Anti-Forensics of Photo Response Non-Uniformity of Digital Images

Sowmiya N
M.E Applied Electronics, Nandha Engineering College, Erode-52, Tamilnadu, India.

Sadish Kumar S.T
Associate professor/ECE, Nandha Engineering College, Erode-52, Tamilnadu, India.

Abstract – The digital image processing is to be used in Anti-forensics of photo response non-uniformity of digital images. Fingerprints are one of those irregular twists of nature. The fingerprints are used for authentication and identification processes in forensic tasks such as detection of digital forgeries. Forensic tasks can to be performed in device identification problem, device linking problem, fingerprint matching problem. For random projections the compression technique is to be required with no information loss and to be measured by PRNU values. Fingerprint matching is still a challenging problem for reliable person authentication because of the complex distortions involved in two impressions of the same finger.

Index Terms – Random projections, PRNU, image forensics, Wavelet compression.

1. INTRODUCTION

The fingerprint image has to be compressed and encrypted by the authentication and matching purposes in the forensic tasks by using the PSNR values to be reconstructed the original image quality. The digital image processing is to be used for compressed camera fingerprint matching via random projections. Fingerprints are one of those irregular twists of nature. The fingerprints are to be used authentication and identification processes in forensic tasks such as detection of digital forgeries. Forensic tasks can to be performed in device identification problem, device linking problem, fingerprint matching problem. For random projections the compression technique is to be required with no information loss and to be measured by PSNR values.

Recently, several authors [6] started to address the problems related with the management of a large (db) database of camera fingerprints. In [7] and [8], these authors propose a so-called *fingerprint digest*, which works by keeping only a fixed number of the largest fingerprint values and their positions, so that the resulting database is independent of the sensor resolution. An improved search strategy based on fingerprint digest is proposed in [9] and [10]. Fingerprint digests can also be used to ease fingerprint registration in case of geometrically distorted images, as shown in [11].

An alternative solution is to represent sensor fingerprints in binary-quantized form [12]: even though the size of binary fingerprints scales with sensor resolution, binarization can considerably speed-up the fingerprint matching process. In the case of PRNU fingerprints, it is easy to show that preserving the distance between two fingerprints is equivalent to preserving the angle between them. Since PRNU fingerprints of different sensors are known to be highly uncorrelated, and thus to form wide angles, we can expect that also the angles between compressed fingerprints obtained by random projections will be wide. As a consequence, in this paper we adapt the standard correlation detector [1] to solve fingerprint matching and camera identification problems in the compressed domain.

As to practical issues, the complexity of randomly projecting a large fingerprint is greatly reduced by employing partial circulant matrices [15], which are known to be almost as good as fully random matrices. Moreover, inspired both by the work of [12] and by recent results in compressed sensing literature [16], we propose a binary version of the compressed fingerprint that further reduces storage and computational requirements. In Section II, we provide notations and definitions and we briefly review forensic tasks based on PRNU and random projections. The proposed compressive PRNU forensic systems are described in Section III, while theoretical performance is analyzed in Section IV. Extensive numerical results on different datasets are presented and discussed in Section V. Finally, in Section VI we draw some conclusions.

IMAGING sensor imperfections can be considered as a unique fingerprint identifying a specific acquisition device, enabling various important forensic tasks, such as device identification, device linking, recovery of processing history, detection of digital forgeries [1]. The most common camera fingerprint is the photo-response nonuniformity (PRNU) of the digital imaging sensor [2]. The PRNU is due to slight variations in the properties of individual pixels, which producea noise-like, yet deterministic pattern affecting every image taken by a sensor. Several works demonstrate that thsse PRNU is a robust fingerprint, usually surviving processing like lossy compression and image resizing [3], [4]. In the case of PRNU, the camera fingerprint is essentially pattern with the same size as the imaging sensor is due to the wide availability of sensors

counting tens of millions of pixels, a realistic database of a few thousand sensors will require to store more than 1010 individual pixel values in uncompressed format.

In addition, the complexity of looking for a particular fingerprint in a large database is also very high, typically requiring the computation of a correlation with each fingerprint in the database. The issue of compression of PRNU patterns does not arise when the results of device identification have to be used as evidence in the court of law, because that case typically involves small databases and requires the highest accuracy. Instead, large scale problems, such as image classification, clustering or image retrieval problems based on camera identities, involve a huge number of PRNU patterns. Hence, these problems call for techniques to efficiently store and query such databases. Another problem with PRNU fingerprints is that the test image should be geometrically aligned with the fingerprint in the database. A possible solution is to provide several versions of the same fingerprint with different scale and/or cropping factors [5], however at the cost of managing an even larger database.

2. BACKGROUND

1.Notation and Definitions

This is a real-world problem: the Federal Bureau of Investigation (FBI) maintains a large database of fingerprints. The FBI uses eight bits per pixel to define the shade of gray and stores 500 pixels per inch, which works out to about 700 000 pixels and 0.7 megabytes per finger to store finger prints in electronic form. By turning to wavelets, the FBI has achieved a 15:1 compression ratio. In this application, wavelet compression is better than the more traditional JPEG compression, as it avoids small square artifacts and is particularly well suited to detect discontinuities (lines) in the fingerprint. Note that the international standard JPEG 2000 includes the wavelets as a part of the compression and quantization process. This points out the present strength of the wavelets.

We denote (column-) vectors and matrices by lowercase and uppercase boldface characters, respectively. The l-th element of column vector **v** is $v\ell$. The i -th column of the matrix **A** is $\boldsymbol{a_i}$ The notation **A**·**B** denotes the elementwise product between matrices **A** and **B**, while **A**/**B** denotes element wise division.

The notation $\langle (a,b) \rangle$ denotes the scalar product between vectors **a** and **b**, and $\|a\|_2 = \sqrt{(a,a)}$.

The notation dH(**a**, **b**) denotes the Hamming distance between **a**, **b** ∈ {0, 1}m, where dH(**a**, **b**) = $\frac{1}{m} \sum_{i=1}^{m} a_i \oplus b_i$ and ⊕ denotes the XOR operator.

The notation $\mathbf{a} \sim \mathcal{N}(\mu, \Sigma)$means that the random vector **a** is Gaussian distributed, its mean is $\boldsymbol{\mu}$, and its covariance matrix is Σ .

2. PRNU Forensics

PRNU [1], [2] of imaging sensors is a property unique to each sensor array due to the different ability of each individual optical sensor to convert photons to electrons. This difference is mainly caused by impurities in silicon wafers and its effect is a noise pattern affecting every image taken by that specific sensor. Hence, the PRNU can be thought of as a spread–spectrum *fingerprint* of the sensor used to take a specific picture or a set of pictures. The PRNU is multiplicative, *i.e.*, if an imaging sensor is illuminated ideally with a uniform intensity **i**,[1]neglecting other sources of noise, the output of the sensor will be **o = i + I . k** where **k** represents the matrix characterizing the PRNU values.

k exhibits the following properties. It has the same pixel size as the sensor, and carries enough information to make it unique to each sensor. It is universal in the sense that every optical sensor exhibits PRNU. It is present in each picture taken by a sensor except from completely dark ones (due to its multiplicative nature). It is stable under different environmental conditions and is robust to several signal processing operations.

The PRNU characterizing one sensor can be extracted from a set of images (tipically, 20 to 50 smooth images are enough). The procedure to extract the fingerprint **k** of a sensor from a set of pictures depends on the model used to characterize the optical sensor. Denoting with **i** the incident light intensity, the sensor output **o** can be modelled as expressed as given below,

Where as gamma correlation is,

$$\mathbf{o} = g^{\gamma} \cdot [(1 + \mathbf{k}) \cdot \mathbf{i} + \mathbf{e}]^{\gamma} + \mathbf{q}, \qquad (1)$$

where $g\gamma$ is the gamma correction (g is different for each color channel and γ is usually close to 0.45), **e** accounts for other noise sources internal to the sensor while **q** models external noise (*e.g.* quantization). The goal is to extract **k**, so, after keeping the first order term in the Taylor expansion of [*(*1 + **k***)* · **i** + **e**]$^{\gamma}$, the output image can be factorized as

$$\mathbf{o} = \mathbf{o}^{\mathrm{id}} + \mathbf{o}^{\mathrm{id}} \cdot \mathbf{k} + \tilde{\mathbf{e}}, \qquad (2)$$

Where $\mathbf{o}^{\mathrm{id}} = (g\mathbf{i})^{\gamma}$ is the ideal sensor output, **o**id · **k** is the PRNU term and ollects other sources of noise. Assuming to be able to obtain through proper $\tilde{\mathbf{e}} = \gamma\, \mathbf{o}^{\mathrm{id}} \cdot \mathbf{e}/\mathbf{i} + \mathbf{q}$ filtering a denoised version of **o**, referred to as **o**dn,

And then this can be used as an approximation of the ideal sensor output and subtracted from each side of (2) to obtain the so-called *noise residual*, which can be modeled as:

$$\mathbf{w} = \mathbf{o} - \mathbf{o}^{\mathrm{dn}} = \mathbf{o} \cdot \mathbf{k} + \tilde{\mathbf{q}}, \qquad (3)$$

where ˜**q** accounts for ˜**e** and for the non-idealities of the model [1]. Suppose now that a certain number $C \geq 1$ of images is available. Considering the pixels of the noise term ˜**q** as zero–mean Gaussian noise with variance $\sigma 2$ and independent from the signal **o** · **k**, for each image *l*,*l*= 1, . . . ,*C*, it can be written

$$\mathbf{w}^{(\ell)}/\mathbf{o}^{(\ell)} = \mathbf{k} + \tilde{\mathbf{q}}/\mathbf{o}^{(\ell)}, \text{ where } \mathbf{w}^{(\ell)} = \mathbf{o}^{(\ell)} - \mathbf{o}^{(\ell)\mathsf{dn}}. \quad (4)$$

Under the above assumptions, the log–likelihood of **w** $^{(l)}$/**o**$^{(l)}$*n*given **k** satisfies

$$L(\mathbf{k}) = -\frac{C}{2}\sum_{\ell=1}^{C}\log\left(2\pi\sigma^2/(\mathbf{o}^{(\ell)})^2\right) \quad (5)$$

$$+\sum_{\ell=1}^{C}\left(\mathbf{w}^{(\ell)}/\mathbf{o}^{(\ell)} - \mathbf{k}\right)^2 \Big/ \left(2\sigma^2/(\mathbf{o}^{(\ell)})^2\right) \quad (6)$$

from which the maximum likelihood estimate ˆ**k** can be obtained as

$$\hat{\mathbf{k}} = \sum_{\ell=1}^{C}\left(\mathbf{w}^{(\ell)} \cdot \mathbf{o}^{(\ell)}\right) \Big/ \sum_{\ell=1}^{C}(\mathbf{o}^{(\ell)})^2 \quad (7)$$

From the Cramer–Rao bound, the variance of the estimator can be estimated as from which we can notice that good photos for fingerprint evaluation are photos with high luminance (but not saturated) and smooth content (which lowers $\sigma 2$). To improve further the quality of the estimation, artifacts shared among cameras of the same brand or model can be removed by subtracting row and column averages. In the case of color images, the estimation must be performed separately on each color channel, *i.e.*, we must obtain ˆ**k** R, ˆ**k** G and ˆ**k**B. After that, a "global" grayscale PRNU fingerprint will be obtained applying the usual RGB–to–gray conversion.

Several forensic tasks can be performed using the aforementioned model for camera sensors.

$$\sigma^2_{\hat{\mathbf{k}}} = \sigma^2 \Big/ \sum_{\ell=1}^{C}(\mathbf{o}^{(\ell)})^2, \quad (8)$$

$$\hat{\mathbf{k}} = 0.3\hat{\mathbf{k}}_{\mathsf{R}} + 0.6\hat{\mathbf{k}}_{\mathsf{G}} + 0.1\hat{\mathbf{k}}_{\mathsf{B}}. \quad (9)$$

• The *device identification* problem [3] (also known in the biometrics field as *verification*) tests whether a given picture was taken by a specific device. An estimate of the fingerprint of the device has been extracted in advance from a set of training pictures and stored in a database. The noise residual or a single-image fingerprint estimate is extracted from the query image and correlated with the fingerprint in the database. The original detector presented in [4] correlates the noise residual of the query image with the database fingerprint modulated by the query image intensity, denoted as corr*(***w**, **o** · ˆ**k** *)*.* • The *device linking* problem [17] is presented with two images and must determine whether they have been acquired by the same device. The noise residuals of he two photos are correlated, namely corr*(***w**1,**w**2*)*. We ill not discuss this usage case in the remainder of the paper.

• The *fingerprint matching* problem (also known in the\ biometrics field as *identification*) is presented with a database of fingerprint estimates and a set of pictures acquired by the same camera, which can be used to extract a fingerprint estimate. The goal is determine which device in the database (if present) has acquired the given pictures. Essentially, for all fingerprints, and if one fingerpring yields acorrelation that is large enough, it is declared to be correct.

3. EXISTING METHOD

Existing method of compressed fingerprint matching can be done by using tampering detection of the image forensics method and related method such as Demosicing Method with partial derivative correlation model, Multimedia forensics method, Image acquisition source method, Image authentication method , Anti-forensics , Forgery localization method,Computer vision digital forensics method, Compressive sensing method and so on. These methods are the existing method in the fingerprint matching.A general description and motivation for the image features This selected or developed is provided below. Except where noted,

This assessed each predictor variable for both the latent print and the known print. For many variables, This also derived a variable that expressed an interaction or relationship of the values of a variable for the latent and known print combined (such as the ratio of latent print area to the known print area, or the Euclidean sum of contrast variability for the latent and known print combined). For details about the procedures used to derive the measures This used, please see the supplementary materials.

4. PROPOSED METHOD

4.1.1 Introduction of Fingerprint

Fingerprint examiners can specialize and become latent or tenprint examiners or both. A latent examiner focuses on comparing "chance" fingerprints left accidentally at crime scenes or elsewhere, to possible source prints. A tenprint examiner, by contrast, compares fingerprints purposefully collected in controlled circumstances (such as at a police station) with those on file in a database. In police stations, impressions from all ten fingers are often collected on a single sheet, which is why they are called tenprints. Tenprints are also referred to as "known prints" because the identity of the source of the impression is known. The term known print to refer to such prints. Latent prints have to be processed in order to be made visible, and often contain only a portion of a finger or other friction ridge area.

They are often smudged, distorted, and may contain artifacts or noise due to the surface upon which they were left, or as a result of processing. By contrast, known prints are collected in controlled situations where poor impressions can be retaken, so they are typically larger, clearer, and richer in information content than latent images.

For low resolution is based on overlapping and coherences in both fingerprints. For high resolution is based on standard deviation of wavelet coefficients in selection criterion. Further, the image has to be matched by the PRNU values when images can be projected randomly and to be increased the compression ratio.

Figure 4.1.1 .Fingerprint images from the database

Latent prints tend to be highly variable in quality, while known prints generally capture fingerprint information with high fidelity. Known prints are often acquired by law enforcement agencies using ink or a scanner. A sample latent and known print are shown in Figure4.1.1.

4.1.2.Fingerprint minuitae

Minutiae are the discontinuities of the ridges.The fingerprint are one of the irregular twist of nature. Everyone have a different minutiae values for their fingerprint. Hence the fingerprint are using asecurity processes in the forensics tasks and other sources.

Figure4.1.2: Fingerprint Minutiae

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of forensic science. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges.

Explanation of the fingerprint minutiae and the figure show on (figure4.1.2.):

- Ridge-fold.It has short ridge, ridge ending, ridge enclosure
- Spur-prompt-rapid-timely: Spurs, a notch protruding from a ridge.
- Island-land mass : , ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges.
- Core-nucleus,center,interior : The core is the inner point, normally in the middle of the print, around which swirls, loops, or arches center. It is frequently characterized by a ridge ending and several acutely curved ridges.
- Bifurcation-split,divergence,division: Bifurcations, the point at which one ridge divides into two Dots, very small ridges.
- Deltas: Deltas are the points, normally at the lower left and right hand of the fingerprint, around which a triangular series of ridges center.
- Crossovers, two ridges which cross each other.
- Bridges are small ridges joining two longer adjacent ridges.
- Ponds: Ponds or lakes, empty spaces between two temporarily divergent ridges.

In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand. A print from the sole of the foot can also leave an impression of friction ridges.

Deliberate impressions of fingerprints may be formed by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

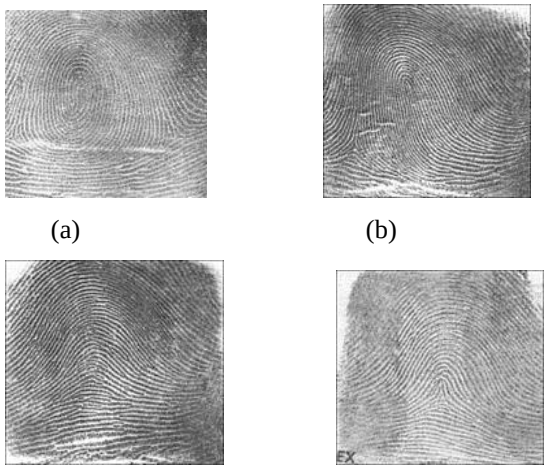
Human fingerprints are detailed, unique difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. They may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify

themselves, as in the aftermath of a natural disaster. Fingerprint analysis, in use since the early 20th century, has led to many crimes being solved.

4.1.3.Classification Of the Fingerprint

Before computerization, manual filing systems were used in large fingerprint repositories. Manual classification systems were based on the general ridge patterns of several or all fingers (such as the presence or absence of circular patterns). This allowed the filing and retrieval of paper records in large collections based on friction ridge patterns alone. The most popular systems used the pattern class of each finger to form a key (a number) to assist lookup in a filing system. Classification systems include the Roscher system, theJuan Vucetich system, and the Henry Classification System. The Roscher system was developed in Germany and implemented in both Germany and Japan, the Vucetich system (developed by a Croatian-born Buenos Aires Police Officer) was developed in Argentina and implemented throughout South America, and the Henry system was developed in India and implemented in most English-speaking countries .

There are three basic fingerprint patterns: loop, whorl and arch, which constitute 60–65%, 30–35% and 5% of all fingerprints respectively There are also more complex classification systems that break down patterns even further, into plain arches or tented arches, and into loops that may be radial or ulnar, depending on the side of the hand toward which the tail points. Ulnar loops start on the pinky-side of the finger, the side closer to the ulna, the lower arm bone. Radial loops start on the thumb-side of the finger, the side closer to the radius. Whorls may also have sub-group classifications including plain whorls, accidental whorls, double loop whorls, peacock's eye, composite, and central pocket loop whorls and the figure show on below figure 4.1.3 .



(a) (b)

(c) (d)

Figure 4.1.3. (a).Arch, (b). Loop(Right Loop), (c).Whorl, (d).Arch(Tented Arch).

Other common fingerprint patterns include the tented arch, the plain arch, and the central pocket loop.

The system used by most experts, although complex, is similar to the Henry System of Classification. It consists of five fractions, in which *R* stands for right, *L* for left, *i* for index finger, *m* for middle finger, *t* for thumb, *r* for ring finger and *p*(pinky) for little finger. The fractions are as follows:

$$Ri/Rt + Rr/Rm + Lt/Rp + Lm/Li + Lp/Lr.$$

The numbers assigned to each print are based on whether or not they are whorls. A whorl in the first fraction is given a 16, the second an 8, the third a 4, the fourth a 2, and 0 to the last fraction. Arches and loops are assigned values of 0. Lastly, the numbers in the numerator and denominator are added up, using the scheme:

$$(Ri + Rr + Lt + Lm + Lp)/(Rt + Rm + Rp + Li + Lr)$$

And a 1 is added to both top and bottom, to exclude any possibility of division by zero. For example, if the right ring finger and the left index finger have whorls, the fractions would look like this:

0/0 + 8/0 + 0/0 + 0/2 + 0/0 + 1/1, and the calculation: (0 + 8 + 0 + 0 + 0 + 1)/(0 + 0 + 0 + 2 + 0 + 1) = 9/3 = 3.

4.2. Identification and Classification of the fingerprint

Fingerprint identification, known as dactyloscopy or hand print identification, is the process of comparing two instances of friction ridge skin impressions (see Minutiae), from human fingers or toes, or even the palm of the hand or sole of the foot, to determine whether these impressions could have come from the same individual.

The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike in every detail; even two impressions recorded immediately after each other from the same hand may be slightly different.

Fingerprint identification, also referred to as individualization, involves an expert, or an expert computer system operating under threshold scoring rules, determining whether two friction ridge impressions are likely to have originated from the same finger or palm (or toe or sole).

4.3.Methodology

4.3.1.Compressed Fingerprint

Fingerprint compression is an application of data compression that encodes the original image with few bits. The objective of image compression is to reduce the redundancy of the image and to store or transmit data in an efficient form. Image compression of the fingerprint by using Discrete Wavelet Transform.

Wavelet transform on Fingerprint Image of size 374-by-388 taken form FVC 2002 Database This have taken this image in two forms i.e. Image without noise and image with noise. Through this paper our aim is to highlight compression ratio achieved in Haar, Daubechies1 and Symlet transforms at third level with varying threshold value. For every threshold value of these transform for both types of images different compression ratio is achieved. This compression ratio is determined on the basis of 2-D Wavelet packet analysis i.e. threshold value, retain energy and number of zeros present in the image after compression. The 2-D Wavelet packet analysis for both noiseless and noisy fingerprint images is shown in Figure 3 highlighted through graphs. Retain Energy (RE) and Number of Zeros (NZ) are calculated by following formulas:

$$RE = \frac{100*(\mathrm{Vn}\,(\mathrm{CCD},2))^2}{(\mathrm{Vn}(origional\ Signal))^2}$$

and

$$NZ = \frac{100*(\mathrm{ZCD})}{No.\ of\ coeificients}$$

Where, Vn is the Vector norm, CCD is the coefficients of the current decomposition and ZCD is the Number of zeros of the current decomposition.

5. EXPERIMENTAL RESULTS

5.1. Input images

The input images are taken from the database FCV2002.This contains the database images of the fingerprint extraction.

The given image has to be converted from the RGB to gray scale conversion.To read the image and show the input image. It has to be marked the thinned values for the minutiae for its morphological function.

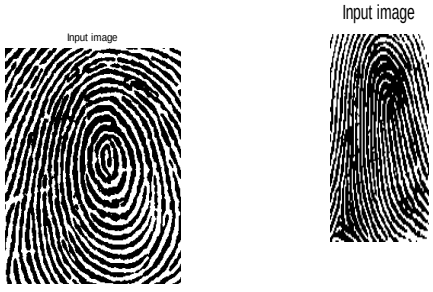


Figure 5.1.1.Simulation of the input image

5.2.Thinned image

It has to be extract easily mark the locations for the minutiae values.

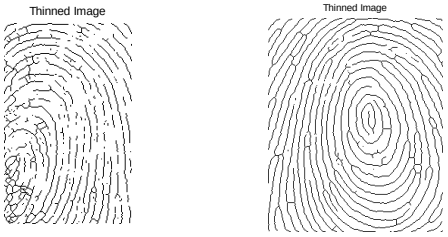


Figure 5.2.1.Simulation of the Thinned image

5.3.Minutiae

To mark the minutiae values are to be marked from specified angles for the minutiae discontinuities.

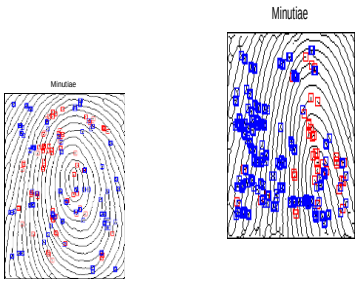


Figure 5.3.1.Simulation of the Minutiae values

5.4.Compressed image

To compress the image by using the wavelet transform (haar transform is used). And its retained energy and number of zeros to be calculated.

Figure 5.4.1.Simulation of the compressed image

5.5.PRNU Values

The PRNU is a Photo Response Non Uniformity. It is the true value of the image quality from its reconstructed value of the given input images.

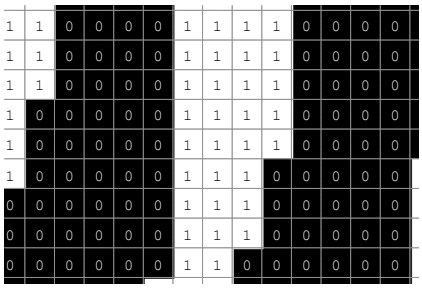


Figure 5.5.1.Simulation of the PRNU Values

The performance of randomly projected fingerprints is analyzed from a theoretical standpoint and experimentally verified on databases of real photographs. Practical issuesconcerning the complexity of implementing random projections are also addressed using circulant matrices.

5.5.Output Result For The Fingerprint GUI

Figure 5.5.1.Output for the binarize and Thinning images

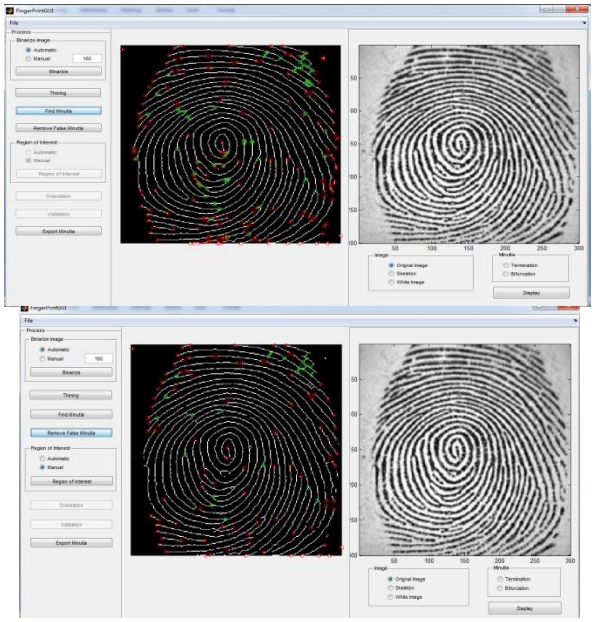


Figure 5.5.2. Output for the find minutiae and remove false minutiae

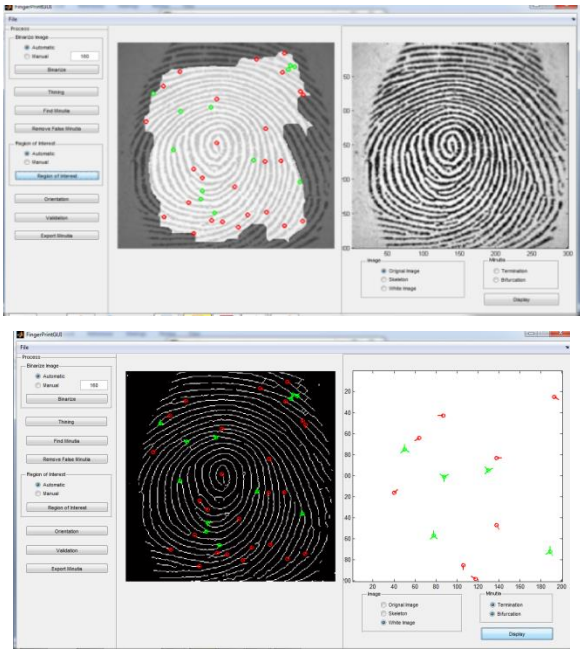


Figure 5.5.3. Output for the Region Of Interest and orientation

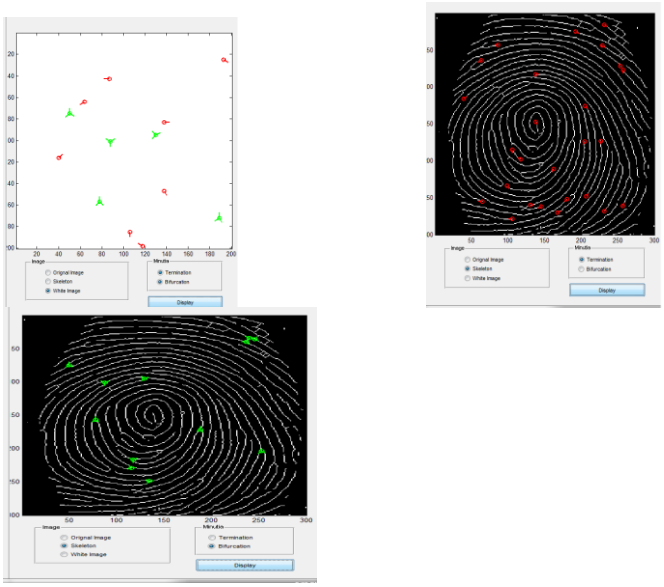


Figure 5.5.4. Output for the plot of the ridges, bifurcation and termination

5.6. Output for the Curve Ftting

The fingerprint images are extracted by using the curve fitting tool for the cftool and so the datasets are taken from its bifurcation and the ridges. These datasets are taken from the same equal lengths and its axes matching. These datasets are further explore its graphically and then it can be fitting by its curves.

- Ex.1. Bifurcation x Vs bifurcation y
- Ex.2. Rides x Vs ridges y

The curvefits are shown below from different fingerprint images collected from the databases such as FVC2002 & FVC2004.

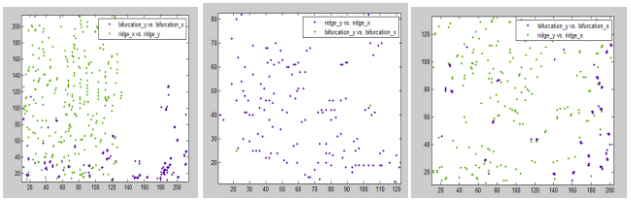


Fig 5.6.1.Output for the curve fits for the different fingerprint images.

The images are matched from its minutiae extraction and its cross correlation value. The images are further reconstruct from its original quality.

Fig.5.7.1.Fingerprint matching for the different images .

5.8. Graphical Representation:

The compressed images had the graphical representations such as residuals, reconstructed images, statistics and denoising effects. These are graphically shown on below.

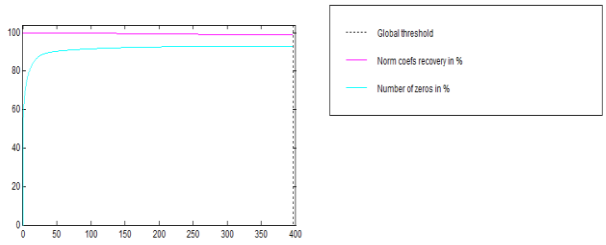


Fig.5.8.1. Global threshold values of fingerprint matching at the compression technique.

An effective approach to performing image reconstruction includes using methods in a technical computing environment for data analysis, isualization, and algorithm d

The arguments `marker` and `mask` can be intensity images or binary images with the same size. The returned image `IM` is the same as the fingerprint, image. Elements of `marker` must be less than or equal to the corresponding elements of `mask`. If values in `marker` are greater than corresponding elements in `mask`, `imreconstruct` clips the values to absolute at the `mask` level. Both input images must be 2-D. The optional connectivity argument (`conn`) can be 4 or 8.

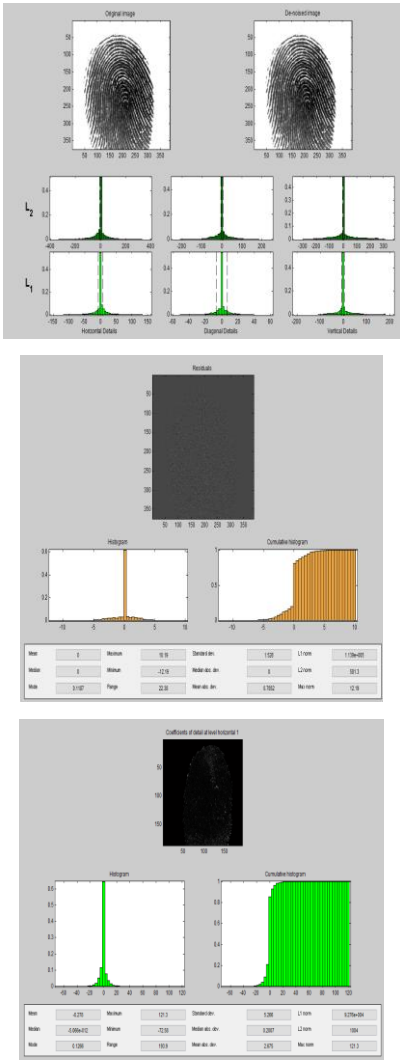
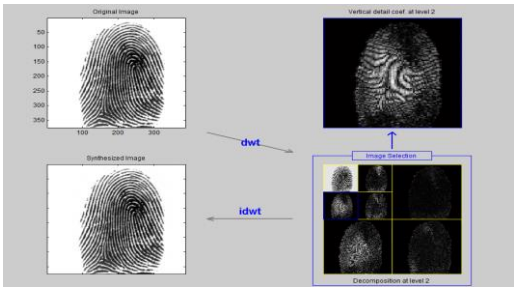


Fig.5.8.2. Denoising effect of the fingerprint images with its statistics



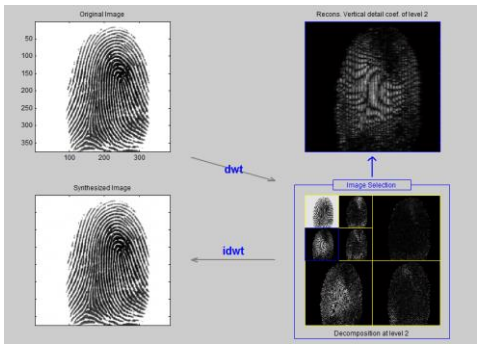


Fig.5.8.3. Reconstruction of the fingerprint images from its compressed images.

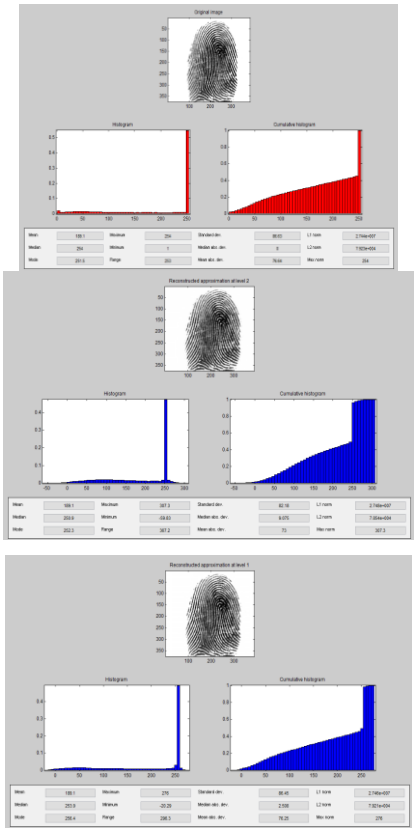


Fig.5.8.4. The approximation level for the reconstruction statistics of the images.

- Reconstruct: Compute wavelet reconstruction using the original approximation coefficients of level N and the modified detail coefficients of levels from 1 to N.
- How to perform the thresholding.

5.8.1.Soft or Hard Thresholding

Thresholding can be done using the function WTHRESH which returns soft or hard thresholding of the input signal. Hard thresholding is the simplest method but soft thresholding has nice mathematical

properties.

Hard thresholding can be described as the usual process of setting to zero the elements FVC2002 absolute values are lower than the threshold. The hard threshold signal is x if x>thr, and is 0 if x<=thr.

Soft thresholding is an extension of hard thresholding, first setting to zero the elements whose absolute values are lower than the threshold, and then shrinking the nonzero coefficients towards 0. The soft threshold signal is sign(x)(x-thr) if x>thr and is 0 if x<=thr.

5.8.2.Image De-Noising

The de-noising method described for the one-dimensional case applies also to images and applies well to geometrical images. The two-dimensional de-noising procedure has the same three steps and uses two-dimensional wavelet tools instead of one-dimensional ones. For the threshold selection, prod(size(y)) is used instead of length(y) if the fixed form threshold is used.

5.8.3.Wavelet Reconstruction

The discrete wavelet transform can be used to analyze, or decompose, signals and images. This process is called *decomposition* or *analysis*. The other half of the story is how those components can be assembled back into the original signal without loss of information. This process is called *reconstruction*, or *synthesis*. The mathematical manipulation that effects synthesis is called the *inverse discrete wavelet transform* (IDWT).

6. CONCLUSIONS

Fingerprints developed for the highest quality and were all identifiable. They were clear and able to be used for identification. The fingerprint matching has to be detected the forgery images, detected the copied images. The Photo Response Non Uniformity values are to be used for these types of detection problem. Hence it has to be calculated from the true value for the original qualities of the images.

The fingerprint images has to be compressed and encrypted by the authentication and matching purposes in the forensic tasks by using the PRNU values to be reconstructed the original image quality. And the random projections of images has to be matched from this method. Correlation based matching has a highest resolution and the high quality of its original image by using the security purposes and forensics tasks.

REFERENCES

[1].Hong cao and alex C. Kot , “accurate detection of demosaicing regularity for digital image forensics”, *IEEE trans.* Information forensics and security., Vol. 4, no. 4,pp.899-910, dec. 2009.

[2].W. Sabrina lin, k. Tjoa, h. Vicky zhao , k. J. Ray liu, "digital image source coder forensics via intrinsic fingerprints", *IEEE trans*, information forensics and security, vol. 4, no. 3, pp-460-475,sep. 2009.
[3].Ashwin Swaminathan, Hongmei Gou and Min Wu, "Intrinsic Sensor Noise Features for Forensic Analysis on Scanners and Scanned Images", *IEEE Trans*, Information Forensics and security, vol. 4, no. 3, pp.476-491, Sep. 2009 .
[4].Yanmei Fang , Ahmet Emir Dirik , Xiaoxi Sun , Nasir Memon ,"Source Class Identification for DSLR and Compact Cameras", *IEEE Trans*, Information Forensics and security,vol.4,no.3,pp .4244-4464,Oct.2009.
[5].Daniel Garcia-Romero and Carol Y. Espy-Wilson,"Automatic Acquisition Device Identification From Speech Recordings", *IEEE Trans*, Information Forensics and security,vol.4,no.3,pp. 4244-4296,Sep.2010
[6].Matthew C. Stamm and K. J. Ray Liu,"Forensic Detection of Image Manipulation Using Statistical Intrinsic Fingerprints", *IEEE Trans*, Information Forensics and security,vol.5,no.3,pp .492-506,Sep.2010.
[7].Weiqi Luo, , Jiwu Huang and Guoping Qiu,"JPEG Error Analysis and Its Applications to Digital Image Forensics", *IEEE Trans*, Information Forensics and security,vol.5,no.3,pp .492-506,Sep.2010.
[8].Matthew C. Stamm and K. J. Ray Liu,"Anti-Forensics of Digital Image Compression", *IEEE Trans*, Information Forensics and security, vol.5,no.3,pp .1050-1065,Sep.2011.
[9].Hung-Min Sun, Chi-Yao Weng, Chin-Feng Lee, and Cheng-Hsing Yang,"Anti-Forensics with Steganographic Data Embedding in Digital Images" *IEEE Trans*, Information Forensics and security,vol.29,no.7,pp .1392-1403,Aug.2011.
[10].Mani Malek Esmaeili, Mehrdad Fatourechi, and Rabab Kreidieh Ward, "A Robust and Fast Video Copy Detection System Using Content-Based Fingerprinting", *IEEE Trans*, Information Forensics and security,vol.5,no.3,pp .213-226,Mar.2011.
[11].Hai-Dong Yuan,"Blind Forensics of Median Filtering in Digital Images", *IEEE Trans*, Information Forensics and security,vol.6,no.4,pp .1335-1345,Dec.2011.
[12].Arun Ross and Asem Othman,"Visual Cryptography for Biometric Privacy",*IEEE Trans*, Information Forensics and security,vol.6,no.1,pp .70-81,Mar.2011.
[13].Chang-Tsun Li, and Yue Li,"Color-Decoupled Photo Response Non-Uniformity for Digital ImageForensics", *IEEE Trans*, Information Forensics and security,vol.22,no.2,pp .260-271,Feb.2012.
[14].Ming Yan, Yi Yang and Stanley Osher, "Robust 1-bit Compressive Sensing using Adaptive Outlier Pursuit" ,*IEEE Trans*, Information Forensics and security,vol.6,no.1,pp .1-8,Mar.2012.
[15].Xiangui Kang, Yinxiang Li, Zhenhua Qu, and Jiwu Huang, "Enhancing Source Camera Identification Performance With a Camera Reference Phase Sensor Pattern Noise", *IEEE Trans*, Information Forensics and security,vol.7,no.2,pp .393-402,Apr.2012.
[16].Hafiz Malik, *Member*,"Acoustic Environment Identification and Its Applications to Audio Forensics", *IEEE Trans*, Information Forensics and security,vol.8,no.11,pp .1827-1837,Nov.2013.
[17].Ahmed F.Shosha, Lee Tobin and Pavel Gladyshev,"Digital Forensic Reconstruction of A Program Actions", *IEEE Trans*, Information Forensics and security,vol.7,no.2,pp .119-122,Nov.2013.
[18].Eryun Liu, Anil K. Jain and Jie Tian,"A Coarse to Fine Minutiae-Based Latent Palmprint Matching" , *IEEE Trans*, Information Forensics and security,vol.35,no.10,pp .2307-2322,Oct.2013.
[19].Giuseppe Valenzise, Marco Tagliasacchi, and Stefano Tubaro, "Revealing the Traces of JPEG Compression Anti-Forensics", *IEEE Trans*, Information Forensics and security,vol.8,no.2,pp .355-349,Feb.2013.
[20].Ahmed F.Shosha, Lee Tobin and Pavel Gladyshev ,"Digital Forensic Reconstruction of A Program Actions" *IEEE Trans*, Information Forensics and security,vol.8,no.2,pp .355-349,Feb.2013.
[21].Eryun Liu, Anil K. Jain, and Jie Tian, "A Coarse to Fine Minutiae-Based Latent Palmprint Matching" *IEEE Trans*, Information Forensics and security,vol.8,no.2,pp .355-349,Feb.2013.
[22].Yoichi Tomioka, and Hitoshi Kitazawa, "Robust Digital Camera Identification Based on Pairwise Magnitude Relations of Clustered Sensor Pattern Noise", *IEEE Trans*, Information Forensics and security,vol.8,no.12,pp .1986-1995,Dec.2013.
[23].Thanh Hai Thai, Rémi Cogranne and Florent Retraint, "Camera Model Identification Based on the Heteroscedastic Noise Model", *IEEE Trans*, Information Forensics and security,vol.8,no.2,pp .355-349,Feb.2013.
[24].Giovanni Chierchiay, Davide Cozzolino, Giovanni Poggi, Carlo Sansone, Luisa Verdoliva,"Guided Filtering For Prnu-Based Localization Of Small-Size Image Forgeries", *IEEE Trans*, Information Forensics and security,vol.22,no.1,pp .250-263,Jan.2014.
[25].Gang Cao, Yao Zhao, Rongrong Ni and Xuelong Li, "Contrast Enhancement-Based Forensics in Digital Images", *IEEE Trans*, Information Forensics and security,vol.9,no.3,pp .515-525,Mar.2014.