Combined Zernike Moment and Multiscale Analysis for Tamper Detection in Digital Images

Thuong Le-Tien, Tu Huynh-Kha, Long Pham-Cong-Hoan, An Tran-Hong
Dept of Electronics and Electrical Eng., Bach Khoa University of Ho Chi Minh City, Vietnam
E-mail: thuongle@hcmut.edu.vn, hktu@hcmiu.edu.vn, phamcong.hoanlong@gmail.com, an.tranhong94@gmail.com

Nilanjan Dey
Techno India College of Technology, Rajarhat, Kolkata, India
E-mail: neelanjandey@gmail.com

Marie Luong
University Paris 13, France
E-mail: marie.luong@univ-paris13.fr

Keywords: wavelet transform, curvelet transform, multiscale analysis, zernike moment, block-based technique, morphological technique, copy-move images

Received: January 12, 2017

The paper proposes a new approach as a combination of the multiscale analysis and the Zernike moment based for detecting tampered image with the formation of copy – move forgeries. Although the traditional Zernike moment based technique has proved its ability to detect image forgeries in block based method, it causes large computational cost. In order to overcome the weakness of the Zernike moment, a combination of multiscale and Zernike moments is applied. In this paper, the wavelets and curvelets are candidates for multiscale role in the proposed method. The Wavelet transform has successful in balancing the running time and precision while the precision of the algorithm applied the Curvelets does not meet the expectation. The comparison and evaluation of the performance between the Curvelets analysis and the Wavelets analysis combining with the Zernike moments in a block based forgery detection technique not only prove the effective of the combination of feature extraction and multiscale but also confirm Wavelets to be the best multiscale candidate in copy-move detection.

Povzetek: Razvita je metoda za pospešitev ugotavljanja prekopiranih ponarejenih slik.

1 Introduction

In the world we are living in, most information is created, captured, transmitted and stored in digital form. It is really the flourished time of digital information. However, the digital information can easily be interfered and forged without being recognized by naked eyes, and thus create a significant challenge when analyzing digital evidences such as images. There are many kinds of counterfeiting images which are classified in two groups: active and passive. The active techniques are known as watermarking or digital signature in which the information of original image is given while there is no any prior information in the passive ones. In recent years, the passive, also called the blind, methods are more interested and challenge the researchers and scientists in the field of image processing and image forensics. And among the manipulations creating faked images in the passive/blind kind, copy-move is the most popular. A copy-move tampered image is created by copying and pasting content within the same image. Nowadays, various software for images processing are getting more sophisticated and easily accessed by anybody. That is why the studies on digital image forgeries are getting more attention lately. Actually, image forgery detection not only belongs to image processing but also is a field of image security. Standing out from other studies, the researches about Zernike moments had shown its advance in detecting forged region in copy-move digital image forgery. The Zernike moment has proved to be superior compare to other types of moment; however the Zernike moment based algorithm requires a large computational cost [. In addition to the moments, studies about the multiscale analyses have long been applied to digital signal processing due to their advantages. A proposed method using a combination of the Zernike moment and the Wavelet transform has been studied and evaluated [1] in which the Wavelets analysis has been used in order to reduce the computational cost of the Zernike moment based technique. The combination of the Zernike moment and the Wavelets has shown its feasibility in detecting the copy-move forgeries and the reduction in running time of the algorithm. An example of a typical copy-move forgery image is shown in Figure 1.

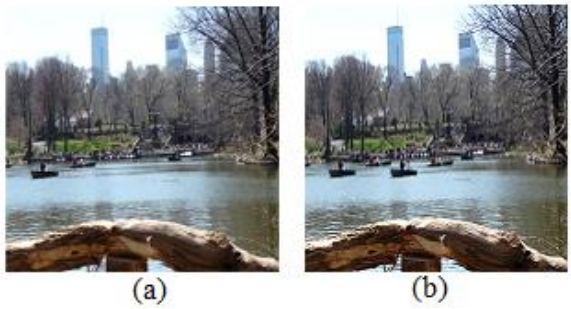


Figure 1: Example image of a typical copy-move forgery; (a). the original image; (b). the tampered image [2].

In this study, the Curvelets is also used to combine with the Zernike moment based technique instead of the Wavelets because of the ability to represent the curves of the objects. A block based technique using the Zernike moment to extract feature for the image forgery detection is used. However, instead of the original testing images, the images which pre-processed by the multiscale analysis is going to be used to calculate the Zernike moments. The goal of this paper is to evaluate the performance of the Wavelets and Curvelets in different perspectives and to examine which multiscale representation is more suitable with the Zernike moment based for detecting copy-move tampered images. The experiments are simulated on MATLAB R2013a with.

2 Related works

In which images' feature extraction techniques are divided into two groups: extracting features directly with and without transformation. And from which, we also chose Zernike moments based techniques for further research. Suggested by Seung – Jin Ryu et al. in [3], Zernike moments technique has advance in feature representation capability, rotation invariance, fast computation, multi-level representation for describing shapes of patterns and low noise sensitivity. The disadvantage of this technique is that it's weak against scaling and other tampering type based on affine transform and it has high computational cost.

Generally, copy – move forgeries detection using block based techniques requires 7 steps [4]; the steps go from dividing the input image into overlapping blocks then calculate features of blocks and final steps are comparing blocks for forgery detection. From [1], a combination between Zernike moments and Wavelet transform was applied to reduce the running time while keeping precision of the original algorithm. Another approach from [5] uses neighborhood sorting, in which G. Li et al. used the Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). As discussed in the introduction, Wavelet transform based techniques has weakness in processing objects in detailed image with lines and curves, and to work-around that disadvantage, the Curvelet transform was propose [6, 7] by Candès and Donoho in 2000 as a Multi-resolution geometric analysis. The base theory of the Curvelet transform is The Ridgelets transform, proposed by the same authors. The Curvelet transform was born to analyze local line or curve singularities, which were a difficulty for original Ridgelets. The Curvelet transform allows an almost optimal sparse representation of objects with singularities along smooth curves. Recently, Ying et al. [8] has extended the Curvelet transform to three dimensions. Comparing with Wavelets, the Curvelets in image processing is still new and also a new orientation [6–15].

In this paper, we will carry out and comparison and evaluation of two combinations that are: Zernike moments based technique and Wavelet transform, the other is Zernike moments based technique and Curvelet transform; in order to examine which multiscale representation is more suitable with the Zernike moment based for detecting copy-move tampered images.

3 Methodology

The main purpose of paper is developing an algorithm to balance the running time and exactness using a combination of multiscale and feature extraction, from which the performances of multiscale methods are evaluated to propose the most suitable multiscale method in image forgery detection. The workflow of the copy-move image forgery detection algorithm is shown in Figure 2. In the pre-processing step, the tampered image is going through some morphological techniques after converted into the grayscale. The foreground component is extracted and divided into overlapping blocks of the same size before going to the next step. The Curvelet transform or the Wavelet transform will be applied to analyze the image before extracting features by Zernike moments. The detection results are concluded using the Euclidean distances of each pair of blocks if they are lower than a threshold. Taking account to the similarity between neighbour blocks, the actual distances of a pair of blocks must higher than a threshold before the algorithm can conclude them as the copy-move regions.

3.1 Pre-processing

The tampered images will be converted into gray scale before enhancing by the morphological techniques and extracting the foreground components. Moreover, by converting to gray scale, the computational cost of the Zernike moment will be reduced since we only need to calculate the Zernike moment in one dimension instead of three color dimensions in the color images.

Morphological processing for gray scale images requires more sophisticated mathematical development. For binary image, the pixel has only two values are bit 1 and bit 0, black and white; in gray scale image, pixels have their scale from 0 to 255. Therefore, the operation requires more works. Structuring elements in grayscale morphology come in two categories: non-flat and flat [16]. To reduce the redundant information in background and concentrate in searching the information of the objects belonging to foreground only, a foreground extraction is applied. Among the morphological functions that used for extracting the foreground

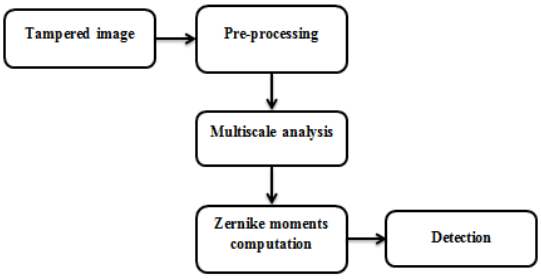


Figure 2: Block diagram of the algorithm.

components such as dilation, erosion, image filling, etc, a combination of dilation and erosion can build all other operations [11].

The dilation of *f* by a flat structuring element (SE) *b* at any location *(x, y)* is defined as the maximum value of the image in the window outlined by $\hat{b}$ when the origin of is $\hat{b}$ at *(x, y)*. That is:

$$[f \oplus b](x,y) = \max_{(s,t)\in b}\{f(x-s, y-t)\} \quad (1)$$

When we used that

$$\hat{b} = b(-x,-y) \quad (2)$$

Where, similarly to the correlation, *x* and *y* are incremented through all values required so that the origin of *b* visits every pixel in *f* . That is, to find the dilation of *f* by *b*, the structuring element is reflected about the origin. The dilation is the maximum value of *f* from all values of *f* in the region of *f* coincident with *b*.

For a non-flat structuring element b_N, the dilation of *f* is defined as:

$$[f \oplus b_N](x,y) = \max_{(s,t)\in b_N}\{f(x-s, y-t) + b_N(s,t)\} \quad (3)$$

Since we add values to *f* , the dilation with a non-flat SE is not bounded by the values of *f*, which may present a problem while interpreting results. Grayscale SEs are rarely used.

The erosion of *f* by a flat structuring element *b* at any location *(x, y)* is defined as the minimum value of the image in the window outlined by $\hat{b}$ when the origin of $\hat{b}$ is at *(x, y)*. Therefore, the erosion at *(x, y)* of an image *f* by a structuring element *b* is given by:

$$[f \Theta b](x,y) = \max_{(s,t)\in b}\{f(x+s, y+t)\} \quad (4)$$

The explanation is similar to one for dilation except for using minimum instead of maximum and that we place the origin of the structuring element at every pixel location in the image.

Similarly, the erosion of image *f* by non-flat structuring elements b_N is defined as the following equation:

$$[f \Theta b_N](x,y) = \max_{(s,t)\in b_N}\{f(x+s, y+t) - b_N(s,t)\} \quad (5)$$

Erosion and dilation, separately, are not very useful in gray-scale image processing. These operations become powerful when used in combination to develop high-level algorithms.

In the image, the components differ greatly from the background image can be segmented. Operators that can calculate the gradient of the image can be used to detect the changes in contrast. Therefore, the edges of the input can be extracted easily and are then processed by dilation and filling holes to create the mask, which is call binary gradient mask, for extracting the foreground component (see Figure 3).

(a) (b) (c)

Figure 3: Example of creating the mask from an input image; (a). Input image; (b). Binary gradient mask; (c). Mask that used to extract foreground component [2].

3.2 Wavelets analysis

According to [11, 17-31], the Wavelet transform is easier to compress, transmit and analyze in image processing compared to the Fourier transform. The Wavelets analysis can be used in order to divide the information of the image into approximation and detail sub-signal. The general trend of pixel values is shown in the approximation sub-band while the three detail sub-bands are so small that they can be neglected. Therefore, it is feasible to use just the approximation sub-band to detect the image forgery. Figure 4 shows the steps to get the approximate image from an original image.

According to [11], the two-dimensional images which requires a two-dimensional scaling function, $\varphi(x, y)$, and three two-dimensional wavelets, $\psi^H(x, y)$, $\psi^V(x, y)$ and $\psi^D(x, y)$. They are the product of one-dimensional scaling function φ and corresponding wavelet ψ,

$$\varphi(x,y) = \varphi(x)\varphi(y) \quad (6)$$

$$\psi^H(x,y) = \psi(x)\varphi(y) \quad (7)$$

$$\psi^V(x,y) = \varphi(x)\psi(y) \quad (8)$$

$$\psi^D(x,y) = \psi(x)\psi(y) \quad (9)$$

In which ψ^H measures variations along horizontal

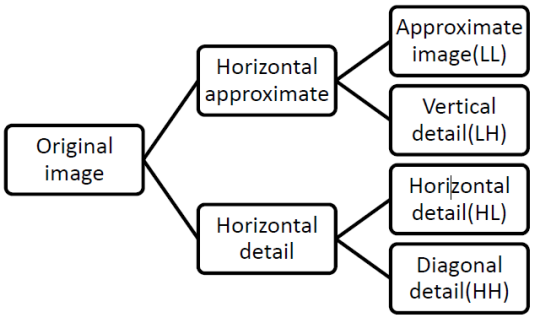


Figure 4: Wavelets transform block diagram.

edges, ψ^v measures variations along vertical edges and ψ^D measures variations along diagonals. After finding two-dimensional scaling and wavelet functions, based on one-dimensional discrete wavelet transform, we define the scaled and translated basis functions:

$$\varphi_{j,m,n}(x,y) = 2^{j/2}\varphi(2^j x - m, 2^j y - n) \quad (10)$$

$$\psi^i_{j,m,n}(x,y) = 2^{j/2}\varphi(2^j x - m, 2^j y - n) \quad (11)$$

$$W_\varphi(j_0,m,n) = \frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\varphi_{j0,m,n}(x,y) \quad (12)$$

$$W^i_\psi(j,m,n) = \frac{1}{\sqrt{MN}}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)\psi^i_{j,m,n}(x,y) \quad (13)$$

i = {H, V, D}, where j_0 is an arbitrary starting scale and the $W_\varphi(j_0,m,n)$ coefficients define an approximation of f(x, y)at scale j_0. The $W^i_\psi(J, m, n)$ coefficients add horizontal, vertical, and diagonal details for scales $j \geq j_0$. Normally we let $j_0 = 0$ and select $N = M = 2^J$ so that we can get $j = 0, 1, 2..., J - 1$ and $m, n = 0, 1, 2, \ldots, 2^J - 1$. Given the W_φ and W^i_ψ of 2 equations (12) (13), $f(x, y)$ is obtained by inverse discrete wavelet transform [11].

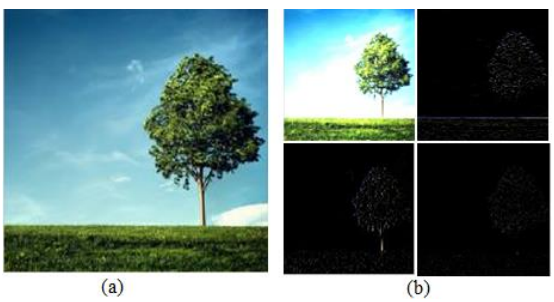
$$f(x,y) = \frac{1}{\sqrt{MN}}\sum_m\sum_n W_\varphi(j_0,m,n)\varphi_{j0,m,n}(x,y) + \frac{1}{\sqrt{MN}}\sum_{i=H,V,D}\sum_{j=j0}^{\infty}\sum_m\sum_n W^i_\psi(j_0,m,n)\psi_{ij,m,n}(x,y) \quad (14)$$

The wavelet transform used in the algorithm is selected from the Wavelet families, such as "db1", "haar", "db2",…with similar results. Optionally, the wavelets "haar" is used to demonstrate wavelets transform level 1 in Figure 5.

From the Figure 5, the reduction in size of the approximate image which analyzed by the Wavelet transform can be clearly seen. The approximate image is only a quarter of the original image.

3.3 Curvelets analysis

In this research, the first generation of the Curvelet transform is used to analyze the image. From [6, 7, 32], the idea of the first generation Curvelet transform is to decompose the image into a set of wavelet bands and analyze each band by a local Ridgelet transform as shown on Figure 6. Different sub-bands of a filter bank



(a) (b)

Figure 5: Image analyzed using Wavelet transform level 1; (a). Original image, (b). The approximate and detail images after applying the Wavelet transform [2].

output are represented by different levels of Ridgelet pyramid. Moreover, a relationship between the width and length of the crucial frame elements is contained in this sub-band decomposition. The first generation discrete Curvelet transform of a continuous function $f(x)$ is making use of a dyadic sequence of scales and a bank of filters with characteristic that the band bass filter Δ_j is concentrated near the frequencies of $[2^{2j},2^{2j+2}]$, as follow:

$$\Delta_j(f) = \Psi_{2^j} * f \quad (15)$$

$$\hat{\Psi}_{2^j}(v) = \hat{\Psi}(2^{-2j}v) \quad (16)$$

Following the research in [33,34], the decomposition of the first generation discrete Curvelet transform is a sequence of the following steps:

Sub-band decomposition: Decomposing the object f into sub-bands.

$$f \to (P_0 f, \Delta_1 f, \Delta_2 f, ...) \quad (17)$$

Each layer contains details of different frequencies. P_0 is low pass filter, Δ_1, Δ_2,… are high-pass (band-pass) filters. The sub-band decomposition can be approximated using the well-known wavelet transform; f is decomposed into S_0, D_1, D_2, D_3, etc. $P_0 f$ is partially constructed from S_0 and D_1, and may include also D_2 and D_3. $\Delta_s f$ is constructed from D_{2s} and D_{2s+1}.

Smooth partitioning: The sub-bands are smoothly windowed into squares of a suitable scale. The scale is optional, but in the proposed method, the scale is 2 to reduce the size of image by a half corresponding to a wavelets decomposition level 1. A grid of dyadic squares is defined as.

$$Q_{(s,k_1,k_2)} = \left[\frac{k_1}{2^s}, \frac{k_1+1}{2^s}\right] \times \left[\frac{k_2}{2^s}, \frac{k_2+1}{2^s}\right] \in Q_s \quad (18)$$

Where, Q_s is all the dyadic squares of the grid. Let w be a smooth windowing function with "main" support of size $2^{-s}x2^{-s}$. For each square, w_Q is a displacement of w localized near Q. Multiplying $\Delta_s f$ with w_Q ($\forall Q \in Q_s$) produces a smooth dissection of the function into "squares".

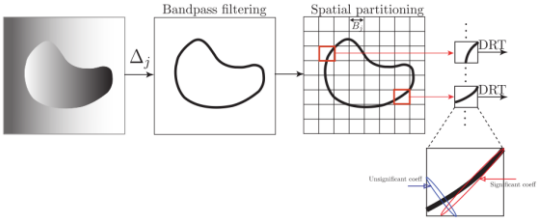


Figure 6: Local Ridgelet transform on bandpass filtered image. The red ellipse is significant coefficient while the blue one is insignificant coefficient [6].

$$h_Q = w_Q \cdot \Delta_s f \quad (19)$$

Renormalization: is centering each dyadic square to unit square. For each Q, the operator T_Q is defined as:

$$(T_Q f)(x_1,x_2) = 2^s f(2^s x_1 - k_1, 2^s x_2 - k_2) \quad (20)$$

Each square is renormalized:

$$g_Q = T_Q^{-1} h_Q \quad (21)$$

Ridgelet analysis: DRT is used to analyze each square.

$$\alpha_{(Q,\lambda)} = \langle g_Q, \rho_\lambda \rangle \quad (22)$$

In which the Ridgelet element has a formula in the frequency domain as:

$$\hat{\rho}_\lambda(\xi) = \frac{1}{2}|\xi|^{-\frac{1}{2}}\left(\hat{\psi}_{j,k}(|\xi|)\cdot\omega_{i,l}(\theta)+\hat{\psi}_{j,k}(-|\xi|)\cdot\omega_{i,l}(\theta+\pi)\right) \quad (23)$$

Where, $\omega_{i,l}$ are periodic wavelets for $[-\pi,\pi)$. i is the angular scale and $l\in[0,2^{i-1}-l]$ is the angular location. $\psi_{j,k}$ are Meyer wavelets for $\Re$. j is the Ridgelet scale and k is the Ridgelet location.

Below is an example result for the Curvelet transform with scale of 2 and the image's edges are shown (see Figure 7).

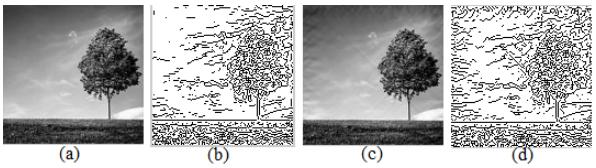


Figure 7: Image analyzed using the Curvelet transform. (a), (b) Original image and its edges; (c), (d) Image processed with scale of 2 and its edges [2].

3.4 Zernike moment's properties

According to the relative research paper about Zernike moments in [3, 35], we can summarize the Zernike moments through some mathematical background. In this section, we describe the Zernike moments as following functions.

The 2D Zernike moment of order n with repetition of m for a continuous image function f(x,y) that vanishes outside the unit circle is:

$$Z_{nm} = \frac{n+1}{\pi}\iint_{x^2y^2\le 1} f(x,y)V_{nm}^* \quad (24)$$

Where n is a non-negative integer and m is an integer such that (n-|m|) is non-negative and even. The 2D Zernike moment, $V_{nm}(\rho,\theta)$ is defined in polar coordinate (ρ,θ) inside the unit circle as:

$$V_{nm}(\rho,\theta) = R_{nm}(\rho)\exp(jm\theta) \quad (25)$$

Where $R_{nm}(\rho,\theta)$ is the n-th order of Zernike radial polynomial given by:

$$R_{nm}(\rho) = \sum_{k=0}^{(n-|m|)/2}(-1)^k \frac{(n-k)!}{k!\left[\frac{n-2k+[m]}{2}\right]!\left[\frac{n-2k-[m]}{2}\right]!}\rho^{n-2k} \quad (26)$$

Zernike moments have rotational invariance, and can be made scale and translational invariant, making them suitable for many applications. Zernike moments are accurate descriptors even with relatively few data points. Reconstruction of Zernike moments can be used to determine the amount of moments necessary to make an accurate descriptor. Though the complexity of the computation process compared to geometric and Legendre moments, Zernike moments have proved to be better in terms of their feature representation capability, rotation invariance, multi-level representation for describing the shapes of patterns and low noise sensitivity [3].

3.5 Forgery Detection Conclusion

After calculating Zernike moments, to remove the similar features due to neighbor blocks, the Euclidean distance of each pair of Zernike will be calculated and compare to a threshold D_1 [3]. This threshold is often set equal to the size of a block. In addition to Euclidean distance, the actual distance of each pair of blocks is also calculated in order to avoid the miss-detection between neighbor blocks.

$$\sqrt{\sum(Z_p - Z_{p+1})} < D_1 \quad (27)$$

$$\sqrt{(i-k)^2+(j-l)^2} > D_2 \quad (28)$$

Where $Z_p = V_{ij}$ and $Z_{p+1} = V_{kl}$. Using these equations, the testing blocks are determined if they are tampered region or not.

4 Proposed system

The paper develops an algorithm to detect the forged regions in term of copy-move in images by using the combination of the multiscale analysis and the Zernike moment based technique. Using this algorithm, the performance of the Wavelet transform and the Curvelet transform will be compared and evaluated at pixel level.

The test image is firstly converted to grayscale before extracting foreground using a binary gradient mask which is created by a combination of dilation and erosion. A wavelet transform decomposition level 1 or a fast discrete curvelet transform (FDCT) is applied to the image which is extracted foreground. In case of 1 level DWT, only the approximation subband is considered. The approximation or an image with FDCT is then divided into many overlapping blocks. The blocks' features are collected by calculating their Zernike moments. The Euclidean and actual distance are also calculated to make sure that they are similar, but not neighbors. Vectors satisfying the constraints in two above distances will be considered the suspicious vectors. Blocks corresponding to these vectors are candidates of copied regions. The flowchart is shown in Figure 8.

From a personal collection and database in [2], we choose 12 images with different characteristics and sizes to conduct our experiments. Figure 9 shows the images used in the experiments. The images have different sizes and features. The smallest images have size of 128x128 while the largest have sizes of 1440x1440. Some of them have very little detail on background while the others have detailed background. The purpose of this is that we can conduct experiments on different types of images for diversity.

Error measurement

At pixel level, the important measures are the number of correctly detected forged pixels, T_P, the number of pixels that have been erroneously detected as forged, F_P, and the falsely missed forged pixels F_N. From these

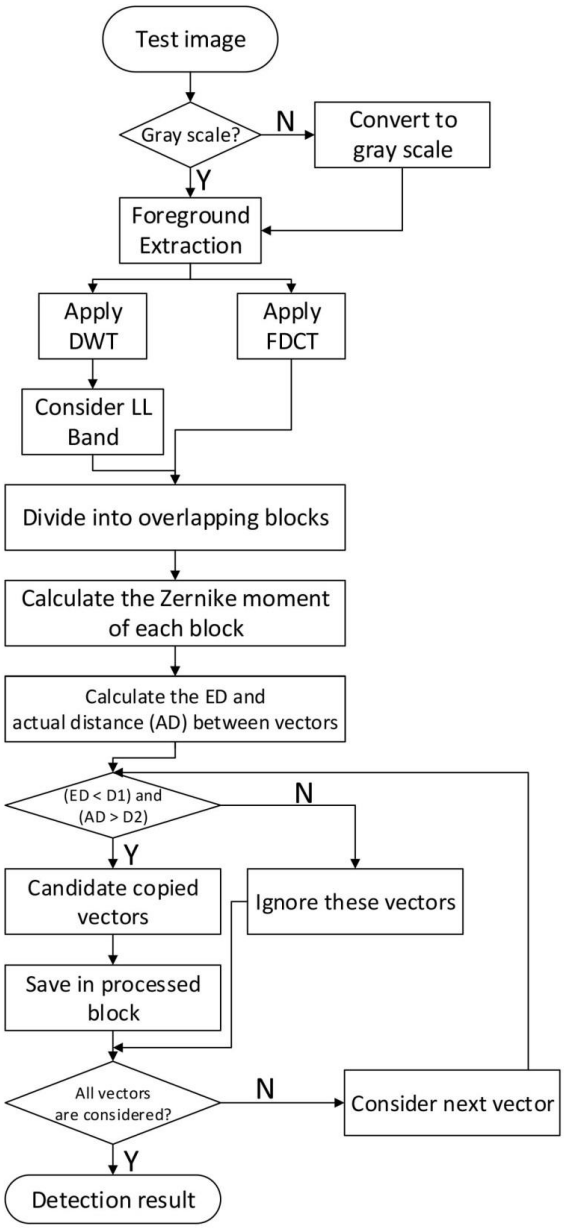


Figure 8: Flowchart of the proposed method.

parameters, we can compute the measure *precision p* and *recall r*. They are defined as:

$$p = T_p / (T_p + F_p) \tag{29}$$

$$r = T_p / (T_p + F_N) \tag{30}$$

Precision shows the probability that a detected forgery is truly a forgery, while the recall or true positive rate expresses the probability that a forged pixel is detected. The trade-off between the precision and recall exists; hence, to consider both precision and recall together, F is the combination of precision and recall in a single value.

$$F = 2pr / (p + r) \tag{31}$$

The three measures are used to evaluate the performance of the copy-move image forgery detection method.

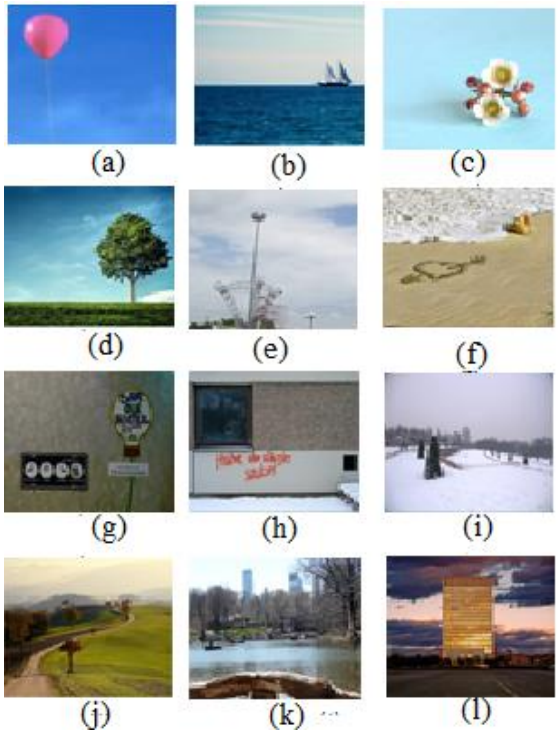


Figure 9: Images used in the experiments [2].

5 Simulations and evaluations

In the experiments, MATLAB program (version 2013a) is used with Window 7 Ultimate 64-bit, CPU Intel Core i5 @ 1.8GHz and 4GB RAM in order to run the simulations.

Using the images in Figure 9, we conducted different experiments by changing the order of Zernike moments, block size, the Curvelet transform's order, etc. Every test image will go through the proposed method and consequently Precision, Recall and F – measure will be evaluated.

Based on the fact that the investigating images are usually color images, there are two options for proposed method. First is to calculate Zernike moments from each color channel and subsequently link the moment values. The other option is to convert the RGB image into a gray-scale image. We choose the latter method because the same copy-move forgery is applied to each color channel similarly. Hence, by only calculating the Zernike moments on one dimension rather than for three dimensions of color image, the computation time of Zernike moments can be minimized.

A. Zernike moment's order

According to [35], a relatively small set of Zernike moments can characterize the global shape of a pattern effectively. The low order moments represent the global shape of a pattern and the higher orders represent the detail. However, the higher the order the more computational cost it takes which result in the increasing in running time. In Figure 10 below show the average running time of proposed method for images with

different Zernike moments' orders in which the higher order is, the more computational time takes and dramatically increases for Curvelets.

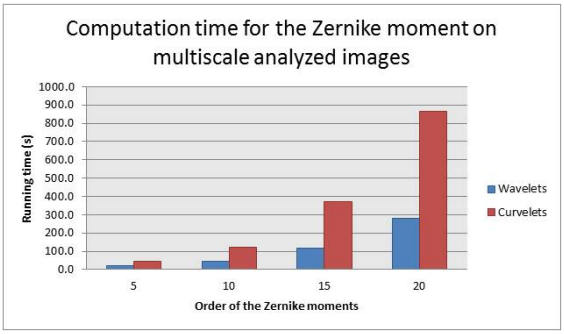


Figure 10: Computation time for the Zernike moment on multiscale analyzed images.

Figure 11: Detection results for forgery images of different Zernike moment's orders with Wavelets analysis.

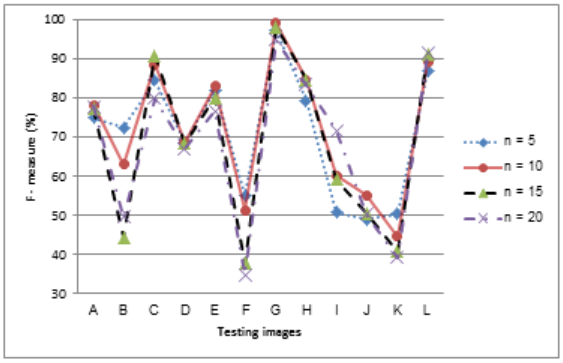


Figure 12: Detection results for forgery images of different Zernike moment's orders with Curvelets analysis.

In this research, the complex Zernike moments based on complex Zernike polynomials as the moment basis set are used in the processing. As we can see from Figure 10, the higher the order, the longer it takes to process. For the Wavelets transform method which only uses the approximation of images to compute the Zernike moments, the running time is much shorter comparing with the Curvelet transform method.

From the Figure 11 and Figure 12, the effect of different Zernike moment's orders on parameter F which shows the relationship between precision and recall was displayed. In this experiment, all images in the dataset will be tested with different Zernike moment's orders and different multiscale analysis. Even though theoretically the Zernike moment with higher order provides better precision compare to the lower ones which means that most part of detected region is correct, the recall which presents the percentage of forgery region detected will relatively reduce as a trade-off for the precision.

Therefore, according to Figure 10 and Figure 11, the F – measure of higher Zernike moment's order detection test is not always higher than the lower orders although it needs more computation time as in Figure 9 shown. Comparing the results of the order of 5, 10, 15 and 20, we can see that the F – measure of 5th order and 10th order is relatively higher than others. For both the Wavelet transform test and the Curvelet transform test, 10th order of Zernike moment is decided to be used as it yields higher F – measure compare to other orders which means the trade-off between the precision and recall of it is better than other order. Hence, for the next experiments, we will use Zernike moment of order 10 to analyze the performance of the Curvelet transform and the Wavelet transform in forgery detection in other different perspectives.

B. Block size

In this experiment, we tested the 13 images in dataset with different dividing block sizes from 8 pixels to 32 pixels in order to analyze the effect of the block size to the detectability and to choose a suitable block size for further experiments. After analyzed by a multiscale method, the testing image will be divided into square blocks with same size before calculating the Zernike moments.

The different in block size effect greatly on the detectability. Figure 12 and Figure 13 show the detection result of forgery images with block sizes of 8, 16, 24 and 32. As we can see from the figures, most of the detection results when dividing the images into block sizes of 24 and 32 pixels fail to detect the forgery regions. This shows that the algorithm is effective if the copied region is comprised by many smaller blocks. This also means if the block size is bigger than the copy-move region, the detectability will drop dramatically since the forgery part in one block is not large enough to provide adequate information for detection. The popular size of divided blocks is 8x8 or 16x16.

From the results shown in Figure 12 and Figure 13, for both the Wavelets analysis and the Curvelets analysis, the image with highest F – measure is G with 99.9% and 98.8% respectively with block size of 16x16. With block size of 24x24, for the Wavelets analysis, the image A, B, F, J and K have visually lower F–measure compare to the highest values, in which the F – values reached 0% in image B and K where the algorithm returns "real image" results. With block size of 32x32, except for the image G, H and I which are large original image with big copy-move region, the other image have 0% for precision and recall. For the Curvelet transform combining with Zernike moment algorithm, the processed images have a bigger size compare to the images analyzed by the

Wavelet transform. Therefore, with the block size of 24x24, only image B have visually lower F – measure (at 0%) compare to other block size and with block size of 32x32, only images B, E, F, J and K have extreme low F – parameters (10% for image F and 0% for the rest).

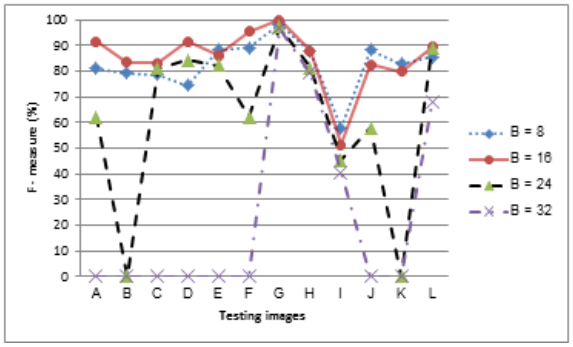


Figure 13: Detection results for forgery images of different block sizes with Wavelets analysis.

For Wavelets analysis, the images' size is reduced to a quarter of the original forgery images which make the copy-move region is shrink to a quarter of original copy-move region. Therefore, compare to the Curvelet analysis detection results, the detectability of bigger block size of Wavelet analysis is lower.

The block size of 16 pixels is chosen since we found this to be a good trade-off between detected image details and the feature robustness. This block size will be fixed across the different analysis, when possible, to allow for a fairer comparison of the feature performance. Note that the majority of the previous research also proposed a block size of 16 pixels.

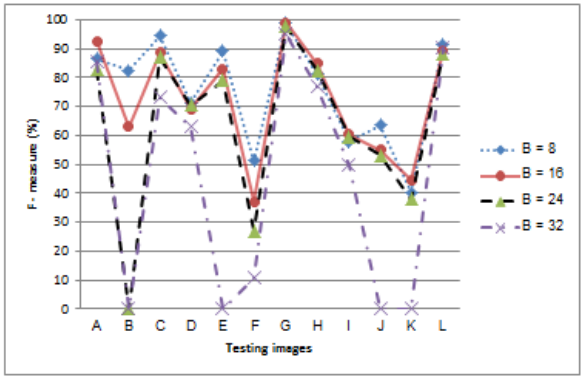


Figure 14: Detection results for forgery images of different block sizes with Curvelets analysis.

Scale of the Curvelet transform

For our experiments, the first-generation Curvelet transform was used to enhance the images. The applications of the first-generation Curvelets are image denoising, image contrast enhancement, etc. The default number of scales including the coarsest wavelet level is equal to $\log_2(N)$-3, in which N is the size of the NxN testing image. In this experiment we will observe the detection results by changing the number of scale from smallest to equal or less than the default value.

Different images will have different default values of scale if they have different sizes. A larger image can be analyzed by larger scale of the Curvelet transform. Therefore, for consistency in this experiment, all 12 images in the dataset will be tested with different number of scale according to the smallest size of the images in dataset which is 128 x 128. With N = 128, we have the number of scale varies from 2, 3 or 4. Hence, the 12 images will be applied Curvelets analysis with one of these scales before going through further steps in the

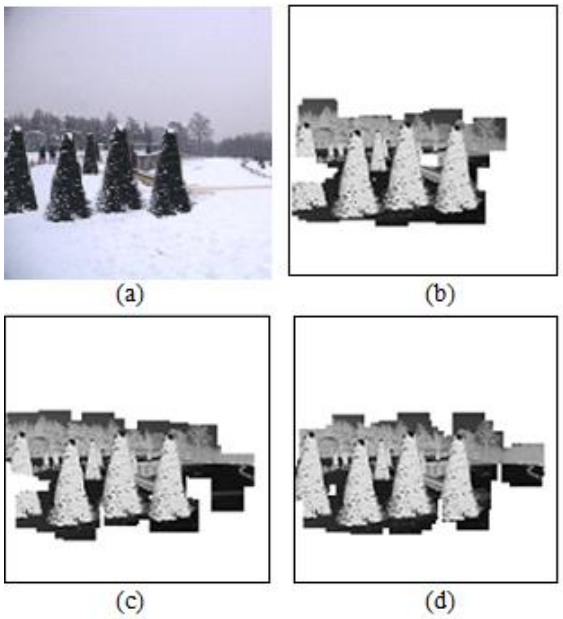


Figure 15: Negative detection results for a forgery image analyzed by the Curvelet transform with different number of scale; (a). Forged image, (b).b n =2,(c) n =3,(d) n =4 [2].

algorithm such as calculating the Zernike moments or computing Euclidean distances.

From the detection results of image J in Figure 15, we can see that with higher number of scale (n = 4) for Curvelet analysis, the percentage of detected forgery region is higher compare to the lower number of scale detection results.

The results of the experiments are shown in Figure 16. Although the experiments are conducted with different number of scales, the F – measure of the detection result is almost the same for most of the testing images except the image A, B, I, J and K. The results of the Curvelets analysis with scale of 2 are slightly higher compare to other scales as we can see from the images A, I, J and K. Although the scale of 4 of the Curvelet analysis algorithm has a higher detection result in image B, the scale of 2 has slightly higher average F – measure compare to other scales. The Curvelet transform with scale of 2 is chosen from the experiments we conducted in this section. Moreover, from [30], the authors also proved that the small scale is more robust. For the next section, we will perform a throughout comparison against the Wavelet transform with the results from the previous experiments.

Figure 16: Detection results for forgery images analyzed by the Curvelet transform with different number of scales.

C. Performance comparison between the Curvelet transform and the Wavelet transform combining with the Zernike moment based technique

In Figure 17, the F – measure of both Curvelets analysis and Wavelets analysis is shown. Except for image (C) and (I) where the F – measure of the Curvelet transform method is higher than the Wavelet transform method, the performance of the Curvelet transform is lower for most the testing images. Especially for image (F), the Curvelet transform method's F – measure is lower than 40% while the Wavelet transform method has approximately 95%. In order to analyze the different between two multiscale analyses, we will investigate some of the testing images that have great dissimilarity. The precision and recall of each testing images will also be analyze for further discussions.

For image B, D, F, J and K, they are not the simple images compared to others in the dataset, but they have detailed background which may be the cause for the drop in performance of the Curvelet transform method. Detail statistics about the precision and recall for the images can be analyzed from the Table 1 and 2.

For practical use, the most important aspect is the ability to distinguish tampered and original images. However, the power of an algorithm to correctly annotate the tampered region is also significant, especially when a human expert is visually inspecting a possible forgery. Thus, when evaluating the copy-move algorithm with different multiscale analyses, we analyze their

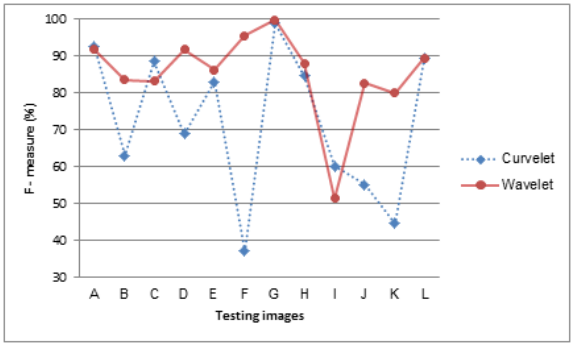


Figure 17: Performance comparison between the Wavelets analysis and the Curvelets analysis combining with the Zernike moment based technique.

Image	Measure (%)			Image	Measure (%)		
	P	R	F		P	R	F
(a)	87.6	96.4	91.8	(g)	99.8	100.0	99.9
(b)	100.0	78.0	87.6	(h)	78.6	100.0	88.0
(c)	74.4	94.3	83.2	(i)	34.7	99.6	51.5
(d)	90.8	92.8	91.8	(j)	93.8	74.1	82.8
(e)	84.2	88.5	86.3	(k)	78.1	81.9	80.0
(f)	91.5	100.0	95.6	(l)	81.1	100.0	89.6
				Average	82.9	92.1	85.7

Table 1: Detection rates for 12 images analyzed by the Wavelet transform combining with Zernike moment

Image	Measure (%)			Image	Measure (%)		
	P	R	F		P	R	F
(a)	89.4	96.0	92.6	(g)	98.1	100.0	99.0
(b)	7.03	57.1	63.0	(h)	73.5	100.0	84.7
(c)	79.8	99.4	88.5	(i)	44.3	94.0	60.2
(d)	76.7	62.7	69.0	(j)	42.5	78.3	55.1
(e)	78.5	88.1	83.0	(k)	30.7	82.2	44.7
(f)	26.5	62.2	37.2	(l)	80.8	100.0	89.4
				Average	65.9	85.0	72.2

Table 2: Detection rates for 12 images analyzed by the Curvelet transform combining with Zernike moment.

performance at pixel level, where we evaluate how accurately tampered regions can be identified through three parameters: Precision, Recall and F – measure.

The experiments conducted are all "plain copy-move" which means we evaluate the performance of each method under ideal conditions. We used the 12 original images and spliced 12 images without any additional modification. We chose per-method optimal thresholds for classifying these 24 images. Although the sizes of the images and the manipulation regions vary on this test set, both tested analyses solved this copy-move problem with a recall rate of above 85% (see Table 1 and 2). However, only the Wavelet transform method has a precision of more than 80%. This means that for the Curvelet transform algorithm, even under these ideal conditions, generate false alarms.

With Curvelet analysis, the algorithm has a difficult time to distinguish the background and detect them falsely as the forgery regions. Through the experiments, it proves that the proposed method which uses the forgery images analyzed by the Curvelet transform is not suitable for the block based method combining with Zernike moment to detect the copy-move forgery images.

Disscusion

Through these experiments, different perspectives of block based technique using a combination of the Zernike moment and multiscale analysis for digital image forgeries are studied. The Zernike moment's orders, block sizes, the number of scale for multiscale analysis and different kinds of multiscale analyses are considered.

For higher Zernike moment's order, the computational time will increase proportionally along with the increasing in orders. Although the complexity in computation increases, the detection results are not worth it. In another word, the F – measure parameter is not going up with higher orders but for higher orders; some

testing images proved that its detectability performance is worse than a lower order.

According the experiments' results and other block based techniques, the block size of 16x16 is more favorable than the others. From the detection results with different block sizes, we can see that the trade-off between precision and recall of 16x16 size is the most suitable for the block based method for detecting image forgeries. Although the block size of 8x8 can also provide a comparable F – measure, for such a small blocks, the information it holds may not enough to be distinctive to other blocks. Therefore, the block size of 16x16 is used for different experiments in this research.

From the test by changing the number of scale of the Curvelet transform, the detection results between different numbers of scale is quite similar to each other. Nevertheless, the scale of two some provides better detection results compare to other number of scale. As shown above, the trade-off between the precision and recall for the scale of two is slightly superior compare to other number of scales.

Although the Curvelets analysis has many superior characteristics compare to the Wavelets analysis, in this block based technique combining with Zernike moment for digital image forgery detection, the detectability of the Curvelets analysis method shown is worse than the Wavelets analysis method's for most of the cases. The performance of the Curvelets analysis has yet reached the expectation of a multiscale analysis which allowed an almost optimal sparse representation of objects with singularities along smooth curves. The detection results have shown that in this digital image forgery detection method, the characteristics of the Curvelet transform have not utilized. Moreover, the precision of the detection results is also lower than the Wavelets analysis which leads to the lower F – measure.

In this research, the proposed idea of using the Curvelets analysis combining with Zernike moments by my study is not suitable. This method not only failed to utilize the characteristics of the Curvelet transform, but also reduced the efficiency of detecting a tampered image. Comparing to the Wavelets analysis, the Curvelets analysis is not feasible for combining with Zernike moments in the block based techniques.

6 Simulations and evaluations

In previous method [1], the combination between the Zernike moments and the Wavelet transform for detecting digital image forgeries has successfully achieve the desired goal. The computational cost reduces significantly while the precision is still acceptable. However, the Wavelets transform has disadvantage when analyzing edges or curves details. Continuing that research paper, another multi-resolution, the Curvelet transform, is used to combine with the Zernike moment in the block based technique for detecting image forgeries in order to solve that problems and increase the precision of the proposed method in the research paper although the computational cost will increase as the compensation for the additional information of the images. The efficiency of the algorithm will be evaluated through three parameters: precision, recall and F – which is combination of precision and recall in one parameter. Other parameter such as Zernike moment's order and the block size are chosen after conducting the experiments to evaluate the effect of them on the performance. From real experiments, we get a conclusion:

The Wavelets transform gives a desired result with low computational time and high precision, its advantages is simplicity, easy to implement and require low computational resources. Most images preprocess by the Wavelets transform have expectation results, however, for some images where the details on edge and curve that neighbor to each other is blended in after the Wavelets preprocessing, therefore having a low precision.

The Curvelet transform provides lower results, contrary to the expectation. Although the edge and curve details are clearer, images preprocessed by the Curvelet transform have lower performance and much higher Zernike moments calculation time than the Wavelets transform combination. From the simulation results, the Curvelet transform is not suitable for the proposed method which used the combination of Zernike moment based and the Curvelet analysis in the block based technique for detecting image forgeries.

The combination of the multiscale analysis and Zernike moment based technique is still not tested with different transformation attack such as rotation and scaling. Although the Zernike moment is known for the rotation invariant, in this block based technique, we have yet conducted experiments for rotation attacks.

For future research, in the problem of identifying the copied areas of a digital image, we may explore the rotation invariant characteristic of the Zernike moments which can robust against rotation attacks. Moreover, by combining with SIFT or SURF, the running time of Zernike moments can be enhanced.

For the Curvelet transform, a new method is needed to utilize its features. There are some feasible algorithms such as keypoint-based algorithms or block based algorithms which do not use Zernike moments but intensity-based or frequency based.

7 Acknowledgement

This research is funded by Vietnam National University Ho Chi Minh City (VNU-HCM) under grant number B2015-20-02.

8 References

[1] Thuong Le – Tien, Marie Luong, Tu Huynh – Kha, Long Pham – Cong – Hoan, An Tran – Hong, "Block Based Technique for Detecting Copy-Move Digital Image Forgeries: Wavelet Transform and Zernike Moments", Proceedings of The Second International Conference on Electrical and Electronic Engineering, Telecommunication Engineering, and Mechatronics, Philippines 2016, ISBN 978-1-941968-30-7.

[2] Vincent Christlein, Christian Riess, Johannes Jordan, Corinna Riess and Elli Angelopoulou, "An Evaluation of Popular Copy-Move Forgery Detection Approaches", IEEE Transactions on Information Forensics and Security, 2012.

[3] Seung-Jin Ryu, Min-Jeong Lee, and Heung-Kyu Lee, "Detection of copy-rotate-move forgery using Zernike moments", Lecture Note in Department of Computer Science, Korea Advanced Institute of Science and Technology Volume 6387, pp 51-65, 2010, Daejeon, Republic of Koea.

[4] Tu Huynh–Kha, Thuong Le–Tien, Khoa Van Huynh, Sy Chi Nguyen, "A survey on image forgery detection techniques," The Proceeding of 11-th IEEE-RIVF International Conference on Computing and Communication Technologies," Can Tho, Vietnam, Jan 25-28 2015.

[5] G. Li, Q. Wu, D. Tu, and S. Sun, "A Sorted Neighborhood Approach for Detecting Duplicated Regions in Image Forgeries based on DWT and SVD," in Proceedings of IEEE International Conference on Multimedia and Expo, Beijing China, July 2-5, 2007, pp. 1750-1753.

[6] E.J. Cand`es and D.L. Donoho. Curvelets and curvilinear integrals. J. Approx. Theory., 113:59–90, 2000.

[7] J.-L. Starck, E. Cand`es, and D.L. Donoho. The curvelet transform for image denoising. IEEE Transactions on Image Processing, 11(6):131–141, 2002.

[8] Fridrich, D. Soukal, and J. Lukás, "Detection of copy move forgery in digital images," in Proc. Digital Forensic Research Workshop, Aug. 2003.

[9] P.Subathro, A.Baskar, D. Senthil Kumar, "Detecting digital image forgeries using re-sampling by automatic Region of Interest (ROI)," ICTACT Journal on image and video processing, Vol. 2, issue. 4, May 2012.

[10] E. S. Gopi, N. Lakshmanan, T. Gokul, S. Kumara Ganesh, and P. R. Shah, "Digital Image Forgery Detection using Artificial Neural Network and Auto Regressive Coefficients," Electrical and Computer Engineering, 2006, pp.194-197.

[11] Rafael C. Gonzalez, "Digital Image Processing", Prentice-Hall, Inc, 2002, ISBN 0-201-18075-8.

[12] D.L. Donoho and M.R. Duncan. Digital Curvelet Transform: Strategy, Implementation and Experiments; Technical Report, Stanford University 1999.

[13] E.J. Candès and D.L. Donoho. Curvelets – A Surprisingly Effective Non-adaptive Representation for Objects with Edges; Curve and Surface Fitting: Saint Malo 1999.

[14] Ma, Jianwei, and Gerlind Plonka. "The curvelet transform." IEEE Signal Processing Magazine 27.2 (2010): 118-133.

[15] Jiulong Zhang and Yinghui Wang, "A comparative study of wavelet and Curvelet transform for face recognition", 2010 3rd International Congress on Image and Signal Processing (Vol 4), IEEE, Oct. 2010

[16] Thuong Le - Tien, "Chapter 10: Morphological image processing", Lecture notes, for image/video processing and application, HCMUT, November, 2015.

[17] Dey, Nilanjan, Anamitra Bardhan Roy, and Sayantan Dey. "A novel approach of color image hiding using RGB color planes and DWT." arXiv preprint arXiv:1208.0803 (2012).

[18] Bhattacharya, Tanmay, Nilanjan Dey, and S. R. Chaudhuri. "A novel session based dual steganographic technique using DWT and spread spectrum." arXiv preprint arXiv:1209.0054 (2012).

[19] Dey, Nilanjan, et al. "DWT-DCT-SVD based intravascular ultrasound video watermarking." Information and Communication Technologies (WICT), 2012 World Congress on. IEEE, 2012.

[20] Dey, Nilanjan, et al. "DWT-DCT-SVD based blind watermarking technique of gray image in electrooculogram signal.", IEEE 12th International Conference on Intelligent Systems Design and Applications (ISDA), 2012.

[21] Dey, Nilanjan, Moumita Pal, and Achintya Das. "A Session Based Blind Watermarking Technique within the NROI of Retinal Fundus Images for Authentication Using DWT, Spread Spectrum and Harris Corner Detection." arXiv preprint arXiv:1209.0053 (2012).

[22] Bhattacharya, Tanmay, Nilanjan Dey, and S. R. Chaudhuri. "A novel session based dual steganographic technique using DWT and spread spectrum." arXiv preprint arXiv:1209.0054 (2012).

[23] Dey, Nilanjan, et al. "Lifting wavelet transformation based blind watermarking technique of photoplethysmographic signals in wireless telecardiology." IEEE World Congress on Information and Communication Technologies (WICT), , 2012.

[24] Dey, Nilanjan, et al. "Stationary wavelet transformation based self-recovery of blind-watermark from electrocardiogram signal in wireless telecardiology.", International Conference on Security in Computer Networks and Distributed Systems. Springer Berlin Heidelberg, 2012.

[25] Dey, Nilanjan, et al. "Wavelet based watermarked normal and abnormal heart sound identification using spectrogram analysis.", IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), 2012.

[26] Mukhopadhyay, Sayantan, et al. "Wavelet based QRS complex detection of ECG signal." arXiv preprint arXiv:1209.1563 (2012).

[27] Hemalatha, S., and S. Margret Anouncia. "A Computational Model for Texture Analysis in Images with Fractional Differential Filter for Texture Detection." International Journal of Ambient Computing and Intelligence (IJACI), Vol.7, Issue 2, 2016.

[28] Sharma, Komal, and Jitendra Virmani. "A Decision Support System for Classification of Normal and Medical Renal Disease Using Ultrasound Images: A Decision Support System for Medical Renal

Diseases.", International Journal of Ambient Computing and Intelligence (IJACI) 8.2 (2017): 52-69.

[29] Boulmaiz, Amira, et al. "Design and Implementation of a Robust Acoustic Recognition System for Waterbird Species using TMS320C6713 DSK.", International Journal of Ambient Computing and Intelligence (IJACI) 8.1 (2017): 98-118.

[30] Murray, Niall, et al. "Future Multimedia System: SIP or the Advanced Multimedia System.", International Journal of Ambient Computing and Intelligence (IJACI), 3.1(2011).

[31] Fouad, Khaled Mohammed, Basma Mohammed Hassan, and Mahmoud F. Hassan. "User Authentication based on Dynamic Keystroke Recognition." International Journal of Ambient Computing and Intelligence (IJACI) 7.2 (2016): 1-32.

[32] D.L. Donoho and M.R. Duncan. Digital curvelet transform: strategy, implementation and experiments. In H.H. Szu, M. Vetterli, W. Campbell, and J.R. Buss, editors, Proc. Aerosense 2000, Wavelet Applications VII, volume 4056, pages 12–29. SPIE, 2000.

[33] E.J. Candès and D.L. Donoho. Curvelets – A Surprisingly Effective Non-adaptive Representation for Objects with Edges; Curve and Surface Fitting: Saint Malo 1999.

[34] Ma, Jianwei, and Gerlind Plonka. "The curvelet transform." IEEE Signal Processing Magazine 27.2 (2010): 118-133.

[35] Sundus Y. Hasan, "Study of Zernike moments using analytical Zernike polynomials", Pelagia Research Library, Iraq, 2012.