, isolated points should be relevant for characters 'i' and 'j' and crossing points for 'x'.

Furthermore, for some characters, serifs can be present. A serif is a small line or stroke attached to the end of a longer stroke in a character. They can induce the extraction of additional feature points. Indeed, in case of serif, there are

a bifurcation point and one or two close ending points. These last extracted features are not significant. Therefore, we propose a smoothed version (S) of the feature extraction step consisting to remove these ending points from the feature point set. In addition, the serifs are not presented in all kinds of fonts, so the smoothed version of features is more adapted for generalization of the matching methods.

In order to perform the smoothing operation, we compute the euclidean distance between a bifurcation point and each extracted ending point. If this distance is lower than the threshold th , the ending point is considered as being part of a serif and is then removed from the feature point set. Note that the value of the threshold th is experimentally fixed and depends on the template database. The practical interest of this smoothing operation is illustrated in Section 4.2 and Fig. 4.

3.3 Template matching

In order to compare a printed-and-scanned character with the digital template, we suggest to test three different matching methods:

- M_1 : For each feature point extracted from the printed-and-scanned character, we are looking for the closest (in terms of euclidean distance between coordinates) reference point in the template of digital character. Therefore, two extracted feature points can be associated to the same reference point. We then average the distances computed for each extracted feature point.
- M_2 : For each reference point in the template of digital character, we are looking for the closest (in terms of euclidean distance between coordinates) feature point extracted from the printed-and-scanned character. We then average the distances computed for each reference point.
- M_3 : Same as M_1 , but we only consider the reference points which have the same crossing number type as the extracted feature point to compare. Moreover, we focus on template of digital characters which have approximately the same number of reference points as the number of extracted features from the printed-and-scanned character (equal numbers ± 2).

The template of digital character which has the smallest difference score with the printed-and-scanned character allows us to find the associated letter in the alphabet. The performances with each of these methods are discussed in Section 4.

4 Experimental results

In this section, we present the database used and the pre-processing steps done. Then, we show the extracted features for matching and we discuss the results obtained for character images printed-and-scanned once with 300 dpi and 600 dpi resolutions.

4.1 Database description

In our database³, we have 10 images per low-case character with Times New Roman font, that gives us in total 260 images per P&S resolution. All images are of size 100×100 pixels with a character centered in the image. For images printed-and-scanned with 300 dpi, we apply the $\times 2$ resize function before centering these characters in the images. We illustrate some images from our database in the Fig. 2. We can notice that there exist small imperfections for characters printed with 300 dpi in comparison with those printed with 600 dpi or digital sample. In addition, the printed characters are in grayscale. Thus, we need to do some pre-processing before the skeleton extraction process.

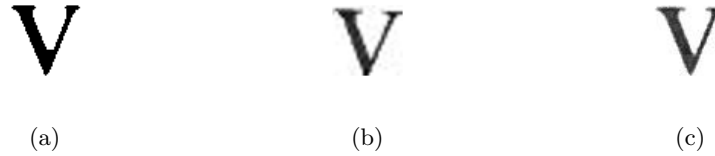


Fig. 2. The letters from our database a) digital sample, b) sample printed and scanned with 300 dpi, c) printed and scanned with 600 dpi.

After several experiments, we have found that the best results for our database are obtained using an open morphological operation with square structural element of size 3×3 . After this operation, the character color is more homogeneous and the binarization process works better. We binarize the characters using classical Otsu's binarization. After the binarization, the skeletonization is done using the build-in Matlab function (*bwskel*) that uses the medial axis transform based on thinning algorithm introduced in [11]. This function uses 4-connectivity with 2-D images and gives us sufficient results for character skeleton extraction. Examples of skeletons extracted using this function are illustrated in Fig. 3.

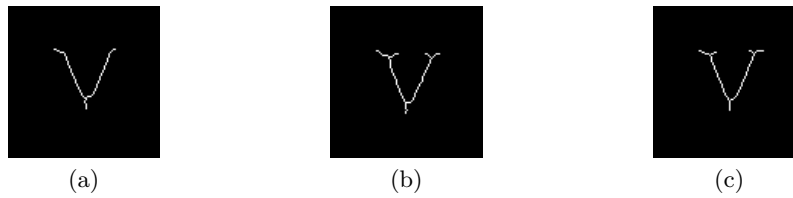


Fig. 3. The skeletons extracted from characters a) digital sample, b) sample printed and scanned with 300 dpi, c) printed and scanned with 600 dpi.

³ The database is available on demand. Contact: iuliia.tkachenko@liris.cnrs.fr

From Fig. 3, we notice that the skeleton is less noisy in the case of digital sample and a sample printed and scanned with 600 dpi. In addition, several strokes detected in samples Fig. 3.b-c are not present in the template (Fig. 3.a). Therefore, we have decided to compare the proposed matching methods using non-smoothed and smoothed features.

4.2 Feature extraction

The comparison of non-smoothed and smoothed features is illustrated in Fig. 4. We present the extracted features from the skeletons of both digital and printed and scanned with 600 dpi versions of the 'v' character. The feature points are displayed in red for a better visualization. Moreover, each point coordinates and type are also indicated. From the skeleton of the digital character, we extract four feature points: one bifurcation point (CN = 3) and three ending points (CN = 1). From the skeleton of the printed-and-scanned character, the number of feature points is bigger. Indeed, there are three bifurcation points and five ending points. However, due to the presence of serifs, some feature points are not relevant for comparison and matching. Using the smoothing operation described in Section 3.2 with a threshold $th = 15$ according to our experiments on the template database, they are removed from the feature point set. One can then note that, after this operation, the same number of feature points is obtained for the digital character and the printed-and-scanned version. In addition, we can remark that their coordinates are quite close from each others, which is an important property to ensure a good match.

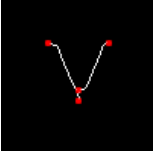
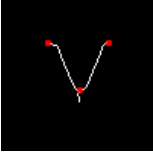
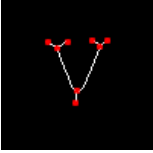
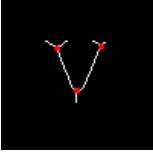
Non-smoothed	Smoothed
Digital (template)	
	
$[(28, 30, 1), (28, 70, 1), (60, 51, 3), (67, 51, 1)]$	$[(28, 30, 1), (28, 70, 1), (60, 51, 1)]$
P&S 600 dpi	
	
$[(28, 29, 1), (28, 43, 1), (28, 60, 1), (29, 68, 1), (31, 65, 3), (32, 36, 3), (61, 49, 3), (68, 49, 1)]$	$[(32, 36, 1), (31, 65, 1), (61, 49, 1)]$

Fig. 4. Example of skeleton extraction and crossing number extraction.

4.3 Character matching

For character matching experiments, we have constructed a database with 26 templates of digital characters. These templates are used during the matching process in order to recognize 260 character images printed-and-scanned with 300 dpi resolution and 260 character images printed-and-scanned with 600 dpi resolution. We do not test the matching methods with digital characters as they always have the same features and, thus, they are always correctly recognized.

Table 1 shows the results obtained for each letter while the characters were printed-and-scanned with 300 dpi resolution. A big number of characters are matched correctly in 100% of cases even if we use non-smoothed features (see rows M_1, M_2, M_3 in Table 1). Nevertheless, for some characters, the use of smoothed features significantly improves the matching results (for example, for letters 'k', 'm', 'v'). The smoothed features improve the results for the characters that have additional strokes in the end points. In general, we can make the conclusion that the matching method M_3 with smoothed features gives us the best matching results. This is proved by the mean values shown in Table 2 (Pre-processing 1). Indeed, we see that the mean correct matching rate for characters printed-and-scanned with 300 dpi resolution, obtained with SM_3 method, is equal to 95%.

	a	b	c	d	e	f	g	h	i	j	k	l	m
M_1	1	0.9	1	1	0.9	1	1	1	1	0.8	1	0.5	1
M_2	1	0.9	1	1	1	1	1	0.1	0.8	1	0.5	0.8	0.7
M_3	1	0.9	1	1	0.9	1	1	0.4	1	0.8	0.9	0.5	0.5
SM_1	1	0.9	1	1	0.9	1	1	1	0.9	0.8	1	0.5	1
SM_2	1	0.9	1	1	1	1	1	0.1	0.7	1	0.1	0.5	0.7
SM_3	1	0.9	1	1	0.9	1	1	1	0.9	0.8	1	0.5	1
	n	o	p	q	r	s	t	u	v	w	x	y	z
M_1	1	1	1	1	1	0.8	1	1	0.1	1	1	1	0.9
M_2	1	1	1	1	1	0.8	1	1	0.5	0.6	1	0.9	0.9
M_3	0.3	1	1	1	1	1	1	1	0.1	1	1	0.8	0.9
SM_1	1	1	1	1	1	0.8	1	1	1	1	1	0.8	0.9
SM_2	1	1	1	1	1	0.8	0.7	1	0.7	0.9	0.9	0.8	0.7
SM_3	1	1	1	1	1	1	1	1	1	1	1	0.8	0.9

Table 1. Character matching rates using different crossing number comparison techniques (P&S 300 dpi).

Fig. 5 illustrates the results obtained for each letter while the characters were printed-and-scanned with 600 dpi resolution. From these results, the same conclusions can be done: the matching method M_3 with smoothed features (SM_3) gives us the best matching results. The mean correct matching rate with SM_3 method is equal to 97.31% from Table 2 (Pre-processing 1). We can conclude that the proposed feature extraction and matching methods work better for these

images as the resolution and, thus, the image quality are higher. We only need to improve the results for letters 'b', 'e', 'o' and 'z' by adjusting the skeletonization step. These results are very promising and show us that we can extract stable features and construct a text hash.

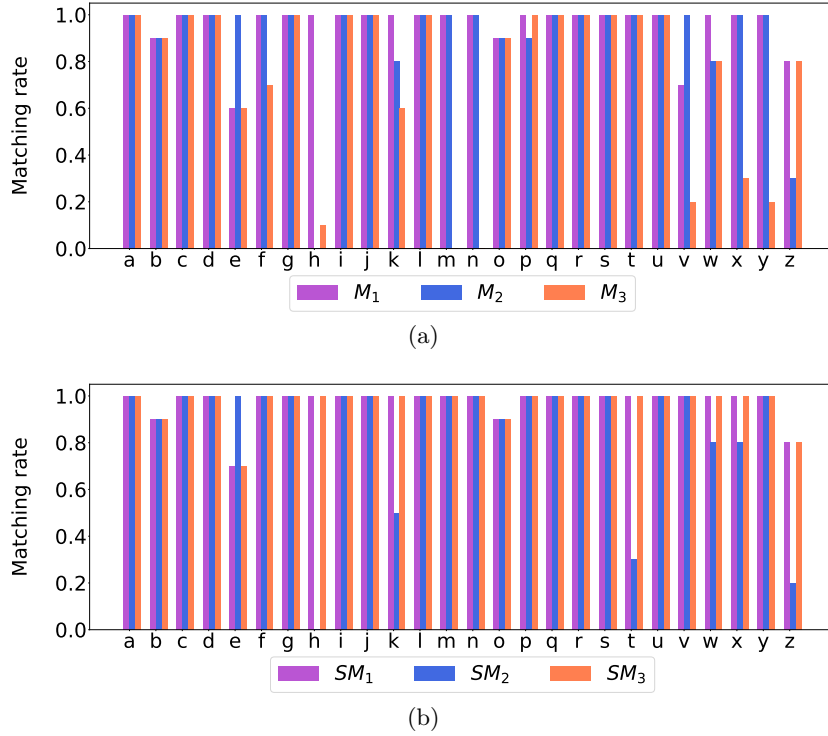


Fig. 5. Character matching rates using different crossing number comparison techniques (P&S 600 dpi): a) non-smoothed methods, b) smoothed methods.

5 Discussion

The results presented in the previous section show that the suggested method can work well for character images printed-and-scanned using different resolutions. Nevertheless, the characters after double P&S have more distortions [22]. Therefore, when we tested our matching methods with images after double P&S process, we have obtained the results presented in Table 2 under the title “Pre-processing 1”. We notice that the recognition results for characters after double P&S process are drastically lower than the results after P&S with 300 dpi and 600 dpi and equal to 74.23%. Analyzing these results, we have visualized the character images after the pre-processing operations (introduced in Section 4) in

Fig. 6.b. From this illustration, we can conclude that suggested pre-processing operations are not adapted to the character images after double P&S process.

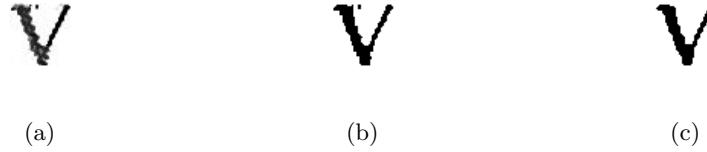


Fig. 6. Examples of a character a) after double P&S, b) after “pre-processing 1” used in Section 4.1, c) after “pre-processing 2” presented in this section.

The double P&S process changes the character shape (see Fig. 6.a) due to the scanner quantization and compression steps. Therefore, we need to apply specific pre-processing to improve the character shape. In order to fill the holes in the images (see Fig. 6.b), we use the 2×2 open-close operation. This pre-processing step significantly improves the character shape and makes the color more homogeneous (see Fig. 6.c). After these morphological operations, the thinning operation works better and the matching results are significantly improved (see Table 2 under the title “Pre-processing 2”).

	M_1	M_2	M_3	SM_1	SM_2	SM_3
Pre-processing 1						
P&S 300 dpi	91.92%	86.54%	84.62%	94.23%	82.69%	95.00%
P&S 600 dpi	95.77%	90.77%	73.46%	97.31%	86.15%	97.31%
double P&S 600 dpi	66.92%	65.77%	54.23%	73.08%	66.54%	74.23%
Pre-processing 2						
P&S 300 dpi	85.38%	86.15%	83.46%	84.62%	78.08%	88.08%
P&S 600 dpi	89.62%	88.85%	90.00%	90.00%	85.38%	91.15%
double P&S 600 dpi	78.08%	75.38%	76.54%	80.00%	70.77%	83.46%

Table 2. Percentage of correctly recognized characters using suggested crossing number comparison techniques.

Table 2 shows that the correctly used pre-processing operations can significantly improve the recognition results: the recognition rate improves up to 83.46%. Nevertheless, the recognition results of characters printed once drop off from 95 – 97% to 88 – 91%. Thus, for that moment, we do not find unique set of pre-processing operations for both characters printed once and characters printed twice.

This study helps us to identify several future paths:

- Find the unique pre-processing operations for characters printed once and twice. We can test image noise reduction and image sharpening methods, or even try to do the pre-processing step using a deep learning approach [3].
- Find stable skeleton extraction method that ensures the stable extraction of proposed features. For this, we can, for example, extract the noise resistant digital euclidean connected skeletons introduced in [10].
- Make the text processing by lines in order to avoid the problems with bounding boxes extraction. Indeed, we can extract the same features by lines and then use a fuzzy hash functions for text hashing. This solution can be similar to sketchprint presented in [26].

Finally, we have decided to compare our matching method with PCA based approach from [22]. The results are reported in Table 3, where abbreviations F_1F_1 and F_2F_2 mean that the training and testing were done using the same font (F_1 - Times New Roman, F_2 - Arial) and abbreviation F_1F_2 means that F_1 was used for training and F_2 for testing. We note that the PCA approach gives slightly better results while training and testing sets come from the same font. Nevertheless, the generalization is better using our proposed matching method SM_3 : the matching accuracy is 17 – 20% higher in case of P&S 300 dpi and P&S 600 dpi, and it is 8% higher in case of double P&S with “pre-processing 2”.

	Proposed matching SM_3			PCA approach [22]		
	F_1F_1	F_1F_2	F_2F_2	F_1F_1	F_1F_2	F_2F_2
Pre-processing 1						
P&S 300 dpi	95%	85.77%	85.38%	99.62%	66.54%	94.62%
P&S 600 dpi	97.31%	82.69%	85%	91.15%	65.00%	97.69%
double P&S 600 dpi	74.23%	70.00%	68.08%	96.54%	76.15%	91.15%
Pre-processing 2						
P&S 300 dpi	88.08%	86.15%	84.62%	94.23%	66.92%	95.00%
P&S 600 dpi	91.15%	86.54%	85.38%	97.31%	66.54%	98.08%
double P&S 600 dpi	83.46%	83.84%	78.85%	90.77%	76.15%	90.77%

Table 3. Comparison of proposed SM_3 matching technique with PCA based approach from [22].

From the results of Table 3 and from the feature extraction method, we can conclude that the proposed matching methods are more adapted for fuzzy text hash construction than the PCA based method.

6 Conclusions

Nowadays, the use of both soft-copy and hard-copy documents increases significantly. In the same time, due to accessibility of editing tools and printing/capturing devices as well as the improvements of deep learning techniques,

the number of document counterfeits increases each year. For fighting against the document counterfeits, it is important to find a novel integrity check systems that work well for both versions of documents (soft- and hard-copies).

In this paper, we have proposed crossing numbers based features for printed character matching. These features were extracted from the character skeletons. We have explored the use of non-smoothed and smoothed features. The smoothed features show us more stable and high accuracy results of 95% and 97.31% both for characters printed with 300 dpi and with 600 dpi, respectively. The additional experiments were done for the characters printed-and-scanned twice. When the pre-processing operations are chosen correctly, the matching accuracy for double P&S characters comes up to 83.46%. In addition, it was shown that the proposed matching methods can be generalized when different fonts are used for template construction and matching.

In the future, we would like to modify the pre-processing operations (noise reduction and skeletonization) in order to improve the matching results and construct compact text hash using the proposed features for printed document integrity check.

References

1. Alh riti re, H., Cloppet, F., Kurtz, C., Ogier, J.M., Vincent, N.: A document straight line based segmentation for complex layout extraction. In: IAPR International Conference on Document Analysis and Recognition (ICDAR). vol. 1, pp. 1126–1131. IEEE (2017)
2. Artaud, C., Sid re, N., Doucet, A., Ogier, J.M., Poulain D’Andecy, V.: Find it! fraud detection contest report. In: International Conference on Pattern Recognition (ICPR). pp. 13–18. IEEE (2018)
3. Bui, Q.A., Mollard, D., Tabbone, S.: Selecting automatically pre-processing methods to improve OCR performances. In: IAPR International Conference on Document Analysis and Recognition (ICDAR). vol. 1, pp. 169–174. IEEE (2017)
4. Chiang, P.J., Khanna, N., Mikkilineni, A.K., Segovia, M.V.O., Allebach, J.P., Chiu, G.T., Delp, E.J.: Printer and scanner forensics: models and methods. In: Intelligent Multimedia Analysis for Security Applications, pp. 145–187. Springer (2010)
5. Eskenazi, S., Bodin, B., Gomez-Kr mer, P., Ogier, J.M.: A perceptual image hashing algorithm for hybrid document security. In: IAPR International Conference on Document Analysis and Recognition (ICDAR). vol. 1, pp. 741–746. IEEE (2017)
6. Eskenazi, S., Gomez-Kr mer, P., Ogier, J.M.: When document security brings new challenges to document analysis. In: Computational Forensics, pp. 104–116. Springer (2012)
7. Eskenazi, S., Gomez-Kr mer, P., Ogier, J.M.: The Delaunay document layout descriptor. In: Symposium on Document Engineering. pp. 167–175. ACM (2015)
8. Eskenazi, S., Gomez-Kr mer, P., Ogier, J.M.: A study of the factors influencing OCR stability for hybrid security. In: IAPR International Conference on Document Analysis and Recognition (ICDAR). vol. 9, pp. 3–8. IEEE (2017)
9. Ferreira, A., Bondi, L., Baroffio, L., Bestagini, P., Huang, J., dos Santos, J.A., Tubaro, S., Rocha, A.: Data-driven feature characterization techniques for laser printer attribution. IEEE Transactions on Information Forensics and Security **12**(8), 1860–1873 (2017)

10. Leborgne, A., Mille, J., Tougne, L.: Noise-resistant digital euclidean connected skeleton for graph-based shape matching. *Journal of Visual Communication and Image Representation* **31**, 165–176 (2015)
11. Lee, T.C., Kashyap, R.L., Chu, C.N.: Building skeleton models via 3-D medial surface axis thinning algorithms. *CVGIP: Graphical Models and Image Processing* **56**(6), 462–478 (1994)
12. Lipkina, A., Mestetskiy, L.M.: Grapheme approach to recognizing letters based on medial representation. In: *International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications - Volume 4: VISAPP*. pp. 351–358 (2019)
13. Mikkilineni, A.K., Khanna, N., Delp, E.J.: Texture based attacks on intrinsic signature based printer identification. In: *Media Forensics and Security*. vol. 7541, p. 75410T. *International Society for Optics and Photonics* (2010)
14. Mikkilineni, A.K., Khanna, N., Delp, E.J.: Forensic printer detection using intrinsic signatures. In: *Media Watermarking, Security, and Forensics*. vol. 7880, p. 78800R. *International Society for Optics and Photonics* (2011)
15. Navarro, L.C., Navarro, A.K., Rocha, A., Dahab, R.: Connecting the dots: Toward accountable machine-learning printer attribution methods. *Journal of Visual Communication and Image Representation* **53**, 257–272 (2018)
16. Otsu, N.: A threshold selection method from gray-level histograms. *IEEE Transactions on Systems, Man, and Cybernetics* **9**(1), 62–66 (1979)
17. Picard, J.: Digital authentication with copy-detection patterns. In: *Electronic Imaging*. pp. 176–183. *International Society for Optics and Photonics* (2004)
18. Roy, P., Bhattacharya, S., Ghosh, S., Pal, U.: Stefann: scene text editor using font adaptive neural network. In: *Conference on Computer Vision and Pattern Recognition (CVPR)*. pp. 13228–13237. *IEEE/CVF* (2020)
19. Shang, S., Memon, N., Kong, X.: Detecting documents forged by printing and copying. *EURASIP Journal on Advances in Signal Processing* **2014**(1), 1–13 (2014)
20. Solanki, K., Madhow, U., Manjunath, B.S., Chandrasekaran, S., El-Khalil, I.: Print and scan resilient data hiding in images. *IEEE Transactions on Information Forensics and Security* **1**(4), 464–478 (2006)
21. Tan, L., Sun, X.: Robust text hashing for content-based document authentication. *Information Technology Journal* **10**(8), 1608–1613 (2011)
22. Tkachenko, I., Gomez-Krämer, P.: Robustness of character recognition techniques to double print-and-scan process. In: *IAPR International Conference on Document Analysis and Recognition (ICDAR)*. vol. 09, pp. 27–32 (2017)
23. Tkachenko, I., Puech, W., Destruel, C., Strauss, O., Gaudin, J.M., Guichard, C.: Two-level QR code for private message sharing and document authentication. *IEEE Transactions on Information Forensics and Security* **11**(3), 571–583 (2016)
24. Van Renesse, R.L.: Optical document security. *Appl Opt* **13528**, 5529–34 (1996)
25. Villán, R., Voloshynovskiy, S., Koval, O., Deguillaume, F., Pun, T.: Tamper-proofing of electronic and printed text documents via robust hashing and data-hiding. In: *Security, Steganography, and Watermarking of Multimedia Contents*. vol. 6505, p. 65051T. *International Society for Optics and Photonics* (2007)
26. Voloshynovskiy, S., Diephuis, M., Holtyak, T.: Mobile visual object identification: from SIFT-BoF-RANSAC to sketchprint. In: *Media Watermarking, Security, and Forensics 2015*. vol. 9409, p. 94090Q. *International Society for Optics and Photonics* (2015)
27. Wu, L., Zhang, C., Liu, J., Han, J., Liu, J., Ding, E., Bai, X.: Editing text in the wild. In: *International Conference on Multimedia*. pp. 1500–1508. *ACM* (2019)

28. Yang, Q., Huang, J., Lin, W.: Swaptext: Image based texts transfer in scenes. In: Conference on Computer Vision and Pattern Recognition (CVPR). pp. 14700–14709. IEEE/CVF (2020)
29. Yu, L., Niu, X., Sun, S.: Print-and-scan model and the watermarking countermeasure. *Image and Vision Computing* **23**(9), 807–814 (2005)
30. Zhao, F., Tang, X.: Preprocessing and postprocessing for skeleton-based fingerprint minutiae extraction. *Pattern Recognition* **40**(4), 1270–1281 (2007)
31. Zhu, B., Wu, J., Kankanhalli, M.S.: Print signatures for document authentication. In: Conference on Computer and Communications Security. pp. 145–154. ACM (2003)