

Chebyshev-Harmonic-Fourier-Moments and Deep CNNs for Detecting Forged Handwriting

¹Lokesh Nandanwar, ¹Palaiahnakote Shivakumara, ²Sayani Kundu, ²Umapada Pal, ³Tong Lu and ⁴Daniel Lopresti
¹Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia. Email: lokeshnandanwar150@gmail.com, shiva@um.edu.my.

²Computer Vision and Pattern Recognition Unit, Indian Statistical Institute, Kolkata, India. Email: sayani.frndz@gmail.com, umapada@isical.ac.in

³National Key Lab for Novel Software Technology, Nanjing University, Nanjing, China. Email: lutong@nju.edu.cn

⁴Computer Science & Engineering, Lehigh University, Bethlehem, PA, USA. Email: lopresti@cse.lehigh.edu.

Abstract— Recently developed sophisticated image processing techniques and tools have made easier the creation of high-quality forgeries of handwritten documents including financial and property records. To detect such forgeries of handwritten documents, this paper presents a new method by exploring the combination of Chebyshev-Harmonic-Fourier-Moments (CHFM) and deep Convolutional Neural Networks (D-CNNs). Unlike existing methods work based on abrupt changes due to distortion created by forgery operation, the proposed method works based on inconsistencies and irregular changes created by forgery operations. Inspired by the special properties of CHFM, such as its reconstruction ability by removing redundant information, the proposed method explores CHFM to obtain reconstructed images for the color components of the Original, Forged Noisy and Blurred classes. Motivated by the strong discriminative power of deep CNNs, for the reconstructed images of respective color components, the proposed method used deep CNNs for forged handwriting detection. Experimental results on our dataset and benchmark datasets (namely, ACPR 2019, ICPR 2018 FCD and IMEI datasets) show that the proposed method outperforms existing methods in terms of classification rate.

Keywords—Orthogonal rotation invariant moments, Fourier moments, Forgery detection, Fraud document identification, Forged handwriting detection.

I. INTRODUCTION

Handwriting analysis in the field of document image processing has received special attention due to its application in detecting signs of criminal activity, such as fraudulent document identification, fake certificate detection, forged property documents detection, tampered suicide note detection, forged answer scripts detection [1] etc. Since powerful tools are available in the market, people misuse the same for committing the crime in the aforementioned applications without leaving any noticeable evidences [2]. As a result, to the unaided eye, it is difficult to distinguish forged and authentic images. Therefore, there are ongoing needs for effective methods that can detect forged handwriting.

Several methods have been described for fraudulent document identification and forgery document detection through printer source identification in the literature [3]. These methods work based on the presence of distortion introduced by forgery operation and noise generated by printer devices [4]. This basis does not work in the case of noise or distortion produced by degradations, such as blur, low resolution, and low contrast. In addition, one can expect noise and distortion due to aged documents, differences in pens and ink, and writing style.

Hence, this work considers forged handwriting detection as a four-class classification problem, which includes Original, Forged, Noisy and Blurred classes. The Original class contains authentic documents that have not been tampered with any operations. The Forged class contains words created by copy-paste and insertion operations. The Noisy class contains words affected by Gaussian noise added manually. The Blurred class contains words affected by Gaussian blur which is also added manually. Sample images for each class are shown in Fig. 1, where one can see that it is hard to see differences between forged words compared to the originals. It is noted from the forged words in Fig. 1 that for the word “higher”, the copied character “w” is pasted at the place of “er” in the original word. In the same way, for the word “pretty”, the character “w” is inserted after “e” in the original word. These are the two operations used for creating forged handwriting text in this work. The aim of the proposed work is to detect forged words irrespective of noise and blur.

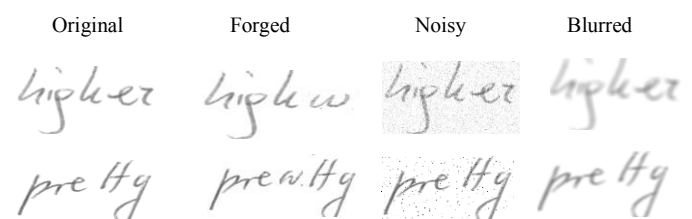


Fig. 1. Sample images of Original, Forged, Noisy and Blurred classes

II. RELATED WORK

To the best of our knowledge, we find hardly the methods on this area in the literature. As a result, we consider the methods of forged document detection through printer source identification and fraud document identification as related work for reviewing.

Barbosa et al. [5] proposed a method for fraud detection in documents written with ballpoint pens. It uses the ink of ballpoint pens as features. If the document contains text written by different pen and ink, the method may not perform well. Elkasrawi and Shafait [6] proposed a method for printer identification using supervised learning to detect forgery. The approach works based on noises produced by different printers for fraud document classification. The method does not work well for the documents with noise and distortion produced by aged documents. Ahmed and Shafait [7] proposed forgery

detection based on intrinsic document contents. The approach explores similarity between blocks of an image to identify forged document identification. The features used here are sensitive to background variations. Khan et al. [8] proposed automatic ink mismatch detection for forensic document analysis. The method analyzes ink of different pens to find fraud documents. This may not be true in reality because the same document can contain text written by different ink and pen. Luo et al. [9] proposed localized forgery detection in hyperspectral document images. This is an improved version of the above method, which explores ink quality in hyperspectral for fraud document identification. Bertrand et al. [10] proposed a system based on intrinsic features for fraudulent document detection. This approach extracts features or characters to match with the ground truth for fraud estimation. Based on mismatch scores, the method identifies fraud documents. If the document is degraded, the method does not perform well.

Raghuandan et al. [11] proposed Fourier coefficients for fraud handwritten document classification through document age analysis. The approach studies positive and negative coefficients for analyzing quality of images, which identifies it as old or new. The quality feature alone may not be sufficient for real world applications. Wang et al. [12] proposed a Fourier-residual method for forgery document detection by identifying the source or print. This method extracts features from residual given by Fourier transform for printer identification. This method is good for typed document images but not for handwriting document images. Fahn et al. [2] proposed a text independent handwriting forgery detection system based on brachlet features and Gaussian mixture models. The method is computationally expensive. Cha et al. [13] proposed automatic detection of handwriting forgery. The method studies the contour of handwriting for forgery detection. The method is sensitive to disconnections. Shivakumara et al. [1] proposed a method for detecting forged IMEI (International Mobile Equipment Identity) based on RGB color channels and fusion concept. The scope of the method is limited to IMEI images and will not work for handwritten document images.

It is noted from the above discussion that none of the methods considers forgery detection in noisy and blurred environments. However, recently, Kundu et al. [14] proposed a method for detecting forged handwriting. The method explores the shape of Fourier spectrum for forgery detection. This method performs well at the word level but not at the character level. As was shown in Fig. 1 tampering at the character level is a significant concern, especially with regard to amounts on financial documents. Therefore, forged handwriting detection at both the character and word levels is the target of the work we describe here. When we use copy-paste and insertion operations for creating forgeries, it affects the content and results abruptly compared to an unaltered document. This is because it is difficult to mimic the dynamic aspects of writing, such as speed, acceleration and force [13]. Therefore, one can expect inconsistencies and irregularities in writing where a forgery is present. This irregularity is distinctive even in the case of noisy and blurred input images.

Based on these observations, inspired by the special properties of Chebyshev-Harmonic-Fourier-Moments (CHFM), namely, their redundancy-free reconstruction

capabilities [15, 16], we introduce CHFM to obtain reconstructed images for each input image. We believe that the reconstruction ability and quality differ for original, forged, noisy and blurred images according to redundant information in the respective images. This makes sense because one can expect more redundancy for unaltered images, low redundancy for forged images, and still less redundancy for noisy and blurred images. To strengthen the reconstruction ability, we divide color image into R, G and B color components for reconstructing images. This is because the division helps us to study the minor changes effectively in the forged images. When we use combined RGB image, there are chances of missing minor changes created by forgery operation. Motivated by discriminative power of Deep Convolutional Neural Networks (D-CNNs), we explore their use for classification of forged handwriting. The main contribution of the proposed work is introducing the combination of CHFM for reconstructing images and D-CNN for classification of forged handwriting images.

III. THE PROPOSED METHOD

As mentioned in the previous section, the CHFM are good for reconstructing images by removing redundant information with the reconstruction ability differing according to the quality of the input image. This is evident from the illustration shown in Fig. 2 and Fig. 3 where mean and standard deviation of CHFM are calculated for inter- and intra-images of different classes, respectively.

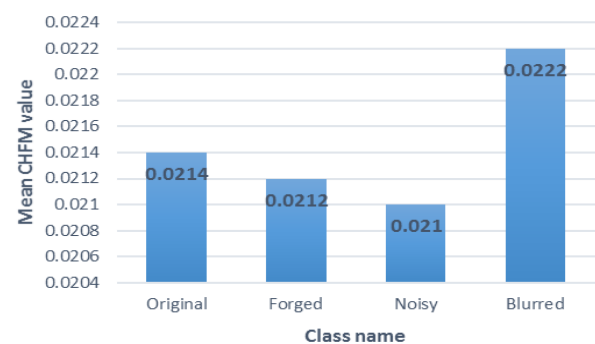


Fig. 2. Mean of CHFM for inter images of different classes

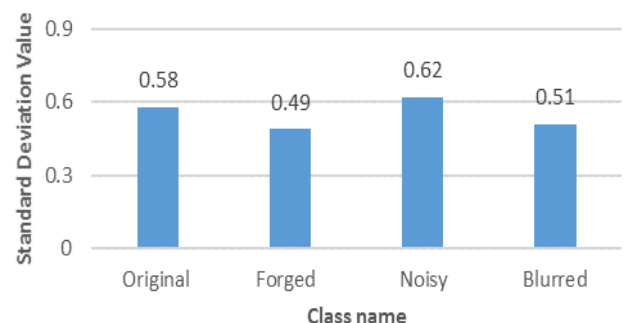


Fig. 3. Normalized Standard deviation of few CHFM for intra images of different classes

It is observed from Fig. 2 and Fig. 3 that the means of CHFMs are different for inter- images of each class while the standard deviation of CHFM is almost towards zero for intra-images of each class. This shows that the CHFMs are capable of classifying handwriting words forged at the character and word levels. With this cue, we obtain the reconstructed images for R, G and B color components, which results in three reconstructed images for each input. Since each reconstructed image of different classes is unique, we feed these reconstructed images to D-CNN for classification of forged handwriting images. The flow of the proposed method is shown in Fig. 4.

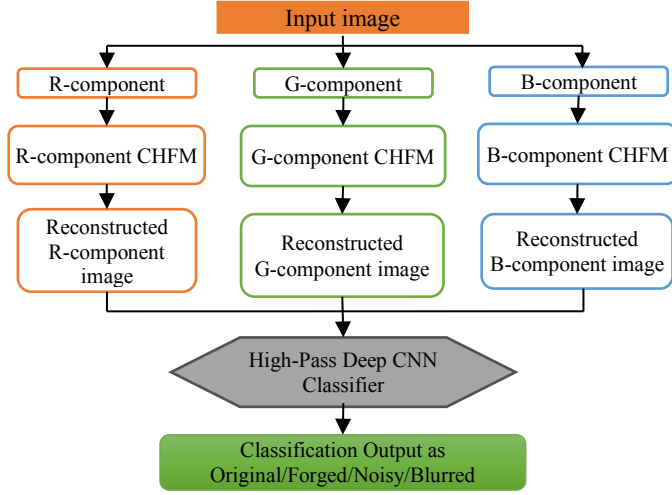


Fig. 4. Block diagram of the proposed method

A. Chebyshev-Harmonic-Fourier-Moments(CHFM) for Image Reconstruction

The Chebyshev-Harmonic-Fourier-Moments are well known as orthogonal rotation invariant moments for image reconstruction. Since the amount of computation depends on the order of the moments, we implement CHFM in an effective way using a recursive procedure as suggested by [15]. The formal mathematical steps for reconstructing images are defined from Equation (1) to Equation (5). More details for the derivation can be found in [15]. The value of order is determined empirically by choosing samples from the datasets randomly. The experiment for determining the order value is discussed in the experimental section.

CHFM (Q) of order n and repetition m with $n > 0$ and $m > 0$ is defined in polar form as:

$$Q_{nm} = \frac{1}{2\pi} \int_0^{2\pi} \int_0^1 f(r, \theta) C_{nm}^*(r, \theta) r dr d\theta \quad (1)$$

where n is a non-negative integer and m is an integer.

The function $C_{nm}^*(r, \theta)$ is the complex conjugate of the CHFM basis function $C_{nm}(r, \theta)$:

$$C_{nm}(r, \theta) = R_n(r) e^{jm\theta} \quad (2)$$

At a given pixel (i, k) , we map the pixel location (i, k) of image of resolution $N \times N$ into the coordinates (x_i, y_k) within the unit disk using the transformation:

$$x_i = \frac{2i-1+N}{D} \text{ and } y_k = \frac{2k-1+N}{D}$$

where $D = N$ for circular disk contained in the square image and $D = N\sqrt{2}$ for outer circular disk containing whole square image

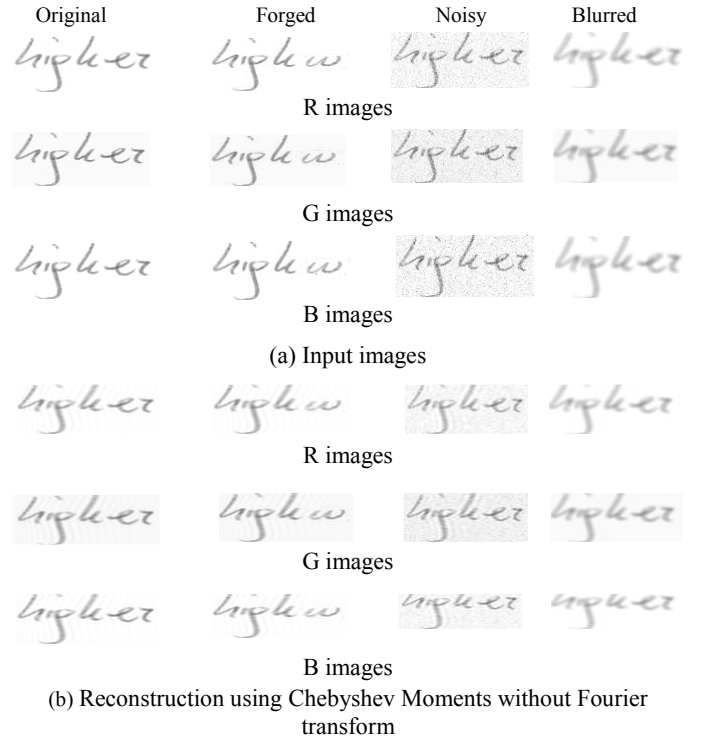


Figure 5. Proposed CHFM for obtaining the reconstructed images for respective color components

$r = \sqrt{x_i^2 + y_k^2}$, and radical part $R_n(r)$ is defined by:

$$R_n(r) = \sqrt{\frac{8}{\pi}} \left(\frac{1-r}{r} \right)^{\frac{1}{4}} \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \frac{(n-k)!}{k!(n-2k)!} (2(2r-1))^{n-2k}$$

For fast computation, radical function is defined as:

$$R_n(r) = \sqrt{\frac{8}{\pi}} \left(\frac{1-r}{r} \right)^{\frac{1}{4}} (-1)^n F_n(r) \quad (3)$$

Where:

$$F_0(r) = 1, F_1(r) = 2(1-2r) \text{ and}$$

$$F_n(r) = F_1(r)F_{n-1}(r) - F_{n-2}(r) \quad \forall n = 2, 3, \dots, n_{\max}$$

Also, for fast computation of complex function we use:

$$e^{-jm\theta} = \cos(m\theta) - j\sin(m\theta) \quad (4)$$

The values of $\cos(m\theta)$ and $\sin(m\theta)$ is computed recursively as:

$$\cos(m\theta) = \cos((m-1)\theta) - \sin((m-1)\theta)$$

$$\sin(m\theta) = \sin((m-1)\theta) + \cos((m-1)\theta)$$

At a given pixel (i, k) ,

$$r_{ik} = \sqrt{x_i^2 + y_k^2}, a = \frac{x_i}{r_{ik}} \text{ and } b = \frac{y_k}{r_{ik}}$$

For image reconstruction, $n=n_{\max}$, $m=m_{\max}$, the total number of CHFMs is $(n_{\max} + 1) \times (2m_{\max} + 1)$.

The image reconstruction function $(\hat{f}(x_i, y_k))$ for image resolution of $N \times N$ is as follows:

$$\hat{f}(x_i, y_k) = \sum_{n=0}^{n_{\max}} \sum_{m=-m_{\max}}^{m_{\max}} Q_{nm} C_{nm}^*(r, \theta) \quad (5)$$

$$\forall i, k = 0, 1, \dots, N-1$$

According to our experiments, $n_{\max}=m_{\max}=75$ is the feasible value across datasets.

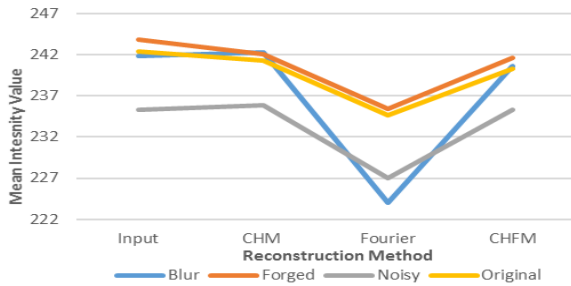


Fig. 6. Mean of reconstructed images of color components of respective images shown in Fig. 5.

The effect of reconstruction by CHFM for the R, G, B images of the Original, Forged, Noisy and Blurred classes are shown in Fig. 5, where R, G and B component are shown in Fig. 5(a) for the respective classes. When we look at the reconstructed images by only Chebyshev-Harmonic-Moments, Fourier transform and the combination of CHMF in Fig. 5(b), Fig. 5(c) and Fig. 5(d), respectively, it is difficult to notice the changes in the images compared to the input R, G and B images.

For the purpose of illustration, we compute the mean of reconstructed images of R, G and B color component of respective images of the classes as shown in Fig. 6, where we can see different values for each class. In Fig.6, since the forgery is at the character level, the word may contain single altered character, which does not introduce more distortion compared to altering more number of characters or the whole word. Due to this, the mean intensity value of original image is closer to the mean intensity values of forged images compared to noisy and blurred images. This indicates that although, the values are close, the means intensity values report small difference between original and forged images. This is the advantage of the proposed CHFM for classifying forged handwriting images.

B. H-D-CNN for Classification of Forged Handwriting Images

For each reconstructed image, we employ the following High Pass Filter-Deep Convolutional Neural Network (H-D-CNN) shown in Fig. 7 in order to perform forged handwriting classification. The architecture consists of the following filter and layers. Since the proposed method feeds a high pass filter of the reconstructed image output by CHFM to a deep network, we call it H-D-CNN. The first layer of this CNN is the Gaussian High pass filter to extract the hidden features which cannot be seen by our unaided eyes, then these features are passed through the Xception Net [17] without the top classifier, which acts as a Backbone feature extractor for our task. Then these extracted features are passed through Global Average Pooling Layer and four fully connected Layers (FC) to get the classification output.

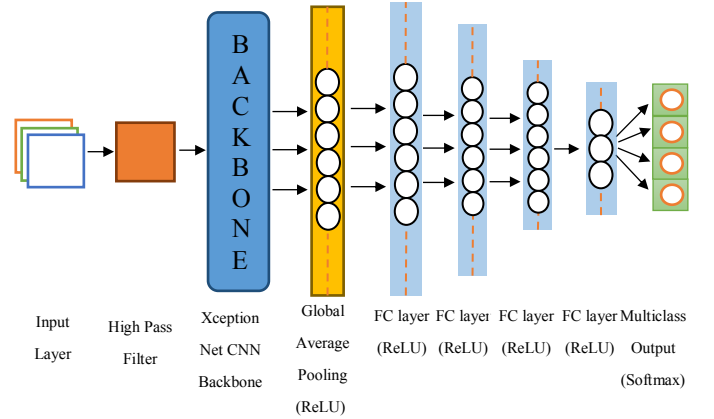


Fig.7. High pass filter deep CNN Architecture.

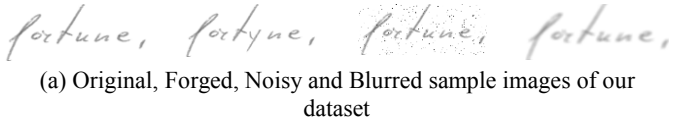
In this architecture, we use 'ReLU' activation function for all the layers except for the final layer where we use 'Softmax' [18] activation function. With 'RMSProp' [19] as optimizer and learning rate of 0.01 and 'Categorical Cross Entropy' [20] loss function (L) defined in Equation (6), where p is the labels and \hat{p} is the predicted probabilities for its respective C classes. The proposed architecture is trained for 50 epochs with the batch size of 8. The dropout rate, 0.2 is added in between the convolutional layers to reduce overfitting and more generalization of the results. For all the experiments, we use the system with Nvidia Quadro M5000 GPU for training and testing of the architecture and python framework Tensor Flow

Keras for this application. The dataset is divided into 80% and 20% for training and testing for all the experiments in this work.

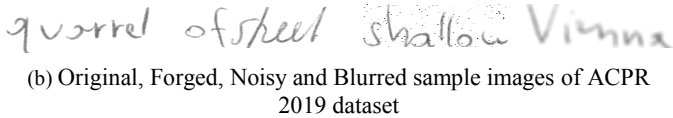
$$L(p, \hat{p}) = - \sum_{i=0}^c p_i \log(\hat{p}_i) \quad (6)$$

IV. EXPERIMENTAL RESULTS

There is no standard dataset for forged handwriting detection at the character and word levels, so we created our own, made up of 500 images for each class of Original, Forged, Noisy and Blurred, resulting in a total dataset size of 2000 images. We used the handwriting dataset created for writer identification and word spotting described elsewhere [21]. Copy-paste and insertion were used for tampering with the handwriting images. The copy-paste operation is defined as copying characters or words from a different source image to paste in a target image at the character or word level. Similarly, the insertion operation is defined as inserting characters or words at appropriate places in the original handwriting. For making forgery, we used Microsoft paintbrush software. Note that to create our forged dataset, we followed the same procedures described in [1, 14 and 22]. Therefore, we believe our dataset is as good as standard datasets for evaluation. If the class contains forged images, it is considered as the Forged class. If the class contains the handwriting words without tampering, it is considered as the Original class. For the original images, we used a Gaussian function to add noise and blur at different levels, which produced the Noisy class and the Blurred class, respectively. In this way, we created a dataset with four classes for experimentation. Sample images for each class are shown in Fig. 8(a), where it can be seen that the forgery is not noticeable compared to the original images and in the case of noisy and blurred images, the noise and the blur is visible.



(a) Original, Forged, Noisy and Blurred sample images of our dataset



(b) Original, Forged, Noisy and Blurred sample images of ACPR 2019 dataset



(c) Original and Forged sample images of ICPR 2018 FCD dataset



(d) Original and Forged sample images of IMEI dataset

Fig. 8. Sample images of four datasets

To test the effectiveness of the proposed method, we considered the standard dataset [14] called ACPR 2019 which contains the same four classes as our dataset, but with tampering done at word level. This dataset consists of 200 images for each class, which gives total 800 images for experimentation. Sample images for each class are shown in Fig. 8(b) where we can draw the same conclusions as with the dataset we constructed. To test the proposed method on forged typed images, which means

printed text on the PDF document images, we considered the benchmark dataset called ICPR 2018 Fraud Contest Data (ICPR 2018-FCD) [22], which comprises of 300 for training and 300 for testing. In total, there are 600 images for experimentation. Most of the images are money receipts containing a price, where the price has been changed. The alternation is done at character level. In addition, some of the receipts in the dataset are quite old, which presents a different form of degradations that must be dealt with. Sample images are shown in Fig. 8(c), where it can be seen how this dataset is different from other datasets.

In order to test robustness of the proposed method, forged IMEI number detection [1] which consists of 1000 images was used for evaluation. This dataset provides images containing IMEI number captured from the mobile images. The IMEI number usually pasted on inside the mobile or sometimes outside mobile cover. Here, the same operations are used for tampering images at the character level. This dataset is different from the other datasets because the images have complex background and the complexity depends on mobile cover while the images of other dataset have plain background because those images are captured from documents. Sample images can be seen in Fig. 8(d), where one can understand the complexity of the images. In total, 4100 images are considered for experimentation. We believe this dataset are sufficient to provide comprehensive testing of the proposed and existing methods. Note that our and ACPR 2019 datasets provide four classes while ICPR 2018 FCD and IMEI datasets provide only two classes, namely, Original and Forged classes.

To show the usefulness of the proposed method, we implement three existing methods for comparison. Kundu et al. [14] proposed a method for forged handwriting detection based on Fourier spectrum shape analysis. Wang et al. [12] proposed Fourier-residual for printer identification, and Shivakumara et al. [1] proposed a method for forged IMEI number detection based on fusion concept. The objective of these methods, forgery detection in document images, is the same as our proposed method. The methods work based on the fact that distortions are introduced during forgery operations. But this may not hold for the application we are proposing here because it also involves distortions resulting from image noise and blur. In addition, each targets its own particular application and dataset. To show that past methods are not adequate to handle the challenges inherent in our application, we use three different methods for comparative study.

For comparing the performance of the proposed and existing methods, we use standard measures, namely, a confusion matrix and the Classification Rate (CR) as defined in Equation (7), which is the mean of the diagonal elements of the confusion matrix. For all the above three datasets, since there is no ground truth, we count manually for calculating measures in this work.

$$CR = \frac{TP}{N_{total}} \times 100 \quad (7)$$

where, TP is the total images labeled correctly and N_{total} is the total number of test images.

For obtaining the reconstructed images using the proposed CHFM, we determined the number of moments order to terminate the iterations based on experiments as shown in Fig.

9. It is observed from Fig. 9 that as number of order increases, the average classification rate increases up to 75th order. In other words, quality of the reconstructed image increases. At 75th order of the moments, the proposed method achieves the best average classification rate. Therefore, 75 is the optimal value for the number of moments order for all the experiments in this work. For experiments, we choose 500 samples from across datasets randomly.

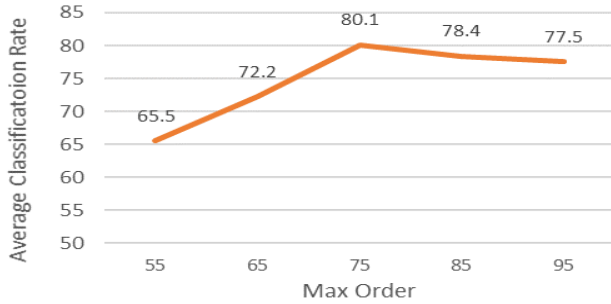


Fig. 9. Optimal value determination for the order of CHFM to obtain reconstructed images.

The proposed method consists of two important concepts, namely, Chebyshev-Harmonic-Moments (CHM) and Fourier Transform (FT) for achieving better results. To analyze the effect of each concept, we generate confusion matrix and calculate average classification rate (CR) on all the four datasets. The proposed method obtains reconstructed images using only CHM without Fourier transform and then the H-D-CNN is used for forged handwriting detection. In the same way, the proposed method obtains reconstructed images using only Fourier transform without CHM for detecting forged handwriting. The results of the both the steps and the proposed method (CHFM) are reported in Table I, Table II and Table III, respectively on all the four datasets. It is observed from Table I, Table II and Table III that the proposed + FT is better than the proposed + CHM in terms of CR for all the datasets. This shows that the FT is more effective than CHM. However, overall, when we look at the performance of individual steps, both are equally effective and contribute to the better results achieved by the proposed CHFM. It is evident from Table III that the results of the proposed CHFM are higher than individual concept in terms of CR. Therefore, one can conclude that both CHM and FT are complimenting each other to achieve better results. Note that in Table I-Table III, “-” indicate that there is no results for Blurred and Noise classes because those two datasets do not contain Blurred and Noise Classes.

Table I. Confusion matrix and average classification rate of the CHM without Fourier transform (in %) (F: Forged, O: Original, B: Blurred and N: Noisy indicates classes, C: Classes, CR: Average classification rate).

| C | Our | | | | ACPR 2019 [14] | | | | ICPR 2018 [22] | | IMEI [1] | |
|----|------|------|------|------|----------------|------|------|------|----------------|------|----------|------|
| | F | O | B | N | F | O | B | N | F | O | F | O |
| F | 60.0 | 36.8 | 3.2 | 0.0 | 84.0 | 6.0 | 10.0 | 0.0 | 43.0 | 57.0 | 39.0 | 61.0 |
| O | 32.8 | 63.2 | 0.0 | 0.0 | 2.0 | 94.0 | 4.0 | 0.0 | 5.0 | 95.0 | 12.0 | 88.0 |
| B | 3.2 | 0.0 | 96.0 | 0.8 | 38.0 | 0.0 | 72.0 | 0.0 | - | - | - | - |
| N | 2.4 | 0.0 | 2.4 | 95.2 | 0.0 | 2.0 | 0.0 | 98.0 | - | - | - | - |
| CR | 78.6 | | | | 87.0 | | | | 69.0 | | 63.5 | |

Table II. Confusion matrix and average classification rate of the Fourier transform without CHM (in %)

| C | Our | | | | ACPR 2019 [14] | | | | ICPR 2018 [22] | | IMEI [1] | |
|----|-------|------|-----|------|----------------|------|------|------|----------------|------|----------|------|
| | F | O | B | N | F | O | B | N | F | O | F | O |
| F | 64.0 | 36.0 | 0.0 | 0.0 | 76.0 | 10.0 | 14.0 | 0.0 | 76.0 | 24.0 | 58.0 | 42.0 |
| O | 28.0 | 68.8 | 3.2 | 0.0 | 6.0 | 86.0 | 8.0 | 0.0 | 11.0 | 89.0 | 4.0 | 96.0 |
| B | 0.0 | 0.8 | 96 | 3.2 | 0.0 | 4.0 | 92.0 | 4.0 | - | - | - | - |
| N | 0.0 | 0.0 | 4.8 | 95.2 | 0.0 | 0.0 | 4.0 | 96.0 | - | - | - | - |
| CR | 81.90 | | | | 87.5 | | | | 82.5 | | 77.0 | |

Table III. Confusion matrix and average classification rate of the proposed CHFM (in %)

| C | Our | | | | ACPR 2019 [14] | | | | ICPR 2018 [22] | | IMEI [1] | |
|----|------|------|------|------|----------------|------|------|-----|----------------|------|----------|------|
| | F | O | B | N | F | O | B | N | F | O | F | O |
| F | 67.2 | 32.8 | 0.0 | 0.0 | 74.0 | 26.0 | 0.0 | 0.0 | 88.3 | 11.7 | 79.0 | 21.0 |
| O | 27.2 | 69.6 | 3.2 | 0.0 | 4.0 | 96.0 | 0.0 | 0.0 | 6.7 | 93.3 | 14.0 | 86.0 |
| B | 0.0 | 0.0 | 99.2 | 0.8 | 2.0 | 2.0 | 96.0 | 0.0 | - | - | - | - |
| N | 0.0 | 0.0 | 1.6 | 98.4 | 0.0 | 0.0 | 0.0 | 100 | - | - | - | - |
| CR | 83.6 | | | | 91.5 | | | | 90.8 | | 82.5 | |

A. Experiments on Forged Handwriting Detection

Quantitative results of the proposed and existing methods for our, ACPR 2019, ICPR 2018 and IMEI datasets are reported in Table IV, Table V, Table VI and Table VII, respectively. It is noted from the Table IV-Table VII that the proposed method is the best at CR for all the datasets compared to the existing methods. For the IMIE dataset, the proposed method reports the lowest CR compared to other datasets. This is because the images of IMEI dataset have complex backgrounds while the images of other datasets have a plain background. However, overall, the proposed method achieves consistent results for all four datasets, while the existing methods do not. Hence, we can infer that the proposed method is robust to different datasets. Interestingly, Kundu et al. [14] score the best CR results among existing methods for our dataset and ACPR 2019 dataset compared to other two datasets. This shows that their method is not robust to different dataset because the features proposed do not have ability to cope with the challenges of forgeries at the character level. Their method is good for detecting forged images at word level. Wang et al. [12] reports the best results for ICPR 2018 FCD dataset compared to other datasets. This is because their method was developed for typed text similar to the images in ICPR 2018 FCD dataset. The reason for the poor results on the other datasets is that the method expects noise as introduced by different printers, which constrains its applicability. Table VII shows that Shivakumara et al. [1] reports the best results compared to other existing methods for this specific kind of data. This is true because the method is developed for detecting IMEI numbers.

Sometimes, the effects of forgery are negligible and variations in handwriting lead to misclassification by our proposed method as shown by the sample misclassified images in Fig. 10. Hence, there is a scope for the improvement of the proposed method. In this case, context-based features determined through natural language processing may help.

Table IV. Confusion matrix and average classification rate of the proposed and existing methods on our dataset (in %).

| C | Proposed method | | | | Kundu et. al. [14] | | | | Wang et al. [12] | | | | Shivakumara et. al [1] | | | |
|----|-----------------|------|------|------|--------------------|------|------|------|------------------|------|------|------|------------------------|------|------|------|
| | F | O | B | N | F | O | B | N | F | O | B | N | F | O | B | N |
| F | 67.2 | 22.8 | 0 | 0 | 48.0 | 48.0 | 2.0 | 2.0 | 39.2 | 35.2 | 30.4 | 0 | 60.0 | 4.0 | 0.8 | 35.2 |
| O | 27.2 | 69.6 | 3.2 | 0 | 46.0 | 52.0 | 2.0 | 0.0 | 2.1 | 5.1 | 2.8 | 0 | 0.0 | 64.0 | 20.0 | 16.0 |
| B | 0 | 0 | 99.2 | 0.8 | 0 | 2.0 | 94.0 | 4.0 | 9.6 | 0 | 90.4 | 0 | 8.0 | 0 | 56.0 | 36.0 |
| N | 0 | 0 | 1.6 | 98.4 | 2.0 | 0.0 | 0.0 | 98.0 | 0 | 3.6 | 0 | 96.4 | 0.0 | 0 | 16.0 | 84.0 |
| CR | 83.6 | | | | 73.0 | | | | 69.25 | | | | 66.0 | | | |

Table V. Confusion matrix and average classification rate of the proposed and existing methods on ACPR2019 dataset (in %).

| C | Proposed method | | | | Kundu et. al. [14] | | | | Wang et al. [12] | | | | Shivakumara et. al [1] | | | |
|----|-----------------|------|------|-------|--------------------|------|------|------|------------------|------|------|------|------------------------|------|------|------|
| | F | O | B | N | F | O | B | N | F | O | B | N | F | O | B | N |
| F | 74.0 | 26.0 | 0 | 0 | 85.7 | 4.8 | 9.5 | 0.0 | 71.4 | 25.0 | 1.8 | 1.8 | 50.0 | 40.0 | 0.0 | 10.0 |
| O | 4.0 | 96.0 | 0 | 0 | 20.0 | 70.0 | 10.0 | 0.0 | 25.0 | 57.8 | 7.8 | 9.4 | 23.0 | 77.0 | 0.0 | 0.0 |
| B | 2.0 | 2.0 | 96.0 | 0 | 15.8 | 15.8 | 63.2 | 5.2 | 1.8 | 9.0 | 78.2 | 11.0 | 0.0 | 22.0 | 78.0 | 0.0 |
| N | 0.0 | 0.0 | 0 | 100.0 | 0.0 | 0.0 | 10.0 | 90.0 | 8.0 | 14.3 | 1.5 | 76.2 | 0.0 | 0.0 | 10.0 | 90.0 |
| CR | 91.5 | | | | 77.5 | | | | 70.1 | | | | 73.75 | | | |

Table VI. Confusion matrix and average classification rate of the proposed and existing methods on ICPR 2018 FCD dataset (in %).

| Methods | Proposed method | | Kundu et. al. [14] | | Wang et al. [12] | | Shivakumara et. al [1] | |
|----------|-----------------|--------|--------------------|--------|------------------|--------|------------------------|--------|
| | Original | Forged | Original | Forged | Original | Forged | Original | Forged |
| Original | 93.3 | 6.7 | 90 | 10 | 84.6 | 15.4 | 92 | 8 |
| Forged | 11.7 | 88.3 | 72.5 | 27.5 | 10.7 | 89.3 | 49.4 | 50.6 |
| Average | 90.8 | | 78.3 | | 86.9 | | 71.3 | |

Table VII. Confusion matrix and average classification rate of the proposed and existing methods on IMEI dataset.

| Methods | Proposed method | | Kundu et. al. [14] | | Wang et al. [12] | | Shivakumara et. al [1] | |
|----------|-----------------|--------|--------------------|--------|------------------|--------|------------------------|--------|
| | Original | Forged | Original | Forged | Original | Forged | Original | Forged |
| Original | 86.0 | 14.0 | 57.8 | 42.2 | 83.2 | 16.8 | 82.2 | 17.8 |
| Forged | 21.0 | 79.0 | 41.8 | 58.2 | 25.6 | 74.4 | 18 | 82 |
| Average | 82.5 | | 58.0 | | 78.8 | | 82.1 | |



(a) Forged classified as original (b) Original classified as forged

Fig. 10. Limitation of the proposed method on our dataset.

V. CONCLUSION AND FUTURE WORK

In this work, we have proposed a novel method for forged handwriting detection by exploring the concept of Chebyshev-Harmonic-Fourier-Moments (CHFM) and a high pass deep convolutional neural network (D-CNN). The CHFM is used for reconstructing input images of Original, Forged, Noisy and Blurred classes. The reconstructed images are fed to high pass deep CNN for classification of forged handwriting images. Our method works based on exploiting irregularities and in consistencies in the tampered information in the images, unlike existing methods which depend on distortions introduced by the

forgery operation. The proposed method is tested on different forged handwriting datasets at the character and word levels, as well as a dataset of printed text and images with complex backgrounds to show that it is robust to different kinds of inputs. However, the proposed method sometimes misclassifies an authentic image as forged, and vice versa. This is due to natural handwriting variations overwhelming the effects of forgery. To find a solution to this problem, it may be possible to incorporate contextual features with the help of natural language processing to improve the performance of the proposed work. Further, the proposed work shall explore different color spaces, such as Y, Cb, Cr for overcome the limitation of the proposed work.

REFERENCES

- [1] P. Shivakumara, V. Basavaraja, H. S. Gowda, D. S. Guru, U. Pal and T. Lu, "A New RGB Based Fusion for Forged IMEI Number Detection in Mobile Images", In Proc. ICFHR, pp 386-391, 2018.
- [2] C. S. Fahn, C. P. Lee and H. I. Chen, "A text independent handwriting forgery detection system based on branchlet features and Gaussian mixture models", In Proc. 14th Annual Conference on Privacy, Security and Trust (PST), pp. 690-697, 2016.
- [3] T. M. Ghanim and A. M. Nabil, "Offline signature verification and forgery detection approach", In Proc. ICCES, pp 293-298, 2018.
- [4] R. Kumar, N. R. Pal, B. Chanda and J. D. Sharma, "Forensic detection of fraudulent alterations in ball point pen strokes", IEEE Trans. IFS, Vol. 7, No. 2, pp 809-820, 2012.
- [5] R. D. S. Barboza, R. D. Lins, E. D. F. D. Lira and A. C. A. Camara, "Later added strokes of text fraud detection in documents written with ballpoint pens", In Proc. ICFHR, pp 517-522, 2014.
- [6] S. Elkasrawi and F. Shafait, "Printer identification using supervised learning for document forgery detection", In Proc. DAS, 146-150, 2014.
- [7] A. Ahmed and F. Shafait, "Forgery detection based on intrinsic document features", In Proc. DAS, 252-256, 2014.
- [8] Khan, F. Shafait and A. Mian, "Automatic Ink mismatch detection for forensic document analysis", Pattern Recognition, Vol. 48, pp 3615-3626, 2015.
- [9] Z. Luo, F. Shafait and A. Mian, "Localized forgery detection in hyperspectral document images", In Proc. ICDAR, 496-500, 2015.
- [10] R. Bertrand, P. G. Kramer, O. R. Terrades, P. Franco and J. M. Ogier, "A system based on intrinsic features for fraudulent document detection", In Proc. ICDAR, pp 106-110, 2013.
- [11] K. S. Raghunandan, P. Shivakumara, B. J. Navya, G. Pooja, Navya, N. Prakash, G. H. Kumar, U. Pal and T. Lu, "Fourier coefficients for fraud handwritten document classification through age analysis", In Proc. ICFHR, pp 25-30, 2016.
- [12] Z. Wang, P. Shivakumara, T. Lu, M. Basavanna, U. Pal and M. Blumenstein, "Fourier-residual for printer identification", In Proc. ICDAR, pp 1114-1119, 2017.
- [13] S. H. Cha and C. C. Tappert, "Automatic detection of handwriting forgery", In Proc. IWFHR, 2012.
- [14] S. Kundu, P. Shivakumara, A. Grouver, U. Pal, T. Lu and M. Blumenstein, "A new forged handwriting detection method based on Fourier spectral density and variation", In Proc. ACPR, pp 136-150, 2019.
- [15] R. Upneja, C. Singh and A. Prashar, "Fast Computation of Chebyshev-Harmonic Fourier Moments", Lecture Notes on Information Theory, Vol. 3, No. 2, pp 60-64, 2015.
- [16] H. Zhu, Y. Yang, Z. Gui, Y. Zhu and Z. Chen, "Image analysis by generalized Chebyshev-Fourier and generalized pseudo-jacobi-Fourier moments", Pattern Recognition, 51, pp 1-11, 2016.
- [17] F. Chollet, "Xception: Deep Learning with Depthwise Separable Convolutions", In Proc. CVPR, pp 1800-1807, 2017.
- [18] I. Goodfellow, Y. Bengio and A. Courville, "6.2.2.3 Softmax Units for Multinoulli Output Distributions". Deep Learning. MIT Press, pp. 180-184, 2016.

- [19] G. Hinton, N. Srivastava and K. Swersky, "Neural networks for machine learning:, lecture 6a overview of mini-batch gradient descent", https://www.cs.toronto.edu/~tijmen/csc321/slides/lecture_slides_lec6.pdf, 2012.
- [20] K. Janocha and W. Czarnecki, "On Loss Functions for Deep Neural Networks in Classification", *Schedae Informaticae*. 25. 2017.
- [21] F. Kleber, S. Fiel, M. Diemand R. Sablatnig, "Cvl-database: An off-line database for writer retrieval, writer identification and word spotting", In *Proc. ICDAR*, pp.560-564, 2013.
- [22] C. Artaud, N. Sidère, A. Doucet, J. Ogier and V. P. D. Yooz, "Find it! Fraud Detection Contest Report", In *Proc. ICPR*, pp 13-18, 2018.