iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 10 **Issue:** IV **Month of publication:** April 2022

**DOI:** https://doi.org/10.22214/ijraset.2022.41635

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 10 Issue IV Apr 2022- Available at www.ijraset.com*

# Finger Print Matching Based on Miniature and Phog Feature Extraction

Ankit Sharan
*Jain (Deemed-to-be University) Karnataka*

## I. INTRODUCTION

### A. Overview

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used an identify to individuals and verify their identity. The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate patterns characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies. Optical fingerprint imaging involves capturing a digital image of the print using visible light. This type of sensor is, in essence, a specialized digital camera. The top layer of the sensor, where the finger is placed, is known as the touch surface. Beneath this layer is a light-emitting phosphor layer which illuminates the surface of the finger. The light reflected from the finger passes through the phosphor layer to an array of solid state pixels (a charge-coupled device) which captures a visual image of the fingerprint.

### B. Aim of the Project

The main aim of our project is to give is to give a system a efficient way of identify the people fingerprint in this project all the operation are automated hencethe accuracy high as compared with tradition approach with 95% also it help to reduce thetime taken by traditional approach by 92% with a good friendly user interface

### C. Scope

1) The scope of this project is to provide a more accurate and effective way of identifying people fingerprint
2) It will reduce the time consuming that happen while we are using traditional approachTo provide a Cost-effective system for company and college
3) To reduce the complicated work done when we are using normal way

### D. Problem Statement

1) It is based on the recent study conducted from which we understood the tradition or normalof verifying the fingerprint is a very time consuming and complicated process so to overcome this we had made this system to over all this thing
2) This system will reduce the time consuming which are present in the traditional work
3) It will give a high accuracy rate as compared to traditional system

## II. LITERATURE SURVEY

### A. Title: Determining Image Origin and Integrity

In this paper, we provide a unified framework for identifying the source digital camera from its images and for revealing digitally altered images using photo-response non uniformity noise (PRNU), which is a unique stochastic fingerprint of imaging sensors. The PRNU is obtained using a Maximum Likelihood estimator derived from a simplified model of the sensor output. Both digital forensics tasks are then achieved by detecting the presence of sensor PRNU in specific regions of the image under investigation. The detection is formulated as a hypothesis testing problem. The statistical distribution of the optimal test statistics is obtained using a predictor of the test statistics on small image blocks. The predictor enables more accurate and meaningful estimation of probabilities of false rejection of a correct camera and missed detection of a tampered region. We also include a benchmark implementation of this framework and detailed experimental validation. The robustness of the proposed forensic methods is tested on common image processing, such as JPEG compression, gamma correction, resizing, and denoising.

While digital representation of reality brings unquestionable advantages, digital images can be easily modified using powerful image editing software, which creates a serious problem of how much their content can be trusted when presented as silent witness in a courtroom. Another problem brought by digitization is verification of origin. Is it possible to prove that a certain image was taken by a specific camera? Reliable methods for establishing the integrity and origin of digital images are urgently needed in situations when a digital image or video forms a key piece of evidence, such as in child pornography and movie piracy cases, insurance claims, and cases involving scientific fraud would like to find out which images were obtained using the same camera.

In this paper, we describe a unified framework for both Device Identification and Integrity Verification using pixel PRNU as proposed in [9]. Both tasks start with estimation of the PRNU, which is achieved using a Maximum Likelihood estimator derived from a simplified model of sensor output. This improved estimator makes better use of available data in the sense that the number of images needed to estimate the PRNU can be significantly smaller than what was reported. By establishing the presence of PRNU in an image or in an image block, we can determine the image origin or verify the block integrity. A good analogy is to think of the PRNU signal as a unique authentication watermark involuntarily inserted by the imaging sensor. Establishing its presence in an image amounts to identifying the sensor, while checking its integrity reveals tampered (forged) regions.

The signal processing chain in digital cameras is quite complex and varies greatly with different camera types and manufacturers. It typically includes signal quantization, white balance, demo saicking (color interpolation), color correction, gamma correction, filtering, and, optionally, JPEG compression. Because details about the processing are not always easily available (they are hard-wired or proprietary), we decided to use a simplified model that captures various elements of typical in-camera processing that are most relevant to our task. This enables us to develop low-complexity algorithms applicable to a wider spectrum of cameras. A more accurate model tailored to a specific camera would likely produce more reliable camera identification and forgery detection results at the cost of increased complexity.

The estimated factor contains all components that are systematically present in every image, most importantly some weak artifacts of color interpolation, on-sensor signal transfer and sensor design. Such artifacts are not unique to the sensor and are shared among cameras of the same brand or cameras sharing the same imaging sensor designˆ K2. The PRNU factors estimated from two different cameras may thus be slightly correlated, which would increase the false identification rate and decrease the reliability of camera identification. Therefore, we suppress these artifacts from the estimated factor before using it in our proposed framework. We evaluate how successfully the unwanted artifacts were removed using the correlation between PRNU factors, aiming for the correlation to be as close to zero as possible.

Cameras equipped with a CFA can only capture one color a teach pixel. Due to varying sensitivity of silicone to light of different wavelengths, the sensor output is first adjusted for gain before color interpolation. The remaining colors are interpolated from neighboring pixels. Thus, interpolated colors are obtained through a different mechanism than colors that were truly registered at the pixel. As a result, slightly offset gains may introduce small but measurable biases in the interpolated colors. Since all CFAs form a periodic structure, these biases will introduce a periodic pattern in column and row averages of the estimated factor.

1) *Advantages:* It enables more accurate and meaningful estimation of probabilities of false rejection of a correct camera and missed detection of a tampered region.
2) *Disadvantages:* It cannot be used for Device Identification

*B. Title: Determining Digital Image Origin Using Sensor Imperfections.*

In this paper, we demonstrate that it is possible to use the sensor's pattern noise for digital camera identification from images. The pattern noise is extracted from the images using a wavelet-based denoising filter. For each camera under investigation, we first determine its reference pattern, which serves as a unique identification fingerprint. This could be done using the process of flat-fielding, if we have the camera in possession, or by averaging the noise obtained from multiple images, which is the option taken in this paper. To identify the camera from a given image, we consider the reference pattern noise as a high-frequency spread spectrum watermark, whose presence in the image is established using a correlation detector. Using this approach, we were able to identify the correct camera out of 9 cameras without a single misclassification for several thousand images.

Furthermore, it is possible to perform reliable identification even from images that underwent subsequent JPEG compression and/or resizing. These claims are supported by experiments on 9 different cameras including two cameras of exactly the same model.

In this paper, we ask the following questions: Is it possible to find an equivalent of gun identification from bullet scratches for identification of digital cameras from images? How reliably can we distinguish between images obtained using different sensors or cameras? Is reliable identification possible from processed images?

In classical film photography, there are methods for camera identification that are commonly used in forensic science. Some of these methods use camera imperfections, such as scratches on the negative caused by the film transport mechanism. As digital images and video continue to replace their analog counterparts, reliable, inexpensive, and fast identification of digital image origin increases on importance. Reliable digital camera identification would especially prove useful in the court. For example, the identification could be used for establishing the origin of images presented as evidence, or, in a child pornography case, one could prove that certain imagery has been obtained using a specific camera and is not a computer-generated image.

The process of image identification can be approached from different directions. On the most obvious and simplest level, one could inspect the electronic file itself and look for clues in headers or any other attached or associated information. For example, the EXIF header contains a plethora of direct information about the digital camera type and the conditions under which the image was taken (e.g., exposure, time, etc.). Additional information could be obtained from the quantization table in the JPEG header (some cameras use customized quantization matrices). This header data, however, may not be available if the image is resaved in a different format or recompressed.

Another approach to camera identification is analysis of pixel defects. In the authors point out that defective pixels, such as hot pixels or dead pixels, could be used for reliable camera identification even from lossy compressed images. This approach fails for cameras that do not contain any defective pixels or cameras that eliminate defective pixels by post-processing their images on-board. Also, the defective pixels may not be obvious in every scene and thus, in order to identify the defective pixels, one either needs to have access to the camera or have sufficiently many images from which the defective pixels can be determined.

Proposed a different idea in which a vector of numerical features is extracted from the image and then presented to a classifier built from a training set of features obtained from images taken by different cameras. The feature vector is constructed from average pixel values, correlation of RGB pairs, center of mass of neighbor distribution, RGB pair energy ratio, and it also exploits some small scale and large scale dependencies in the image expressed numerically using a wavelet decomposition previously used for image stego analysis.

This “blind identification” appears to work relatively reliably. Tests on a larger number of cameras could bring a more decisive answer if this approach has a good distinguishing power with respect to different cameras. One of the concerns is whether this method is capable of distinguishing between similar camera models (e.g., models with the same sensor type) or between cameras of the exactly same model. Also, the large number of images needed to train a classifier for each camera may not always be available.

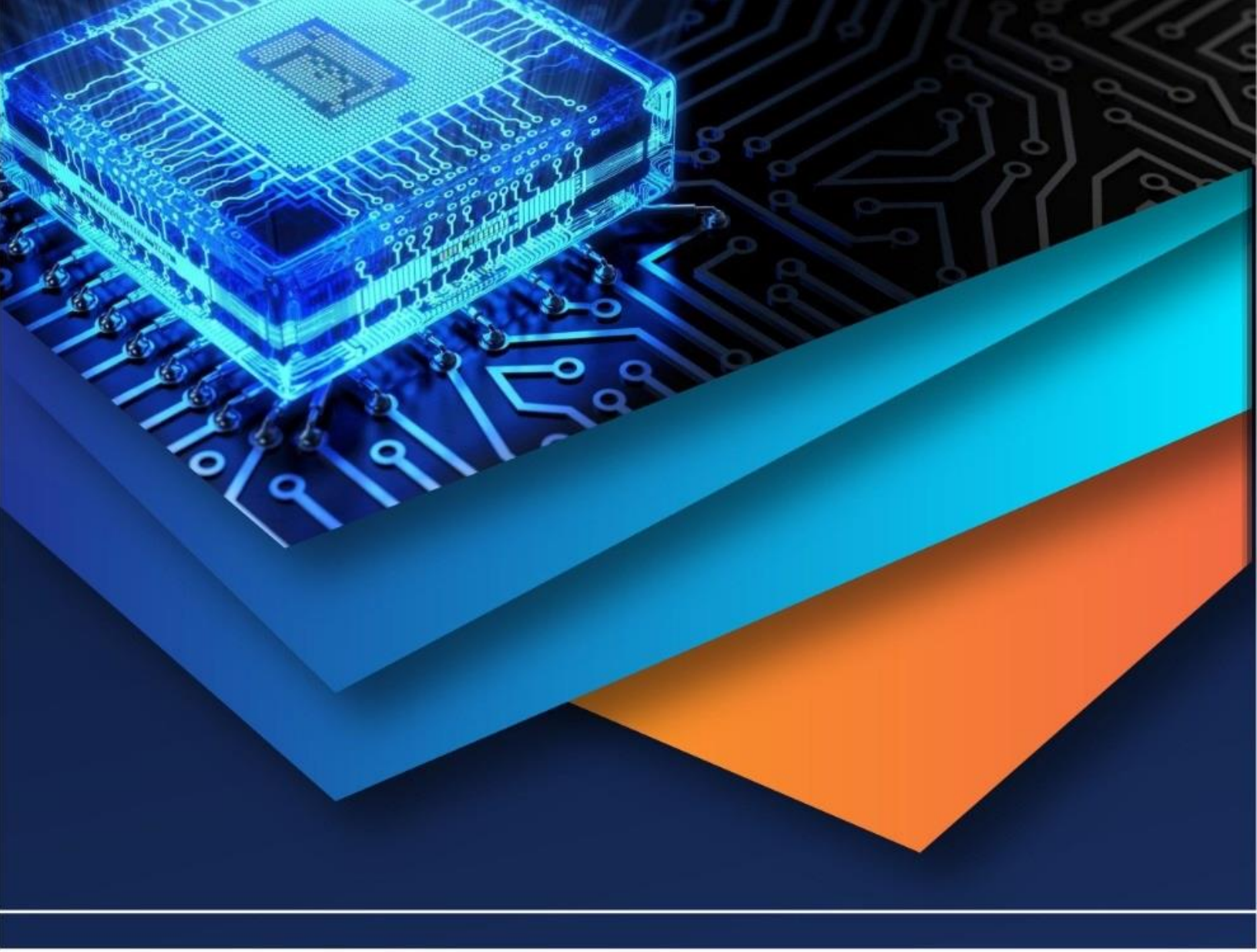
In this paper, we propose another approach to digital camera identification that uses the pattern noise of CCD arrays. The pattern noise is caused by several different factors, such as pixel non-uniformity, dust specs on optics, interference in optical elements, dark currents, etc. Using the denoising filter described in [5], we extract the high frequency part of the pattern noise and then use correlation (as in robust watermark detection using spread spectrum) to evaluate the presence of the pattern noise in the image.

1) *Advantages:* It is possible to use the sensor’s pattern noise for digital camera identification from images.
2) *Disadvantages:* It may not be available if the image is resaved in a different format or recompressed.

## III. SYSTEM ANALYSIS

Matlab is a high-level technical computing language and interactive environment for algorithm development, data visualization, data analysis, and numerical computation. Using MATLAB, you can solve technical computing problems faster than with traditional programming languages, such as C, C++, and Fortran. Matlab is a data analysis and visualization tool which has been designed with powerful support for matrices and matrix operations. As well as this, Matlab has excellent graphics capabilities, and its own powerful programming language. One of the reasons that Matlab has become such an important tool is through the use of sets of Matlab programs designed to support a particular task. These sets of programs are called toolboxes, and the particular toolbox of interest to us is the image processing toolbox. Rather than give a description of all of Matlab's capabilities, we shall restrict ourselves to just those aspects concerned with handling of images. We shall introduce functions, commands and techniques as required. A Matlab function is a keyword which accepts various parameters, and produces some sort of output: for example a matrix, a string, a graph. Examples of such functions are sin, imread, imclose. There are many functions in Matlab, and as we shall see, it is very easy (and sometimes necessary) to write our own.

Matlab's standard data type is the matrix_all data are considered to be matrices of some sort. Images, of course, are matrices whose elements are the grey values (or possibly the RGB values) of its pixels. Single values are considered by Matlab to be matrices, while a string is merely a matrix of characters; being the string's length. In this chapter we will look at the more generic Matlab commands, and discuss images in further chapters.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY