Face Identification

*A*

*Project Report Submitted in partial fulfillment of the requirements For the degree of*

Master of Science (Data Science)

### Submitted

by

Piyush Kumar (Enrollment no. O21MSD16235)



### Department of Science

CHANDIGARH UNIVERSITY

Chandigarh 2023

# ACKNOWLEDGEMENTS

First, I would like to express my sincere gratitude to my advisor, **Ms. Sujata Kully,** for her realistic, encouraging, critical and constructive approach throughout my M.Sc (Data Science) study and her efforts during supervision of my project. Her wisdom, knowledge and commitment to the highest standards inspired and motivated me. She has been very generous in providing the necessary resources to carry out my project work.

I am greatly indebted to all my friends, who have graciously applied themselves to the task of helping me with ample moral supports and valuable suggestions.

On a personal note, I owe everything to the Almighty and my parents. The support which I enjoyed from my father, mother and other family members provided me the mental support I needed.

**Piyush Kumar(021MSD16235)**

## ABSTRACT

In this digital era, digital images have become one of the principals means of information carrier. As the acquisition, distribution and storage of these images is very easy, so they are used as a common source of evidence in everyday life controversies and trials. In spite of ease in acquisition, distribution and storage, the accessibility of these images brings a major drawback. They can be easily edited with a variety of common editing tools like Adobe Photoshop. Therefore, it is easy to modify content and meaning of these images without leaving the visually detectable traces. In the literature many instances of tampering or forgery can be found and are very common now a days. Hence, there is need to confirm their authenticity before relying on their content further. In response to this, researchers have begun to develop digital image forensic techniques which are capable to identify multimedia forgeries. The digital image forensics aims to provide tools and techniques which support blind investigation of images and help in confirming their authenticity. Digital image forensics analyses the images by making use of the fact that most of image processing operations leave visually undetectable traces in the altered image content. Image forensics relies on these undetectable traces to identify tampering. Researchers have addressed two main problems in digital image forensics. The first one is face identification i.e., to identify the source camera which is used to capture the images by performing some kind of ballistic analysis. The second is to detect the various traces of forgeries by studying inconsistencies in the image statistics.

This report includes the implementation and comparison of two source camera identification methods. Both of these methods use the sensor pattern noise in identification. Only difference is that in second method the extracted noise residual from sample images is enhanced to suppress the scene details. For each threshold value in range [-1, 1], the TPR of second method is always greater than that of first one and FPR is always lesser than that of first one. Hence, the performance of second method is better than that of first method.

[i]

## TABLE OF CONTENTS

##### ABSTRACT I

LIST OF FIGURES IV

[LIST OF TABLES VI](#_bookmark0)

1. INTRODUCTION 1
   1. [Motivation](#_bookmark1) [**1**](#_bookmark1)
   2. [Image Acquisition & Storage](#_bookmark2) [**3**](#_bookmark2)
   3. [Organization of the Report](#_bookmark3)

5

1. LITERATURE REVIEW
2. BASICS OF SOURCE CAMERA IDENTIFICATION 9
   1. [Fingerprint Estimation](#_bookmark4) [**9**](#_bookmark4)
   2. [Fingerprint Preprocessing](#_bookmark5) [**11**](#_bookmark5)
   3. [Sensor Pattern Noise (SPN) Extraction](#_bookmark6) [**11**](#_bookmark6)
   4. [Enhancement of SPN](#_bookmark7) [**12**](#_bookmark7)
   5. Similarity Metric **12**
   6. [Performance Statistics](#_bookmark8) [**13**](#_bookmark8)
3. DIGITAL CAMERA IDENTIFICATION USING SENSOR PATTERN NOISE 15
   1. [Algorithm Implementation](#_bookmark9) [**15**](#_bookmark9)
   2. [Data set and simulation parameters](#_bookmark10) [**15**](#_bookmark10)
   3. [Results](#_bookmark11)

[ii] [**17**](#_bookmark11)

1. **CAMERA IDENTIFICATION USING ENHANCED SENSOR SOURCE PATTERN 21**

**NOISE**

* 1. [Algorithm Implementation](#_bookmark12) [**21**](#_bookmark12)
  2. [Data set and simulation parameters](#_bookmark13) [**24**](#_bookmark13)
  3. [Results](#_bookmark14) [**24**](#_bookmark14)

##### CONCLUSIONS 30

**REFERENCES**

|  |  |  |
| --- | --- | --- |
|  | **LIST OF FIGURES** |  |
| **Fig. 1.1** | First fake image | **1** |
| **Fig .1.2** | Sequence of steps during digital multimedia acquisition | **3** |
| **Fig. 1.3** | Bayer CFA pattern (left) & RGB intensity values from imaging sensor | |

|  |  |  |
| --- | --- | --- |
|  | (right) |  |
|  | **4** |
| **Fig. 4.1.1** | Flowchart of the Algorithm. | **16** |
| **Fig. 4.3.1** | Distribution of correlation for 200 positive sample images with Nikon D200 fingerprint. | **18** |
| **Fig. 4.3.2** | Distribution of correlation for 1200 negative sample images with Nikon D200 fingerprint. | **19** |
| **Fig. 4.3.3** | ROC Curves | **20** |
| **Fig. 5.1.1** | (a) Camera referenceSPN taken from flat field images. (b) Image of a | **21** |
|  | natural scene. (c) SPN extracted from (b) that is contaminated by the |  |
|  | details from the scene. (d) Enhanced version of (c) using Model 5 [i.e., |  |
|  | eq. (2 4.1)] with *a*=7. |  |

|  |  |  |
| --- | --- | --- |
| **Fig. 5.1.2** | Flowchart of the Algorithm (Enhanced noise residual method). | **23** |
| **Fig. 5.3.1** | Distribution of correlation for 200 positive sample images with Nikon D200 fingerprint (obtained by enhancing the noise residual). | **25** |
| **Fig. 5.3.2** | Distribution of correlation for 1200 negative sample images with Nikon D200 fingerprint (obtained by enhancing the noise residual). | **26** |

**Fig. 5.3.3** ROC Curves (obtained by enhancing the noise residual) **28**

**Fig. 5.3.4** Comparison of ROC Curves **29**

## LIST OF TABLES

|  |  |  |
| --- | --- | --- |
| **Table 3.1** | Performance of these methods to geometric operations & JPEG | **7** |
|  | Compression |  |
| **Table 4.3.1** | TPR & FPR values for different image sizes cropped from center at Threshold value = 0.0015. | **19** |
| **Table 5.3.1** | TPR & FPR values for different image sizes cropped from center at Threshold value = 0.0015 (obtained by enhancing the noise residual) | **27** |

# Chapter 1

**INTRODUCTION**

#### Motivation

In this digital world, the acquisition, distribution and storage of images have become very easier because of ease of availability of digital cameras and mobile phones with fcamera. Hence, images are used as source of evidences in various controversial situations. The accessibility of these images brings a major drawback because it can be easily edited with a variety of common editing tools like Adobe Photoshop. These editing tools are very sophisticated in the sense that they do not leave visually detectable traces. For example, the first fake image(Fig. 1.1) is created by Hippolyte Bayrad in 1840s; in that image he was shown committing suicide [1]. Another fake image was appeared in 1860s; in that image the head of Abraham Lincoln was fixed over the body of a politician name John Calhoun [2]. In the literature many such instances can be found. Hence, there is need to confirm their authenticity but the establishment of the authenticity of images has become a challenging task since the available editing tools are very sophisticated.



Fig. 1.1 First fake image [1]

To encounter this problem, digital image watermarking technique has been proposed [3]. It is one of the active techniques which provides multimedia security. In active techniques, the additional information is embedded into an image in advance and this embedded information is extracted to confirm their authenticity. In watermarking techniques, a watermark is inserted into the image content. But these techniques are effective only if the watermark is inserted before any manipulation or editing takes place. In many scenarios this is unrealistic in the sense that the party that captures the digital content can manipulate or edit its content before inserting the watermark.This is one of the limitations of active techniques i.e. digital watermarking and hence it cannot be used in many practical situations.

To overcome the limitations of active techniques i.e., digital watermarking, the field of digital image forensics has been evolved. The main aim of digital image forensics is to provide tools and techniques which support blind investigation of images and help in confirming their authenticity. It is one of the passive techniques which exploit image processing and analysis tools to recover information about the history of multimedia. Passive techniques are those which do not require any prior embedding information for authentication like digital image watermarking. Digital image forensics analyses the multimedia by making use of the fact that most of image processing operations leave visually undetectable traces in the altered image content. These traces in digital image content are known as fingerprints in the analogy that a criminal leaves behind fingerprints at a crime scene. Researchers can identify digital image forgeries by developing the techniques which are able to detect these fingerprints. Digital image forensics have applications in many domains, such as intelligence, legal services, news reporting and insurance claim investigations [4][5] and hence it is becoming a popular research field.

Researchers have addressed two main problems in digital image forensics.

* ***Source Camera Identification*** *i.e.,* to identify the device which is used to capture the image byperforming some kind of ballistic analysis.
* ***Image Tampering Detection*** *i.e.,* to detect the various traces of forgeries like copy- moveforgery etc. by studying inconsistencies in image statistics.

To address these two main problems, various techniques have been proposed. In the next section Iwill identify the most common steps which are performed in the image acquisition and storage processes for the better understanding of the implementation of these existing techniques.

##### Image Acquisition & Storage

The sequences of processing steps that are performed during image acquisition are shown in the Fig. 1.2.

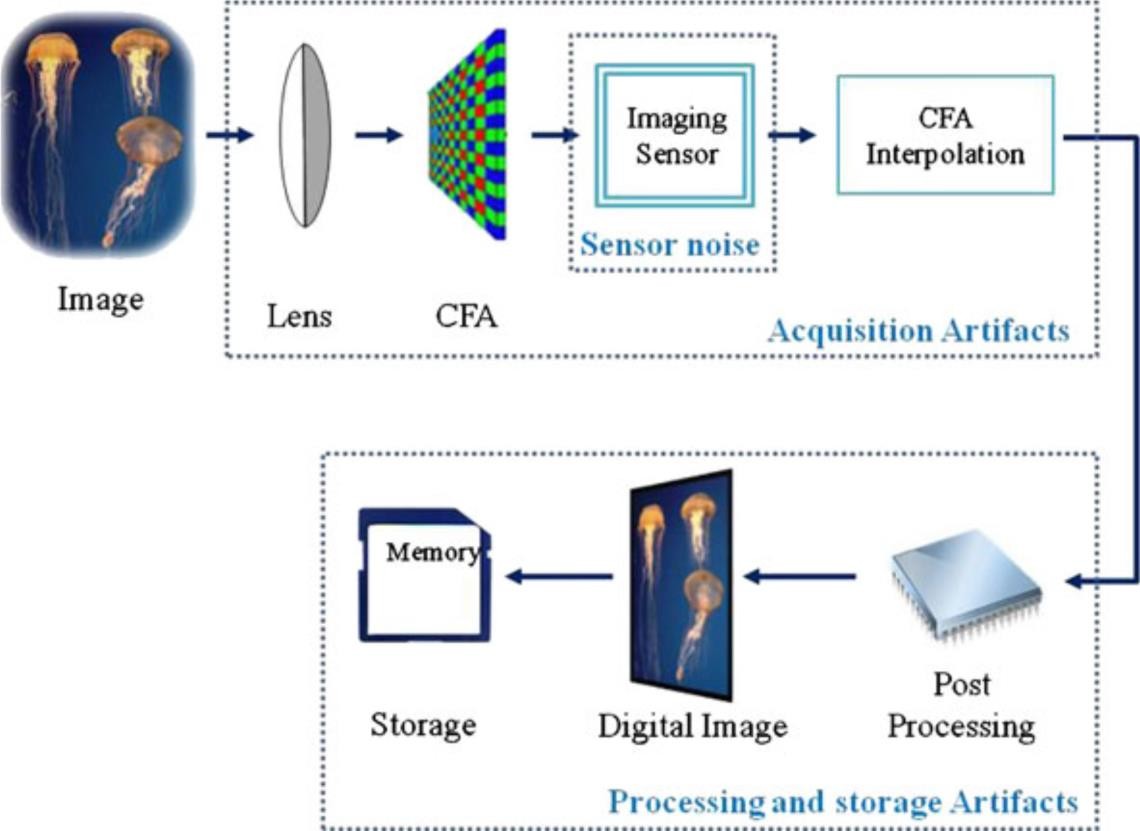


Fig 1.2 Sequence of steps during digital image acquisition [6]

Firstly, a digital camera takes the light rays and focuses it onto imaging sensor with the help of lenses. An imaging sensor consists of an array of photodiodes. When light strikes this array, each photodiode generates an analog signal which is then converted into digital signal by built- in

analog to digital convertor. Most of digital camera manufacturers use a charge-coupled device (CCD) as the image sensor. Now a days CMOS chips are also emerging as a popular alternative. These photodiodes just record the brightness of light i.e., they are not sensitive to colors and hence produce a monochromatic output. So, in order to produce a color image, a color filter array (CFA) is used before the imaging sensors. CFA is a thin ﬁlm on the sensor that passes a certain color component of light through it. Therefore, each photodiode records the light intensity for a single color only. This CFA pattern varies from one manufacturer to another. Figure 1.3 shows the commonly used Bayer CFA pattern. As a result, the raw image generated by imaging sensors consists of red, green and blue (RGB) intensity values as shown in Fig. 1.3. To obtain the color image, the obtained RGB intensity values need to be interpolated. In order to perform this interpolation, demos icing algorithms are applied which estimate the missing intensity values based on the values of existing neighbors in each of red, blue and green channel.

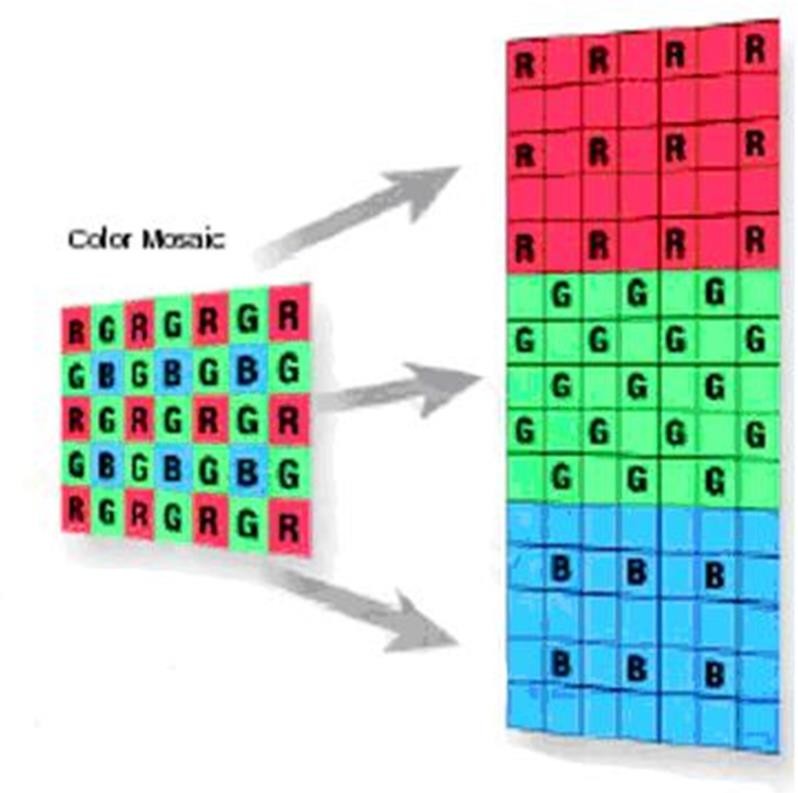


Fig. 1.3Bayer CFA pattern (left) &RGB intensity values from imaging sensor (right)

After this additional processing white balance, gamma correction, and contrast enhancement are performed. Finally, the image is stored in the memory device in a particular image format (RAW, TIFF or JPEG)), but JPEG is the most common choice.

It is observed that these imaging sensors introduce sensor pattern noise (SPN) in the captured images. This SPN is generated due to the variation in the sensitivity of image sensors when exposed to light [7]. This variation arises because of impurities in silicon wafers and imperfections introduced during the manufacturing process. Hence, all images taken by same device are overlaid by a specific sensor pattern noise. This sensor noise pattern acts as a unique and intrinsic fingerprint of the acquisition device [8]. In the next chapter I have shown the basics of source camera identification and how these fingerprints are used to identify the source camera.

##### Organization of the report

* Chapter 2: The basics of face identification.
* Chapter 3: Literature Survey.
* Chapter 4: The face identification using Sensor Pattern Noise.
* Chapter 5: The face identification using Enhanced Sensor Pattern Noise.
* Chapter 6: Conclusions.

# Chapter 2

## LITERATURE REVIEW

In the literature, Lukas and Friedrich, proposed a very popular method for estimating camera fingerprint (also referred to as camera reference SPN). Here, fingerprints are estimated using averaging method and normalized correlation is taken as similarity metric. All images taken by camera are at highest resolution setting. This method is able to distinguish two cameras of same brand and model. This method is robust to gamma correction with 𝛾 = 0.7 & 1.4. It is also robust to JPEG compression with quality factors 50, 70 and 90. The correct identification rate of this method decreases whenever geometrical operation such as cropping, resizing, scaling, rotation, etc. is performed.

Liu proposed another method to further improve the identification performance of above method with respect to cropping. Since the extracted noise residual contains the scene details so it is needed to enhance it by suppressing the scene details. The models used in enhancement are already discussed in section 1.1.4. All images are cropped from center and ROC performance degrades with decreasing the cropping size. As compared to Lukas's method, this method performs better with respect to cropping.

Chen and Friedrich, proposed a method which uses ML estimation method to estimate the fingerprint. After estimation fingerprints are preprocessed using zero mean filtering and wiener filtering in DFT domain. The estimation procedure and pre-processing procedure is already discussed in section 1.1.1 and 1.1.2 respectively. Peak to correlation energy is used as similarity metric. All images taken by camera are at highest resolution setting. This method is robust to gamma correction with 𝛾 = 0.5. It is also robust to JPEG compression with quality factors 75 & 90. The correct identification rate of this method also decreases whenever geometrical operation such as cropping, resizing, scaling, rotation etc. is performed.

Kang and Li proposed phase averaging method to estimate the fingerprints and correlation over CCN as similarity metric. This method achieves the best ROC performance among all above methods with respect to cropping. This method also outperforms above methods in resisting

the JPEG compression with quality factor 50, 75, 90. The performance of this degrades significantly for image size < 256x256.

Yoichi and Yuya proposed a new approach for face identification. It uses pair wise magnitude relationships of pixel clusters that are created from extracted noise residual. In this method there is no need to estimate fingerprint. Instead of estimating fingerprint, it estimates the mismatch probability of pixel cluster pairs for each camera model for both flat field images and natural images. And the estimated mismatch probability is used as a threshold in deciding whether the given sample image belongs to the claimed camera model or not. It is also used in FAR calculation. All positive sample images and negative sample images are taken from Dresden image database. This method has better ROC performance than in case of cropping. As the cluster size increases, identification accuracy is also increased. However, when the image is small, cluster size will be reduced and hence the performance of this method will degrade. The performance of this method degrades significantly for image size < 400x300.

Table 1 shows the brief summary of performance of these methods to geometric operations and JPEG compression.

Table 3.1 Performance of these methods to geometric operations & JPEG compression

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Method** | **Cropping** | **JPEG**  **Compression (Images are at highest resolution setting of camera)** | **Scaling** | **Rotation** |
| [1] | Not Robust for size <  1024x1024 | Robust for QF = 50,70,90 | Not Robust | Not Robust |
| [2] | Not Robust for size < 512x512 | Not Discussed | Not Robust | Not Robust |
| [3] | Not Robust for size <  1024x1024 | Robust for QF = 75,90 | Not Robust | Not Robust |
| [4] | Not Robust for size < 256x256 | Robust for QF = 50,75,90 | Not Robust | Not Robust |
| [5] | Not Robust for size < 400x300 | Not discussed | Not Robust | Not Robust |

All last page methods fail to identify the shifted, scaled and rotated images. Research is still going on to encounter these drawbacks in the existing methods. In the next chapters I have tried to show the implementation of these methods and the comparison of the ROC performances of these methods.

# Chapter 3

## BASICS IMAGE IDENTIFICATION

Image identification aims at establishing a link between an image and the acquisition device that generates it. As discussed in section 1.2, all image acquisition devices consist of imaging sensors which introduces sensor pattern noise (SPN) in the captured images. Hence, all images taken by same device are overlaid by a specific sensor pattern noise. This sensor noise pattern acts as a unique and intrinsic fingerprint of the acquisition device. In literature various techniques to identify source camera are proposed. These techniques involve the following main steps in identifying the source device:

1. Fingerprint Estimation using the flat field images of same device. Blue sky images are the example of flat field images.
2. Fingerprint pre-processing to remove CFA artifacts and JPEG compression artifacts.
3. Sensor pattern noise (Noise residual) is extracted from a given sample image or a set of sample images.
4. Then, the extracted noise residual is enhanced to suppress the scene details.
5. After this, similarity metric is used to measure the similarity between the estimated fingerprint and the enhanced noise residual.
6. Based on similarity measures, performance statistics are calculated and decision is taken whether the given sample image is taken by the claimed acquisition device or not.

##### 3.1 Fingerprint Estimation:

There are three types of fingerprint estimation methods proposed in literature: Basic averaging method , Maximum Likelihood (ML) estimation method and Phase averaging method.

1. *Averaging Method*

In this method, noise residual is extracted from N number of flat field images of same device as in eq. 3.1.1. Then, the fingerprint is estimated by averaging of extracted noise residuals as in

eq. 2.2.1. The number of flat field images used i.e. N should be greater than 50. Here, I had used N=50 in our experiments.

𝑛k = 𝐼k − 𝐹(𝐼k)(3.1.1)

*fg* = ∑k nk(3.1.2) N

𝐼kis the kth flat field image, 𝑛kis the noise residual from kth flat field image, F(.) is the wavelet-based de-noising filter (for details refer to [9]) and 𝑓𝑔 is the estimated fingerprint.

1. *ML estimation method*

In the case of ML estimation, the following sensor output model is used.

𝐼 = 𝐼0 + 𝐼0𝐾 + 𝜃 (3.1.1)

𝐼 denotes the camera output image, 𝐼0 is "true ideal" image in the absence of any noise, 𝐾 is the sensor fingerprint and 𝜃 includes all possible noise components. The fingerprint 𝐾 can be estimated from N flat field images using eq. 3.1.2. The value of N should be greater than 50. Here, N=50 is taken during experiments.

*K*= ∑k wkIk

∑k(Ik)2

(3.1.4)

𝐼kis the kth flat field image, 𝑤kis the noise residual from kth flat field image same as in eq. 1.1.1.

1. *Phase Averaging:*

It is obtained by averaging the phase-only component of the DFT of noise residual as in eq. 3.1.5, 3.1.6 and 3.1.7.

𝑊k

= 𝐷𝐹𝑇 (𝑤k

)(3.1.5) 𝑊∅k

= Wk (3.1.6)

|Wk|

𝑓𝑔 = 𝑟𝑒𝑎𝑙(𝐼𝐷𝐹𝑇 (∑k W∅k)) ) (3.1.7)

N

𝑤kis the noise residual from kth flat field image same as in eq. 1.1.1, 𝑊k is the Discrete Fourier Transform of noise residual, 𝑊∅k is the phase of DFT of extracted noise residual, N is no. of flat field images and fg is the estimated fingerprint. Here, real part is only considered because imaginary part has very small value and can be ignored.

##### Fingerprint pre-processing:

The estimated fingerprint contains CFA (Color Filter Array) artifacts and JPEG compression artifacts. These artifacts increase the correlation between the fingerprints of two different cameras of different models or two different cameras of same model. This would increase the false identification rate and hence degrade the ROC performance of the source camera identification algorithms. Hence, it is necessary to preprocess the estimated fingerprints to enhance the ROC performance. The following methods are proposed in [11] to preprocess the estimated fingerprints:

1. *Zero Mean Filtering*

It is used to remove CFA artifacts. In this, first the column average is subtracted from each pixel in the column and then the row average is subtracted from each pixel in the row. The processed fingerprint is denoted by *ZM(K)* and will have zero mean in every row and every column.

1. *Wiener Filtering in DFT domain*

It is used to remove JPEG compression blocking artifacts. In this, first *ZM(K)* is transformed into Fourier domain, then it is filtered using wiener filtering and finally the noise component is kept in spatial domain as in eq. 3.2.1.

𝑊𝐹 (𝑍𝑀(𝐾)) = 𝐹–1{𝐹(𝑍𝑀(𝐾)) − 𝑊(𝐹(𝑍𝑀(𝐾)))} (3.2.1)

*W* is the 3x3 wiener filter with variance obtained from the variance of magnitude of Fourier transform |*F(ZM(K))*|. The resultant processed fingerprint will have flatter frequency spectrum.

##### Sensor pattern noise (SPN) Extraction:

For a given sample image or a set of sample images, noise residual is extracted using eq. 3.3.1.

𝑛k = 𝐼k − 𝐹(𝐼k) (3.3.1)

𝐼kis the kth given sample image, 𝑛kis the noise residual from kth given sample image. F(.) is wavelet-based de-noising filter.

##### Enhancement of SPN:

The extracted noise residual from given sample images contains scene details, which decreases correlation between the fingerprint of the device and given sample image of same device. Hence the false identification rate increases and degrades ROC performance. To increase the ROC performance, the extracted noise residual is need to be enhanced by suppressing the scene details. Various models are proposed in [13] to encounter this. In this report, only one model is

n(i,j)2

𝑒–0.5 a2 if n(i, j) <= 0

included as in eq. 3.4.1.𝑛𝑒(𝑖, 𝑗) = { n(i,j)2 (3.4.1)

−𝑒–0.5 a2 otherwise

where *n*(*i,j*) is the (*i,j*)th component of extracted noise residual nand*ne*(*i,j*) is the (*i,j*)th component of enhanced noise residual *ne*. The enhanced noise residual will contain lesser scene details.

##### Similarity Metrics:

The following three similarity metrics are used in literature [12]:

1. Normalized Correlation:

The normalized correlation coefficient between two images x & y is defined as

*corr(x,y)* = (x– x̅)((y– y¯))

||(x– x̅) || ||(y– y¯)||

(3.5.1)

𝑥̅is the mean value of *x*, 𝑦¯ is the mean value of *y* and ||.|| denotes norm operator. This similarity metric performs good when the image under investigation did not undergo any geometric processing.

1. Peak to Correlation Energy:

The peak to correlation energy between two images x & y is defined as

r2 (0)

*PCE (x,y)* = xy

1 ∑m∄A r2 (m)

(3.5.2)

N—|A| xy

N is image size, A is small neighborhood around 𝑟xy(0) which denotes the peak value of cross

correlation, |A| is size of A and circular cross correlation 𝑟xy(𝑚) is defined as

𝒙𝒚 ∑N—1 xiyi+m

𝑟xy(𝑚) = 𝒎 = i=0 (3.5.3)

N N

PCE is more stable similarity metric than the correlation as it is independent of image size and suppresses the periodic noise contaminations. One drawback of PCE is that it increases the false identification rate because of squaring of 𝑟xy(0) which turns negative PCE value to a positive PCE value.

1. Correlation over circular cross-correlation norm (CCN):

This similarity metric overcomes the drawback of PCE by considering the negative sign problem and it is defined as

C*CN (x,y)* = rxy(0)

1 ∑ r2 (m)

(3.5.4)

√N—|A| m∄A xy

N is image size, A is small neighborhood around 𝑟xy(0) which denotes the peak value of cross correlation, |A| is size of A and 𝑟xy(𝑚) denotes the circular cross correlation as defined above.

##### Performance Statistics:

Based on similarity metric, decision are made whether the given sample image belongs to device or not. If similarity metric is greater than a particular threshold then positive decision is taken i.e. image belongs to device otherwise negative decision is taken i.e. image do not belong to that device.

1. True positive rate (TPR):

It is calculated as ratio of number of positive decisions over the total number of images of same camera.

1. False positive rate (FPR):

It is calculated as ratio of number of positive decisions over the total number of images of different cameras.

1. Receiver operating characteristics (ROC):

It is graphical plot between false positive rate and true positive rate when threshold is varied from a possible minimum value to a possible maximum value. The slope at any point in this graph gives the threshold value.

# Chapter 4

## DIGITAL CAMERA IDENTIFICATION USING SENSOR PATTERN NOISE

In this chapter, we will discuss the implementation of one the most popular source camera identification method [9]. We will also discuss the results that we have obtained.

##### Algorithm Implementation

In this method, basic averaging method as discussed in section 2.1.1 is used to estimate the camera fingerprint. This estimated fingerprint is also referred to as camera reference pattern. Then the SPN is extracted from a given image or set of images using eq. 2.3.1. This extracted SPN is also referred to as noise residual. After this the normalized correlation between the camera reference pattern and the extracted noise is calculated using eq.2.5.1. If the calculated correlation is greater than a particular threshold then the given sample image is deemed to be taken by the claimed device. If the correlation is greater than the threshold then it is taken as positive decision otherwise taken as negative decision. Here we have varied threshold from a minimum possible value to maximum possible value. For each threshold, True Positive Rate (TPR) & False Acceptance Ratio (FAR) is calculated. Then the graph between FAR and TPR is plotted with x-axis as FAR & y-axis as TPR. This graph is termed as Receiver Operating Characteristic (ROC). The flowchart of this algorithm is shown in figure 4.1.1

##### Data Set and Simulation Parameters

In our experiment I had taken Nikon D200 camera model and all images are taken from *Dresden image database*[15]*.* 50 flat field images are taken to estimate camera reference pattern (fingerprint) of Nikon D200. To calculate TPR, 200 images of Nikon D200 are taken and termed as positive samples. For each of 200 images, correlation is calculated and total numbers of positive decisions are counted by comparing the calculated correlation with a particular threshold value. For a fixed threshold, TPR is calculated as ratio of total number of

positive decisions and total positive samples (here it is 200). To calculate FAR, 1200 images of six other camera models (200 each) are taken and termed as negative samples. For each of 1200 images, correlation is calculated and total numbers of positive decisions are counted by comparing the calculated correlation with a particular threshold value. For a fixed threshold, FAR is calculated as ratio of total number of positive decisions and total negative samples (here it is 1200). Here threshold is varied from 1 to -1 with decrement of 0.001. For each threshold, TPR and FAR is calculated and ROC is plotted. All images are cropped from center.

Start

Fingerprint Estimation using eq.2.1.1 and it is denoted as “fgd200”.

N=50 flat field images of Nikon D200 camera are taken.



SPN is extracted from each of positive samples and negative samples.

Normalized Correlation is calculated between fgd00 & SPN extracted from

positive sample images to get 200 correlation values for positive sample images.

All images both positive samples and negative samples are cropped from center. Three different sizes are under taken; those are 1024x1024, 512X512, 256X256 and 128X128.

Normalized Correlation is calculated between fgd00 & SPN extracted from negative sample images to get 1200 correlation values for negative sample images.

Cont…..

Cont….

Now threshold is varied from 1 to -1 with decrement of 0.001. True positive rate is calculated for each threshold by comparing correlation values for positive samples with threshold. Similarly, false positive rate is calculated for each threshold by comparing correlation values for negative samples with threshold.

ROC is plotted between TPR & FPR with FPR as x-axis and TPR as y- axis.

End

Fig. 4.1.1 Flowchart of the Algorithm

##### Results

In this section we will discuss the results we have obtained by applying this algorithm in the dataset taken from Dresden image database.

##### Histogram

In an image processing context, the histogram of an image normally refers to a histogram of the pixel intensity values. This histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. For an 8-bit gray scale image there are 256 different possible intensities, and so the histogram will graphically display 256 numbers showing the distribution of pixels amongst those grayscale values. *Histograms have many uses. One of the more common is to decide what value of threshold to use as per our requirement.*

Here, I had plotted the histogram of correlation values for positive sample images with image size 1024x1024 (cropped from center) shown in figure 4.3.1. This histogram is a graph (distribution) showing the number of correlation values i.e. count at different range of correlation value found in the calculated correlation values for 200 positive sample images.

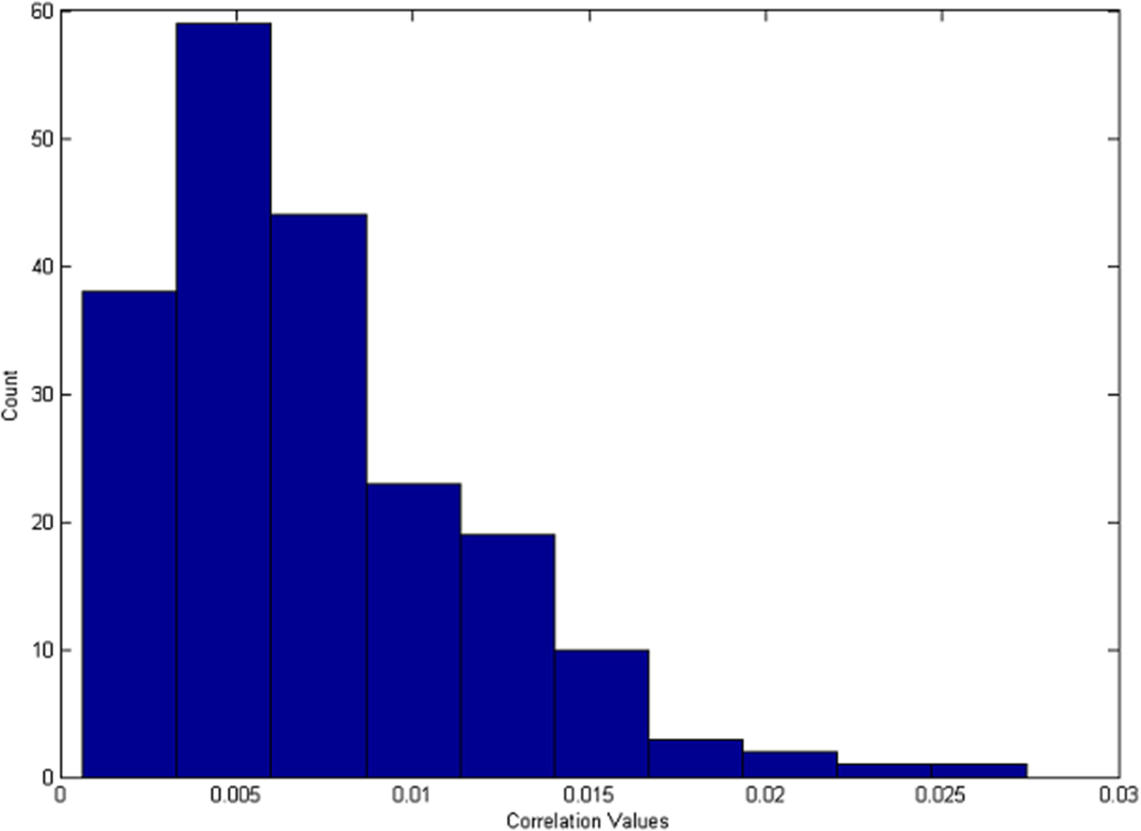


Fig. 4.3.1 Distribution of correlation for 200 positive sample images with Nikon D200 fingerprint.

I had also plotted the histogram of correlation values for negative sample images with image size 1024x1024 (cropped from center) shown in figure 4.3.2. In figure 4.3.1 I can see that more than 95% of the total correlation values are greater than 0.0015 while in figure 4.3.2 I can see that more than 87% of all correlation values are less than 0.0015. So it is concluded that the correlation between the camera reference pattern (fingerprint) and the positive image samples of same camera model are having higher correlation value than that of the correlation between the camera reference pattern (fingerprint) and the negative sample images of different camera model. If I choose a threshold value of 0.0015, then its TPR is coming out to be 0.9550 and FPR (FAR) is coming out to be 0.1275. This signifies that the algorithm can detect 95.50% of 200 positive sample images correctly with false acceptance of 12.75% of 1200 negative sample images at threshold value = 0.0015.

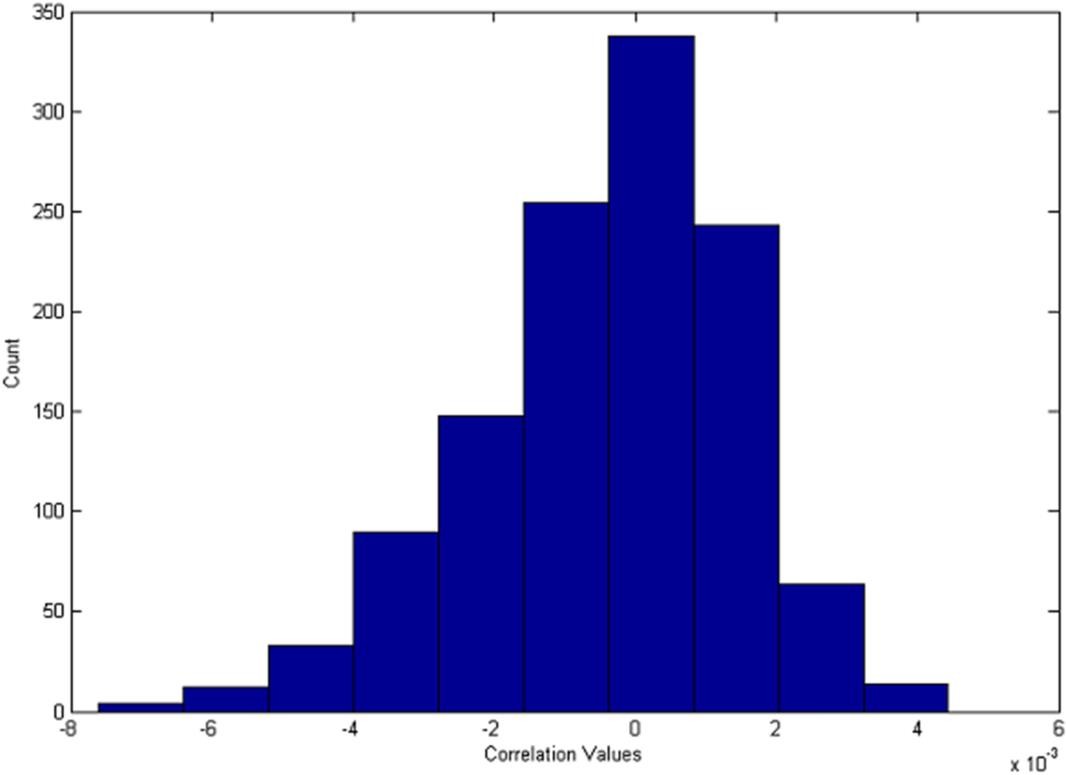


Fig. 4.3.2 Distribution of correlation for 1200 negative sample images with Nikon D200 fingerprint.

##### TPR and FPR values for different image sizes

I had dalculated the TPR and FPR values for four different image sizes cropped from center. As the cropping sizes decreases, True positive rate (TPR) decreases and False positive rate (FPR) increases.

Table 4.3.1 TPR & FPR values for different image sizes cropped from center at Threshold value = 0.0015.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Image Size** | **128x128** | **256x256** | **512x512** | **1024x1024** |
| **TPR** | 0.6700 | 0.7400 | 0.8500 | 0.9550 |
| **FPR** | 0.4675 | 0.3825 | 0.2700 | 0.1275 |

##### 4.3.2. ROC Curves

Here I had varied threshold from 1 to -1 with decrement of 0.001. For each threshold, TPR & FPR is calculated. Then the graph between FPR and TPR is plotted with x-axis as FPR & y- axis as TPR as shown in figure 4.3.3. This graph is termed as Receiver Operating Characteristic (ROC). As the cropping sizes decreases, True positive rate (TPR) decreases and False positive rate (FPR) increases. As a result, ROC performance degrades whenever cropping size decreases.

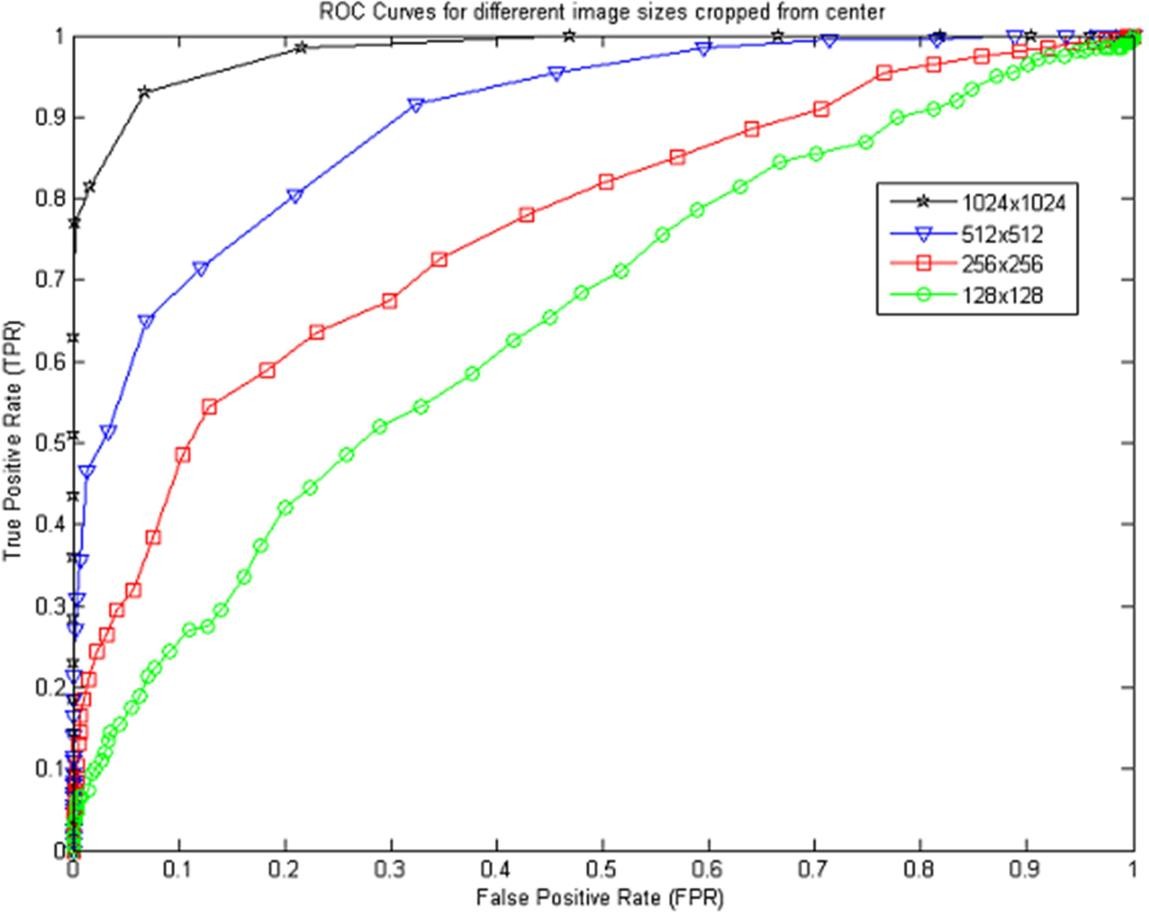


Fig. 4.3.3 ROC Curve

# Chapter 5

## FACE IDENTIFICATION USING ENHANCED SENSOR PATTERN NOISE

In this chapter, I am observing the implementation of another most popular source camera identification method [13]. In this method the extracted noise residual is enhanced to suppress the scene details which reduces the false positive rate (FPR) and hence improves the ROC performance and results obtained.

##### Algorithm Implementation

In this method, basic averaging method as discussed in section 2.1.1 is used to estimate the camera fingerprint. This estimated fingerprint is also referred to as camera reference pattern. Then the SPN is extracted from a given image or set of images using eq. 2.3.1. This extracted SPN is also referred to as noise residual. This extracted noise residual contains the scene details. For example, figure 5.1.1(a) shows a camera reference SPN which is the average SPN of 50 flat field images of same camera, figure 5.1.1(b) shows the image of a natural scene taken by the same camera, and figure 5.1.1(c) shows the SPN extracted from the image of figure 5.1.1(b). Figure 5.1.1(a) is what a “clean” SPN should look like. However, from figure 5.1.1(c) I can see that the SPN contains strong details from the scene, which dominates the real SPN.



* + 1. (b)

(c) (d)

Fig. 5.1.1 (a) Camera reference SPN taken from flat field images. (b) Image of a natural scene. (c) SPN extracted from (b) that is contaminated by the details from the scene. (d) Enhanced version of (c) using Model 5 [i.e., eq. (2.4.1)] with *a*=7.

Hence, the extracted noise residual needs to be enhanced to suppress the scene details. Figure 5.1.1(d) shows the enhanced version of (c) using Model 5 [i.e., eq. (2.4.1)] with *a*=7. After this the normalized correlation between the camera reference pattern and the enhanced extracted noise is calculated using eq.2.5.1. If the calculated correlation is greater than a particular threshold then the given sample image is deemed to be taken by the claimed device. If the correlation is greater than the threshold then it is taken as positive decision otherwise taken as negative decision. Here we have varied threshold from a minimum possible value to maximum possible value. For each threshold, True Positive Rate (TPR) & False Acceptance Ratio (FAR) is calculated. Then the graph between FAR and TPR is plotted with x-axis as FAR & y-axis as TPR. This graph is termed as Receiver Operating Characteristic (ROC). The flowchart of this algorithm is shown in figure 5.1.2. We also compare the ROC performance of this algorithm with the ROC performance of the previous algorithm for image size 1024 x0124 cropped from the center.



Start

Fingerprint Estimation using and it is denoted as "fgd200". N=50 flat field images of Nikon D200 camera are taken.

All images both positive samples and negative samples are cropped from center. Three different sizes are under taken; those are 1024x1024, 512X512, 256X256 and 128X128.

**Extracted noise residual (SPN) is enhanced using eq. 2.4.1 to suppress scene details**

Normalized Correlation is calculated between fgd00 & Enhanced version of SPN extracted

from positive sample images to get 200 correlation values for positive sample images.

SPN is extracted from each of positive samples and negative samples.

Normalized Correlation is calculated between fgd00 & Enhanced version of SPN extracted from negative sample images to get 1200 correlation values for negative sample images.



Now threshold is varied from 1 to -1 with decrement of 0.001. True positive rate is calculated for each threshold by comparing correlation values for positive samples with threshold. Similarly, false positive rate is calculated for each threshold by comparing correlation values for negative samples with threshold .

ROC is plotted between TPR & FPR with FPR as x-axis and TPR as y-axis.

End

Fig. 5.1.2 Flowchart of the Algorithm (Enhanced noise residual method).

##### Data Set and Simulation Parameters

In our experiment we have taken Nikon D200 camera model and all images are taken from *Dresden image database.* 50 flat field images are taken to estimate camera reference pattern (fingerprint) of Nikon D200. To calculate TPR, 200 images of Nikon D200 are taken and termed as positive samples. For each of 200 images, correlation is calculated and total numbers of positive decisions are counted by comparing the calculated correlation with a particular threshold value. For a fixed threshold, TPR is calculated as ratio of total number of positive decisions and total positive samples (here it is 200). To calculate FAR, 1200 images of six other camera models (200 each) are taken and termed as negative samples. For each of 1200 images, correlation is calculated and total numbers of positive decisions are counted by comparing the calculated correlation with a particular threshold value. For a fixed threshold, FAR is calculated as ratio of total number of positive decisions and total negative samples (here it is 1200). Here threshold is varied from 1 to -1 with decrement of 0.001. For each threshold, TPR and FAR is calculated and ROC is plotted. All images are cropped from center.

##### Results

In this section we will discuss the results we have obtained by applying this algorithm in the dataset taken from Dresden image database.

##### Histogram

In an image processing context, the histogram of an image normally refers to a histogram of the pixel intensity values. This histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. For an 8-bit grayscale image there are 256 different possible intensities, and so the histogram will graphically display 256 numbers showing the distribution of pixels amongst those grayscale values. Histograms have many uses. One of the more common is to decide what value of threshold to use as per our requirement.

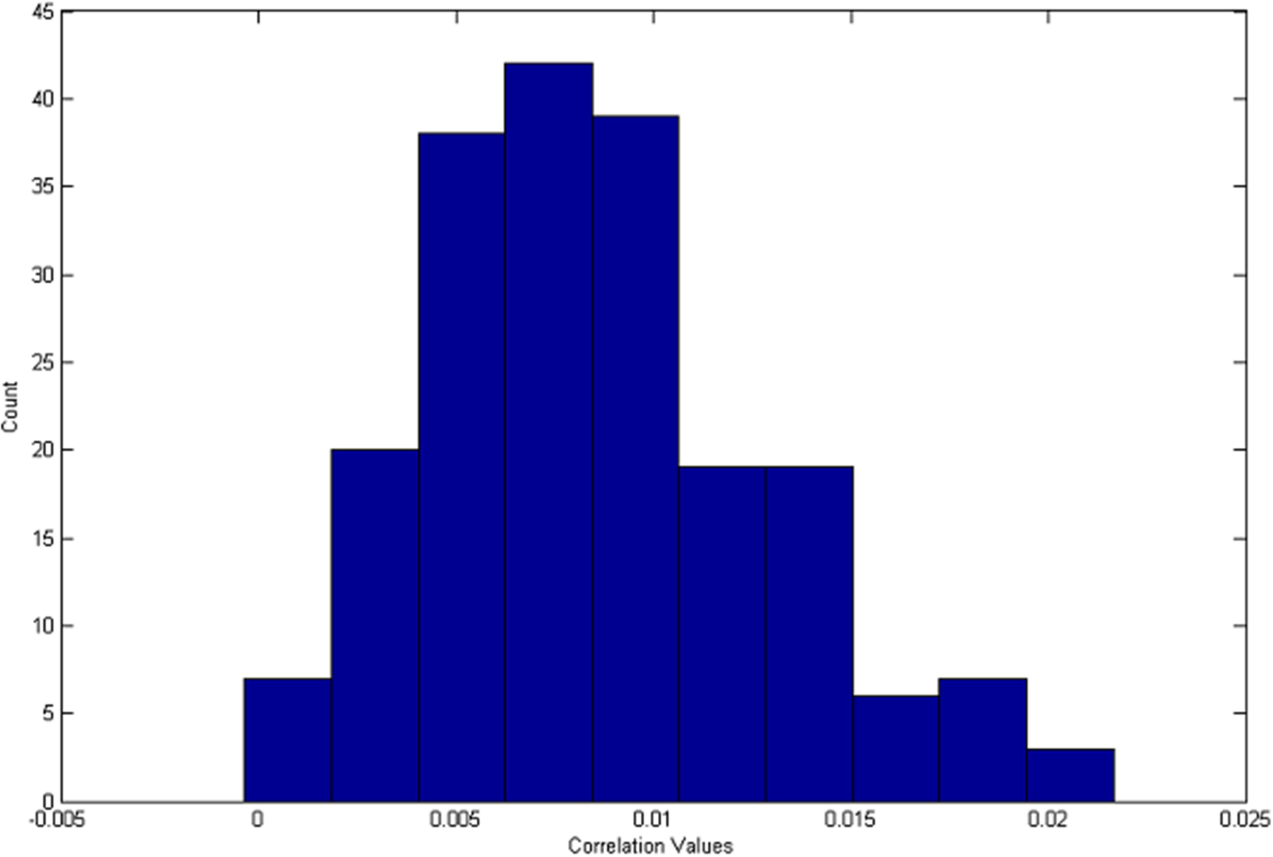
Here, we have plotted the histogram of correlation values for positive sample images with image size 1024x1024 (cropped from center) shown in figure 5.3.1. This histogram is a graph (distribution) showing the number of correlation values i.e. count at different range of correlation value found in the calculated correlation values for 200 positive sample images.

Fig. 5.3.1 Distribution of correlation for 200 positive sample images with Nikon D200 fingerprint obtained by enhancing the noise residual.

We also plotted histogram of correlation values for negative sample images with image size 1024x1024 (cropped from center) shown in figure 5.3.2. In figure 5.3.1 we can see that more than 97% of the total correlation values are greater than 0.0015 while in figure 5.3.2 we can see that more than 97% of all correlation values are less than 0.0015. So it is concluded that the correlation between the camera reference pattern (fingerprint) and the positive image samples of same camera model are having higher correlation value than that of the correlation between the camera reference pattern (fingerprint) and the negative sample images of different camera model. If we choose a threshold value of 0.0015, then its TPR is coming out to be 0.97250 and FPR (FAR) is coming out to be 0.0292. This signifies that the algorithm can detect 97.25% of

200 positive sample images correctly with false acceptance of 2.92% of 1200 negative sample images at threshold value = 0.0015. We can also notice that the performance of this method is better than that of the previous method since its TPR is higher and FPR is lower than that of previous one.

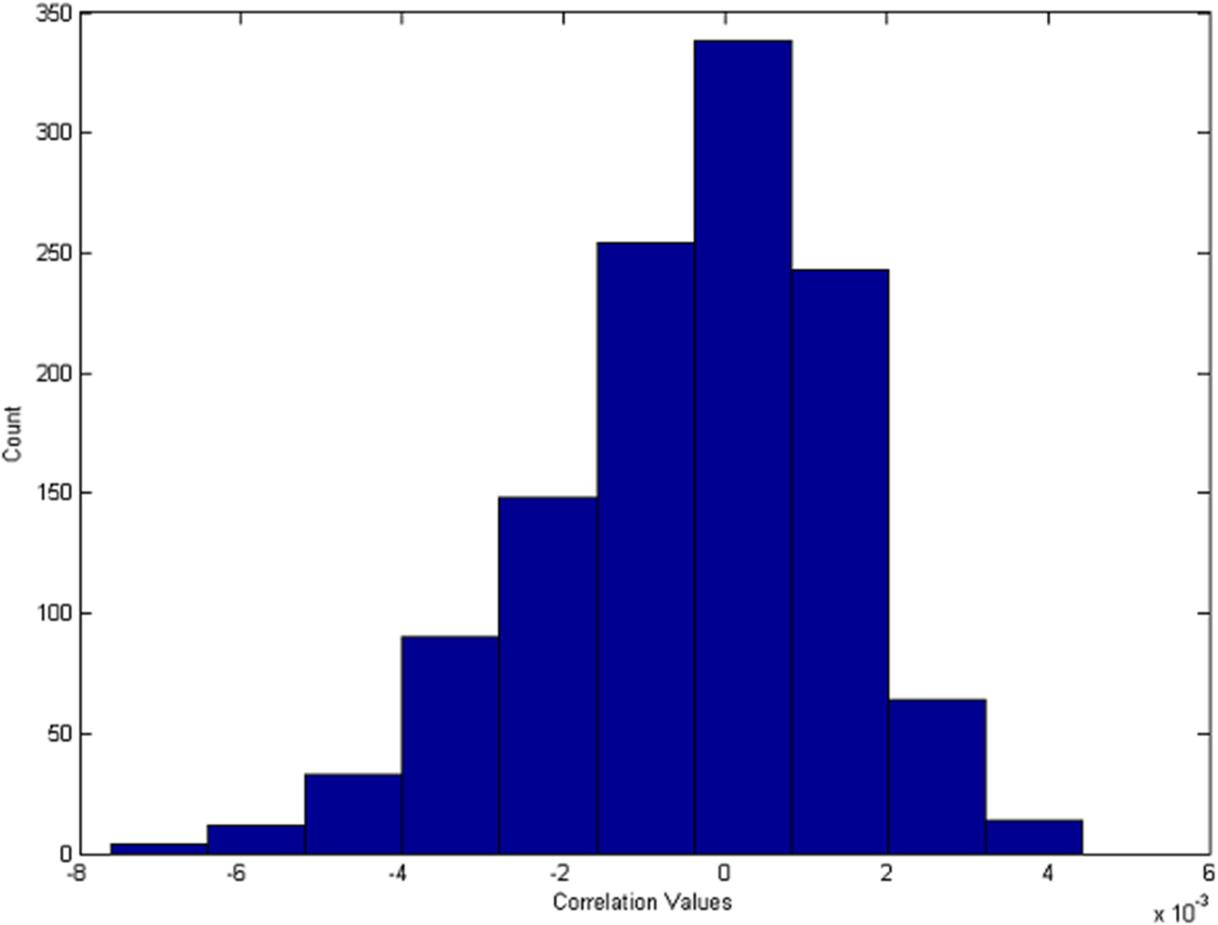


Fig. 5.3.2 Distribution of correlation for 1200 negative sample images with Nikon D200 fingerprintobtained by enhancing the noise residual.

##### TPR and FPR values for different image sizes

We have calculated the TPR and FPR values for four different image sizes cropped from center. As the cropping sizes decreases, True positive rate (TPR) decreases and False positive rate (FPR) increases.

Table 5.3.1 TPR & FPR values for different image sizes cropped from center at Threshold value = 0.0015 (obtained by enhancing the noise residual)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Image Size** | **128x128** | **256x256** | **512x512** | **1024x1024** |
| **TPR** | 0.6800 | 0.8200 | 0.9150 | 0.9750 |
| **FPR** | 0.4150 | 0.2725 | 0.1233 | 0.0292 |

##### ROC Curves

Here we have varied threshold from 1 to -1 with decrement of 0.001. For each threshold, TPR & FPR is calculated. Then the graph between FPR and TPR is plotted with x-axis as FPR & y- axis as TPR as shown in figure 5.3.3. This graph is termed as Receiver Operating Characteristic (ROC). As the cropping sizes decreases, True positive rate (TPR) decreases and False positive rate (FPR) increases. As a result, ROC performance degrades whenever cropping size decreases.

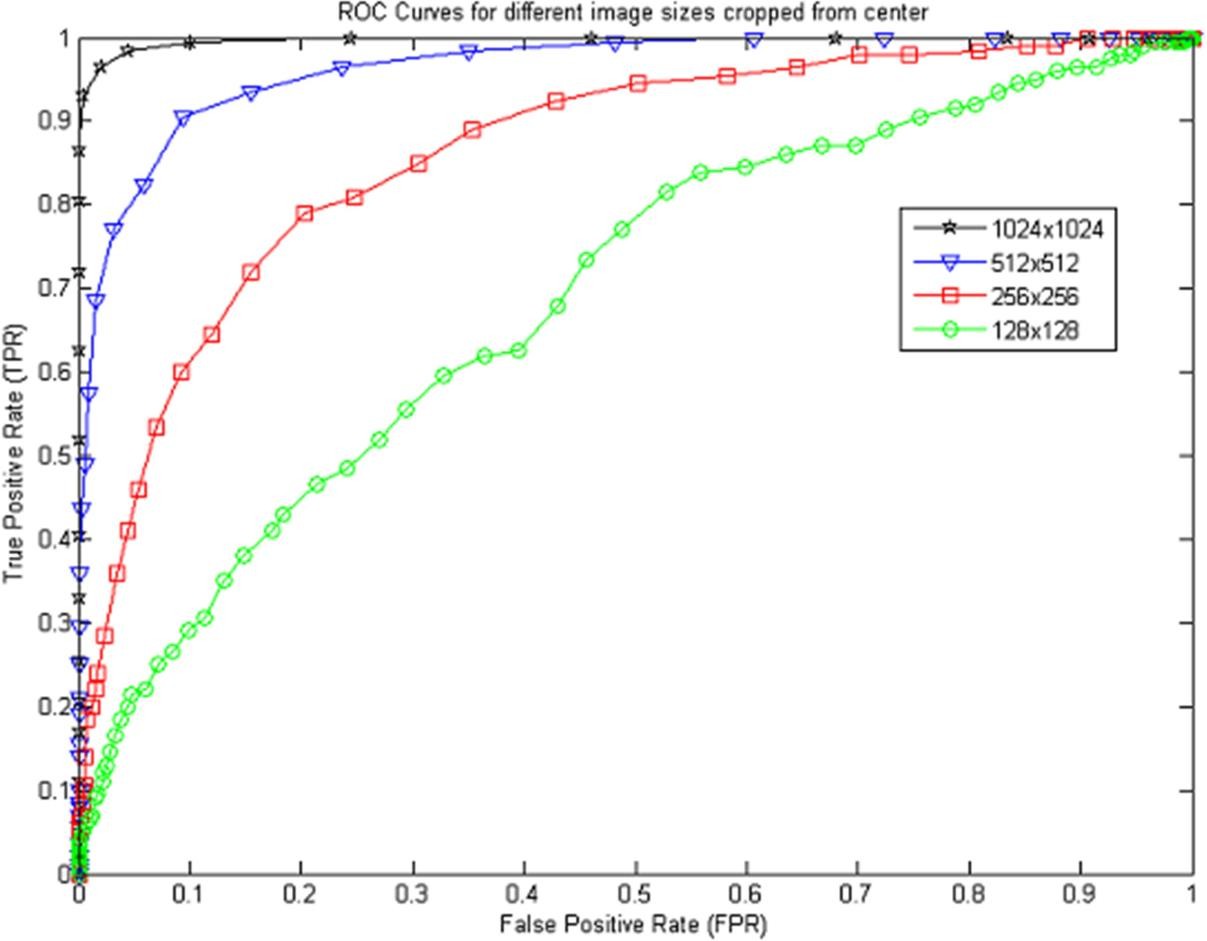


Fig5.3.3 ROC Curves (obtained by enhancing the noise residual)

##### Comparison of both methods

The ROC performance obtained by enhancing the noise residual is better than that of basic SPN (Sensor Pattern Noise) method. It can be seen in figure 5.3.4 that for a fixed threshold the TPR of enhanced noise residual method is always greater than that of basic method and FPR of enhanced method is always less than that of basic method. Here image size taken is 1024x1024. For threshold = 0.0015, we can see in table 5.3.1 & table 4.3.1 that the TPR of enhanced method is always greater and FPR of enhanced method is always lesser than that of basic method.

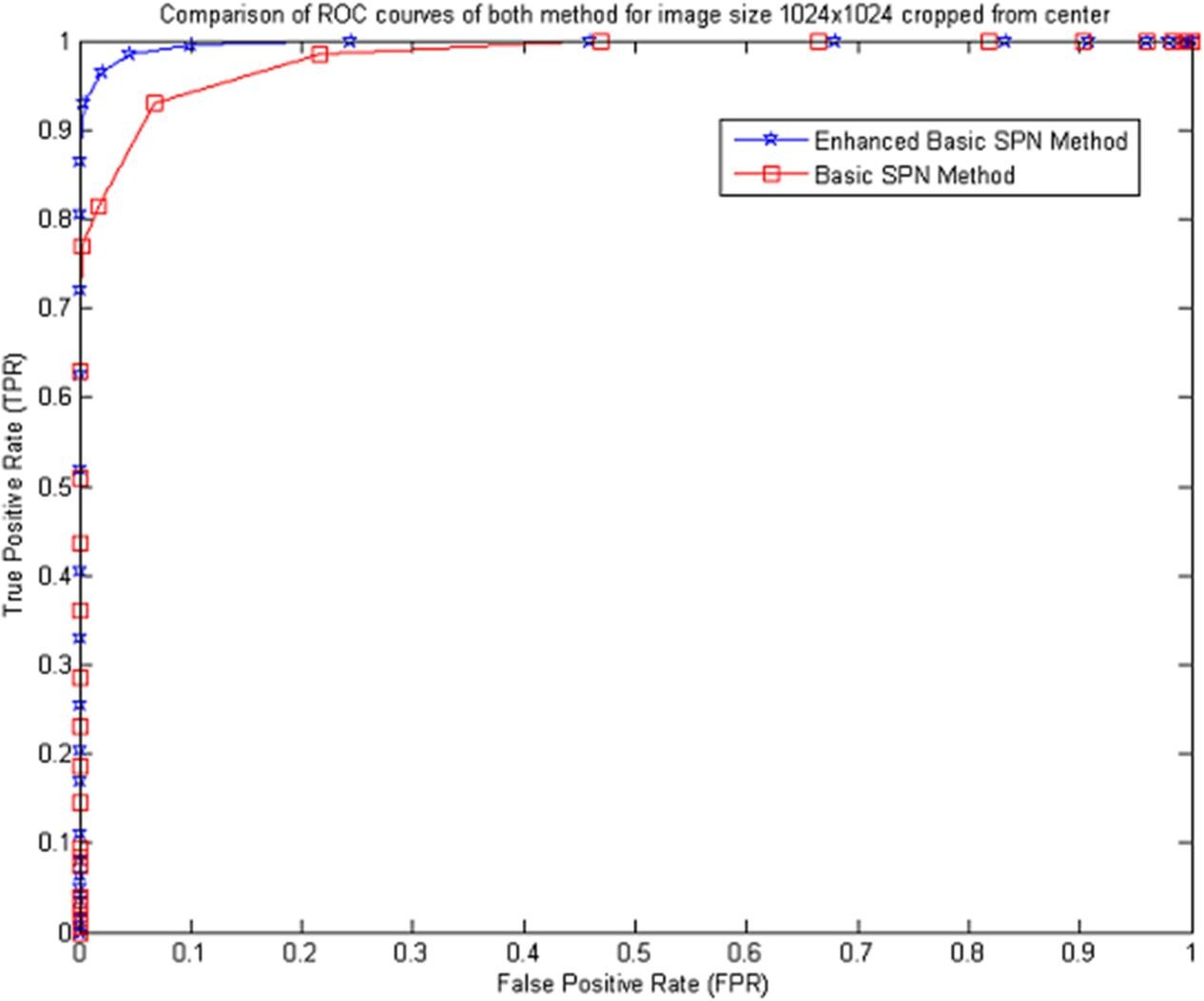


Fig. 5.3.3 Comparison of ROC Curves

## Chapter 6 CONCLUSIONS

In this report I have mentioned the advantage of digital image forensics over digital image watermarking and also observed that digital image forensics is now becoming a hot area of research which opens new problems and investigation threads for researchers. I have discussed the various steps involved in image acquisition. Each step during image acquisition introduces various artifacts in the captured image. Among those artifacts, the sensor pattern noise is able to identify the different camera models as well as different exemplars of the same camera model.

I have implemented two methods to identify source camera. Both of these methods use the sensor pattern noise in identification. Only difference is that in second method the extracted noise residual from sample images is enhanced to suppress the scene details. Because of suppression of scene details TPR of second method i.e. enhanced SPN method is greater than that of method one i.e. basic SPN method. If we compare FPR, FPR of second method i.e. enhanced SPN method is lesser than that of method one i.e. basic SPN method. Hence the ROC performance of enhanced method is better than that of basic SPN method.

## REFERENCES

* + - 1. B. Mahdian, S. Saic, “Blind methods for detecting image fakery,”*IEEE Aerospace Electronics System Magazine*, Vol. 25(4), pp. 18–24, April 2010.
      2. H. Farid, “Digital doctoring: how to tell the real from the fake,” *Significance*, Vol.3(4), pp. 162–166, December 2006.
      3. J. Fridrich,“Image watermarking for tamper detection,” *IEEE Intenational Conference on Image Processing (ICIP)*, pp. 404 –408, October 1998.
      4. B. Mahdian, S. Saic, “Blind methods for detecting image fakery,”*42nd Annual IEEE International Carnahan Conference onSecurity Technology*, pp. 280-286, October 2008.
      5. B.L. Shivakumar, S.S. Baboo, “Detecting copy-move forgery in digitalimages: a survey and analysis of current methods,” *Global Journal of ComputerScience & Technology*, Vol. 10 (7), pp. 61–65, 2011.
      6. J. A. Redi, W. Taktak and et. al., “Digital image forensics: a booklet for beginners”,

*Multimedia Tools and Applications*, Vol. 51(1), pp.133-162, January 2011.

* + - 1. G. C. Holst*, CCD Arrays, Cameras, and Displays*, 2nd ed. Philadelphia, PA: JCD and SPIE Press, 1998.
      2. J. Lukáŝ, J. Fridrich, and M. Goljan, “Digital ‘bullet scratches’ for images,” *IEEE Intenational Conference on Image Processing (ICIP)*, Italy, Sept. 2005.
      3. J. Lukáš, J. Fridrich, and M.Goljan, “Digital camera identification from sensor pattern noise,” *IEEE Trans. Inform. Forensics Security*, vol. 1, no. 2, pp. 205–214, Jun. 2006.
      4. M. Goljan, J. Fridrich, and T. Filler, “Large scale test of sensor fingerprint camera identification,” in *Proc. SPIE*, San Jose, CA, Jan. 18–22, 2009, vol. 7254, pp. 0I 1–0I 12, Electronic Imaging, Media Forensics and Security XI.
      5. M. Chen, J. Fridrich, M. Goljan, and J. Lukáš, “Determining image origin and integrity using sensor noise,” *IEEE Trans. Inform. Forensics Security*, vol. 3, no. 1, pp. 74–90, Mar. 2008.
      6. X. Kang*,*Y. Li and Z. Qu, et. al., "Enhancing source camera identification performance with a camera reference phase sensor pattern noise," *IEEE Trans. Inform. Forensics Security*, vol. 7, no. 2, pp. 393-402, April 2012.
      7. C.-T. Li, “Source camera identification using enhanced sensor pattern noise,” *IEEE Trans. Inform. Forensics Security*, vol. 5, no. 2, pp. 280–287, Jun. 2010.
      8. Y. Tomioka, Y. Ito, and H. Kitazawa, "Digital Camera Identification Based on Pairwise Magnitude Relations of Clustered Sensor Pattern Noise," *IEEE Trans. Inform. Forensics Security*, vol. 8, no. 12, pp. 1986–1995, December 2013.
      9. T. Gloe, R. Böhme, "The Dresden Image Database for Benchmarking Digital Image Forensics," *Proc. of ACM Symposium of Applied Computing*, *SAC*, pp. 1584-1590, March 2010.