Thesis for the Degree of Master of Engineering

Improved Feature Extraction Using Gabor Filter for Copy-Move Forgery Detection

by

Sheilha NININAHAZWE

Department of IT Convergence and Application Engineering

The Graduate School

Pukyong National University

February, 2015

Improved Feature Extraction Using Gabor Filter for Copy-Move Forgery Detection

복사-이동 위조 검출을 위한 가보 필터를 이용한 개선된 특징 추출

Advisor: Prof. Kyung-Hyune Rhee

by

Sheilha NININAHAZWE

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Engineering

in the Department of IT Convergence and Application Engineering,
The Graduate School, Pukyong National University

February, 2015

Improved Feature Extraction Using Gabor Filter for Copy-Move Forgery Detection

A thesis

by

Sheilha NININAHAZWE

Approved by:

(Chairman) ***Dr. Man- Gon Park***

(Member) ***Dr. Kim Chang Soo***

(Member) ***Dr. Kyung-Hyune Rhee***

February, 2015

Contents

Contents

List of Tables

List of Figures

복사-이동 위조 검출을 위한 가보 필터를 이용한 개선된 특징 추출

Sheilha NININAHAZWE (쉬라 니니나하즈에)

부경대학교 일반대학원 IT융합응용공학과

요 약

오늘날, 디지털 이미지와 비디오에 대한 정보보호는 안전하고 신뢰성 있는 멀티미디어 산업 확산을 위한 주요 핵심기술로써 간주되고 있다. 그러나 현재 사용되고 있는 많은 멀티미디어 편집 소프트웨어의 발달로 인하여, 디지털 이미지의 위변조에 대한 입증은 다양한 문제를 포괄하는 어려운 과제가 되고 있다. 특히, 디지털 이미지는 여러가지 기술을 이용하여 위조될 수 있는데, 이 중 가장 대표적인 이미지 위조 기술은 이미지의 한 영역을 복사하고 동일한 이미지의 다른 곳으로 붙이는 복사-이동 위조 기법으로써 이러한 위조를 검출하기 위한 여러 가지 기법이 제안되었다.

본 논문에서는 Gabor 필터 기반 복사-이동 위조 탐지 기법을 제안한다. 제안 기법에서는 아핀 변환, 명도 변환 등과 같은 여러 이미지 연산에 강건한 위조 탐지를 위하여 MSA(Multiscale Average)를 이용한 후 Gabor 필터를 사용하여 이미지 특징점을 추출하였다. 이후 Gabor 필터에 의해 계산된 특징점 벡터 비교를 통한 유사성 검증을 수행하여 복사-이동 위조 탐지의 정밀도를 향상시켰다.

Chapter 1

Introduction

1.1 Background

In this modern and developed word, the authentication of an image is very important because of the availability and easy tools from many types of software on different devices. Forensic investigation, is an area with a very important role, with the aim of proving that the presenting document is original or have been undergone some transformations in order to change completely its meaning with the one it was supposed to be. Notice also that forensic works in many areas such as insurance processing, surveillance systems, intelligent services, medical imaging, journalism, image processing, multimedia and so on [1,5].

Generally, we can say that the most frequent type of forgeries that we found is turning on: hiding a region in the image, deleting (or adding) an object in image, misrepresenting the image information. Regarding those types, we can categorized three most frequent forgeries [5, 6]: Copy-move (copy-paste) forgery, splicing and retouching.

Although we know the type of forgery we might face, it is not easy to detect the forgery when you have an image without any additional informations of it. For that purpose, many researches have been done and have found that there are some basic approaches that we can use to detect the forgery. Among those approaches, we can just enumerate some of them such: The information about the device that has been processed the image, the direction of light, some traces left intentionally or not on the image during the manipulation of the image, compression and so on.

It is more clear if we already have those informations; it will be quite easy to procede the detection by choosing an algorithm with the best characteristics to detect the forgery. Also as we know forensics is a huge area for forgery, many algorithms have been proposed with their characteristics and their performances [7-9].

1.2 Purpose and Structure of the Thesis

In this thesis, we proposed new forgery detection based on Gabor. Regarding different works that have been done in forgery detection, we propose a new approach which analyses the texture first and enhance the properties of image by making this texture more clear and robust against some transformation like affine transform, noise, illumination change. This will improve the quality of the image that we want to analyze. The MSA (Multiscale Average) is the first algorithm that we will apply on image to reach that result. After that step, Gabor filter will be used to extract the important features that are needed for our ongoing work. Notice that by using this Gabor it is to make our texture features more robust against some post posting operation like scale and rotation. Thus means that if the attacker has committed some operation like scaling and rotation on our image, features vectors that we will extract will be still recognize the similar features. Then a similarity measure will be applied to compare the same features and give the decision whether the present image is forged or original.

The structure of this thesis is broken down into the following modules: Chapter 1, briefly introduces the image forgery detection in it whole domain. Chapter 2 examines the needs and the challenges that we find in forgery detection. In Chapter 3, we discuss different algorithms that have been proposed by researches and we give another approach of how we can improve the detection. The analysis of our methods and its best performances comparing to the previous works is presented in Chapter 4. Finally, in Chapter 5, we conclude the thesis.

Chapter 2

Basic of Image Forgery Detection

2.1 The Need for Detection of Digital Image Forgeries

A picture may have more importance than words but, alongside, it has a lot of interpretations [10]. Images and videos can be easily manipulated with variety of common editing tools. Some of those altered image are not detectable as forged with the human eye and consequently can be attributed as original images. It is easy to expect that a forged image will cause troubling consequences. Forged image could be used to mislead the public opinion or for distorting the truth in news reports. They can also be used to destroy someone's reputation and privacy by modifying the picture or video to give another meaning completely different with the one it was supposed to have(example: cheating people) or in politic, the picture can lead to war between enemies. Understand that owing such sophisticated digital multimedia editing software tools and argue that an image is at no revocable response to be authentic is a challenging task. As result, the authenticities of images, cannot be taken for granted anymore, which bring the use of multimedia data as evidence in the court of law to be not accepted.

These issues of multimedia security have led the creation a field of a digital image forensics which analyses images to establish credibility and authenticity through a variety of means. This field is fast becoming popular because of its huge exploitations in many domains, such medical imaging, news reporting, sport and insurance, face detection, pattern recognition and so on [2, 3].

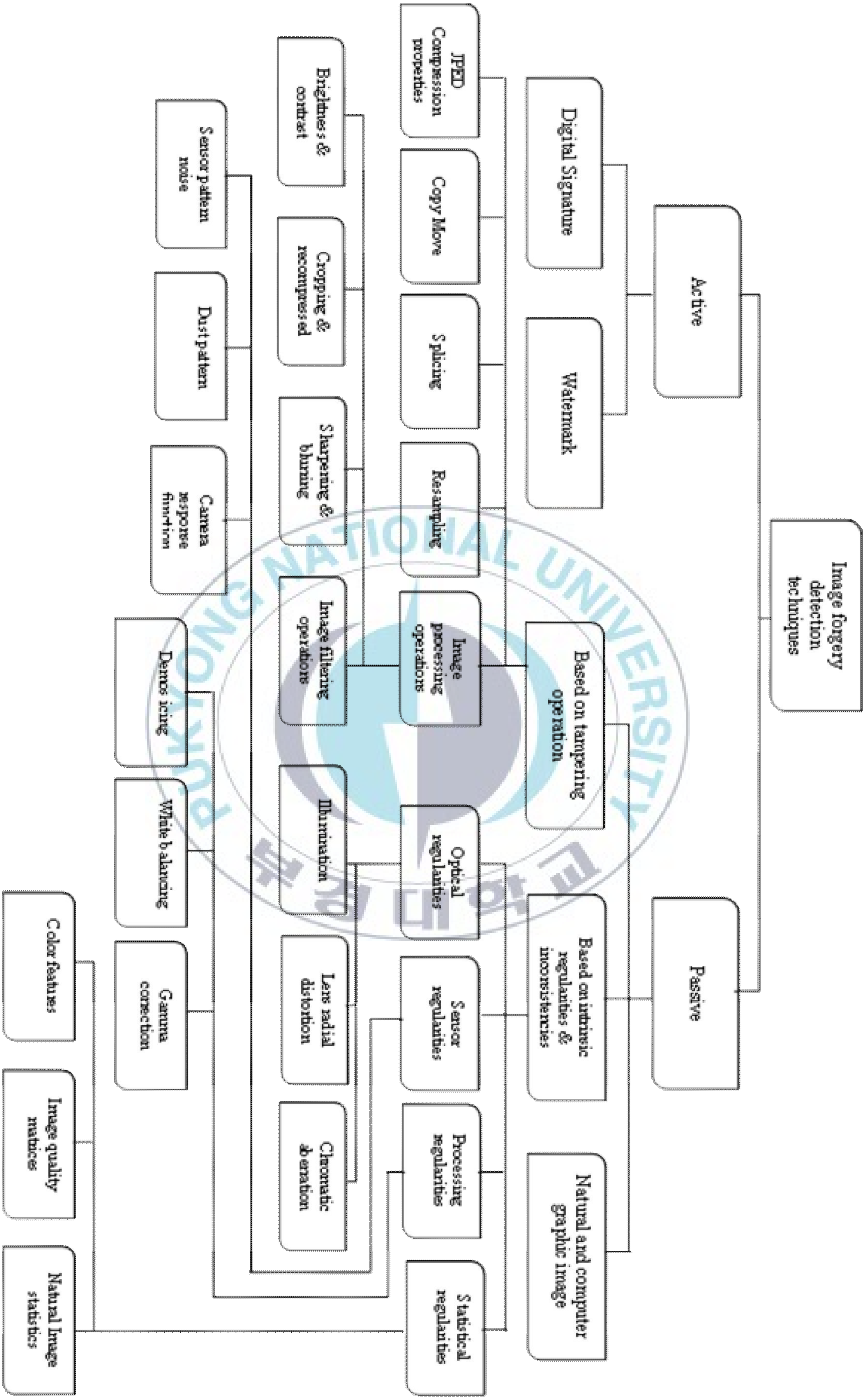


Figure 1: Forgery Detection Classification

2.2 Challenge to Detect Image Forgery

Now that we know the need of the authenticity of an image, it will be good to understand the issues of multimedia security have led to the development of several approaches to forgery detection [11, 12]. There are two types of techniques that can be used for image forgery detection. The active authentication methods and the passive authentication methods (see Figure 1).

The active authentication is divided in two categories:

- *The digital watermarking:* This type of methods conceals a watermark into an image at the capturing end and extracts it at the authentication end to proof if the image is original. Get to know that the watermark is inserted either at the time of capturing the image using a camera or later by an authorized person.
- *The digital signature*: In this category of methods features are extracted as a signature at the image capturing end. For the authentication end, the signature is regenerated using the same way, and the verification of the originality of the image can be done by comparison.

Passive image authentication, which is also called a blind method, is the process of authenticating digital images without any information about image. They are also divided in three categories (tampering, intrinsic regularities and inconsistencies and natural and computer graphic image) but we have been focused on two of them which are more important:

- *Intrinsic regularities and inconsistencies:* Here the authentication is based on detecting traces that are left by the image acquisition steps and the storage phases. For example, the camera fingerprint is used to distinguish between different camera models or different exemplars of the same camera model.
- *Tamper detection:* In this technique we distinguish two categories of forgery. The first category is the independent detection techniques which are attributed for forgeries detection regardless his type. It exploits three different types of artifact [13]: Traces of resampling, compression and inconsistencies.

The second is the dependent detection techniques which are assigned for forgeries like: Splicing, copy-move and retouching.

- Image splicing is a common process that is used in image forgery. To achieve such forgery, it is simply combining two or more regions from different images to make one image. This process can cause inconsistences in many features (by detecting this forgery you will find irregularities in texture such as an abnormally sharp transient at splicing region).
- The copy –move (or copy-paste) is also one frequent forgery that we will find in forensics [4]. This forgery is making by cutting different regions and pasting (or cloning) them in the same image. Notice that this forgery is mostly done by multiplying objects or simply concealing an object (or region) undesirable inside the image. Understand that the clue for detecting this forgery is to find regions that share inherent characteristics (example: pattern noise).the analysis of the suspected regions might reveal a high level of similarity between them [14-16].

2.2.1 Attacks of Digital Image Forgery

By making forgery, [4] some operations are made by the attacker either intentionally or not. Those operations are divided in two groups (Figure 2):

- The intermediate operations which are used to give a spatial synchronization and homogeneous regions between forged regions and its neighbor. This can be done by modifying illumination or chrominance, rotation or scaling.
- The post- processing operations are mostly seen in copy-move detection where they constitute a clue of detecting the traces left by the attacker trying to conceal his forgery. This is such blurring, additive noise, JPEG Compression….

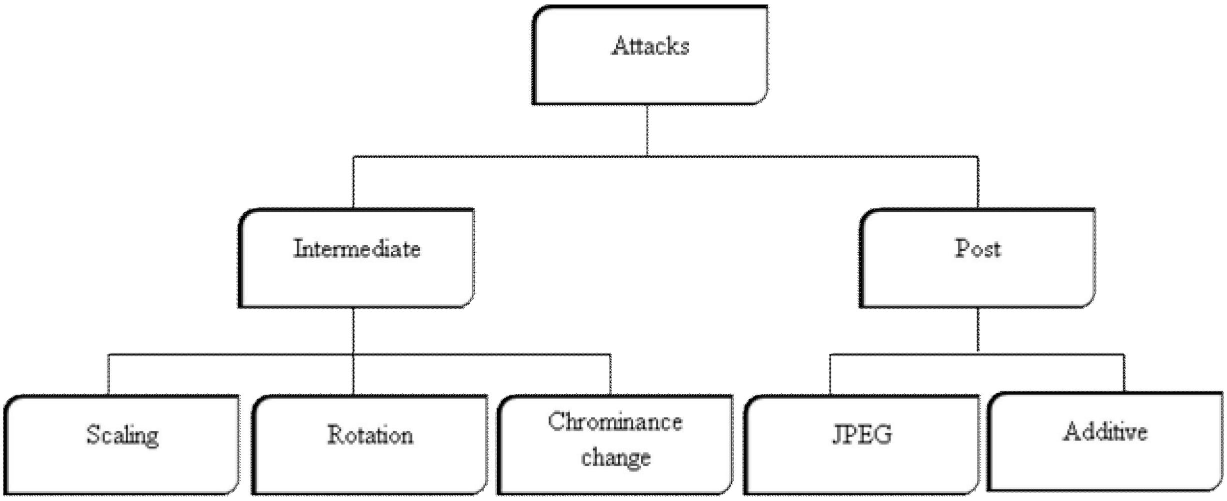


Figure 2: Image Processing Operations.

2.2.2 Digital Image Forgery Detection Methods

We have already seen that the image forensics detection is classified in two types of authentications which are the active and passive methods [5]. The blind image forensic detection, which doesn't need any prior information about the source image, can be cluster in six groups or categories (Figure 3): pixel-based, format-based, camera based, source camera identification-based, physics-based and geometric-based.

- *Pixel-Based Techniques:* These techniques are common found in practice and, are based on pixel where we detect anomalies during the forgery process. It analyses the correlations that appear from a specific form of forgery in spatial domain or in some transform domain.
- *Format - based techniques:* In here the process is to convert a forged image in format you desire to make the compression or other applications a very difficult task during the detection (i.e., JPEG compression).
- *Camera-based techniques:* Camera-based techniques detect the traces left by different steps of image process. This is done by exploiting artifacts during the tampering detection such chromatic aberration, color filter array, camera response, sensor noise…

- *Source Camera Identification-Based Techniques:* In these techniques, the characteristic of the source camera is used to identify the forgery. The method is based usually on analysis of lens aberrations, color filter array interpolations, sensor noise….
- *Physics-Based Techniques:* This section, the source and the position of the light is important especially during the detection. It is difficult to match the light inconsistency from different images. Thus can be a clue for image splicing detection by detecting the light variations in image.
- *Geometric-Based Techniques:* In geometric-based techniques, the important thing is to look for the principal point which is the projection of the camera center onto the image plane. It is near the center of the image. During the forgery, it is difficult to keep the image principal point in its correct perspective.

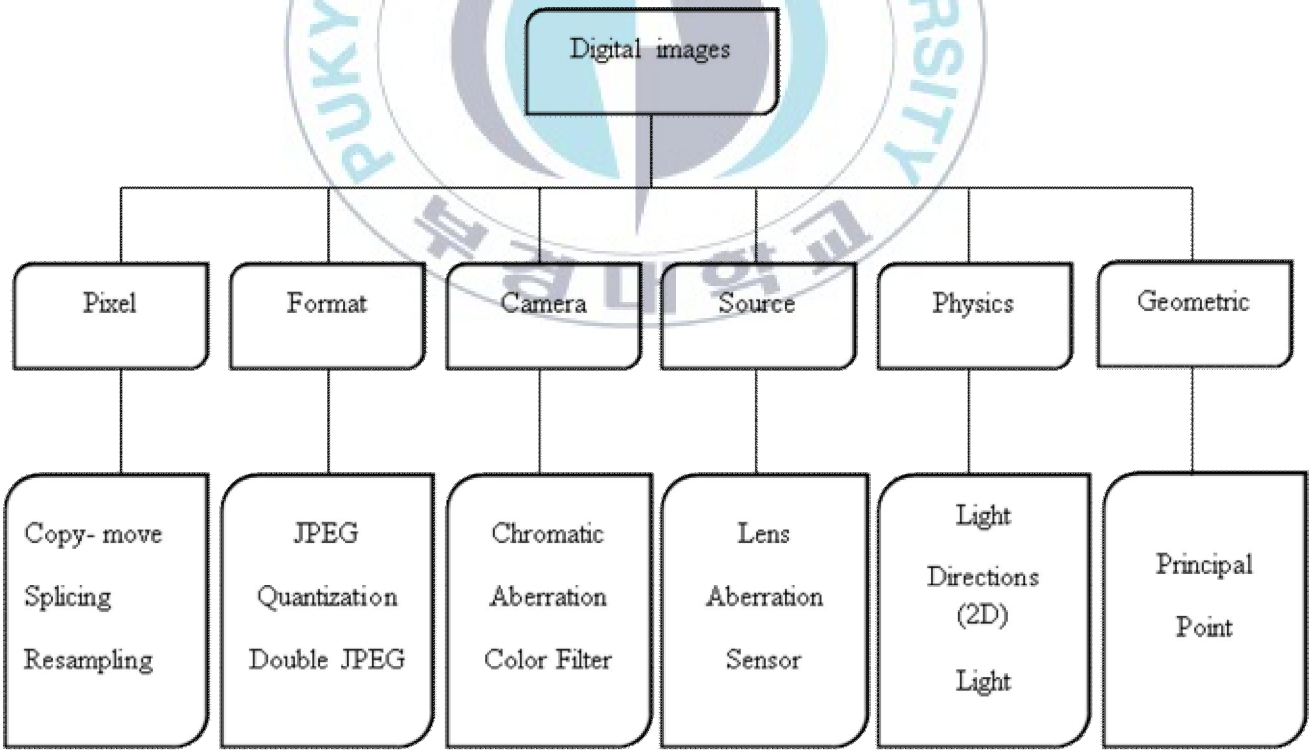


Figure 3: Blind Image Forensics Detection Methods

Chapter 3

Improved Feature Extraction Using Gabor Filter for Copy-Move Forgery Detection

3.1 Gabor Filter

In this section let first start by giving a brief review of Gabor features and Gabor space for a better understanding [22].

3.1.1 Gabor Features

The general functional form of a 2-D Gabor filter function in the continuous spatial domain can be specified as:

$$\begin{cases} \psi\left(x,y;f,\theta\right)=\dfrac{f^2}{\pi\gamma\eta}e^{-\left(\frac{f^2}{\gamma^2}x'^2+\frac{f^2}{\eta^2}y'^2\right)}e^{j2\pi fx'}, \\ x'=x\cos\theta+y\sin\theta, \\ y'=-x\sin\theta+y\cos\theta, \end{cases} \qquad (3.1)$$

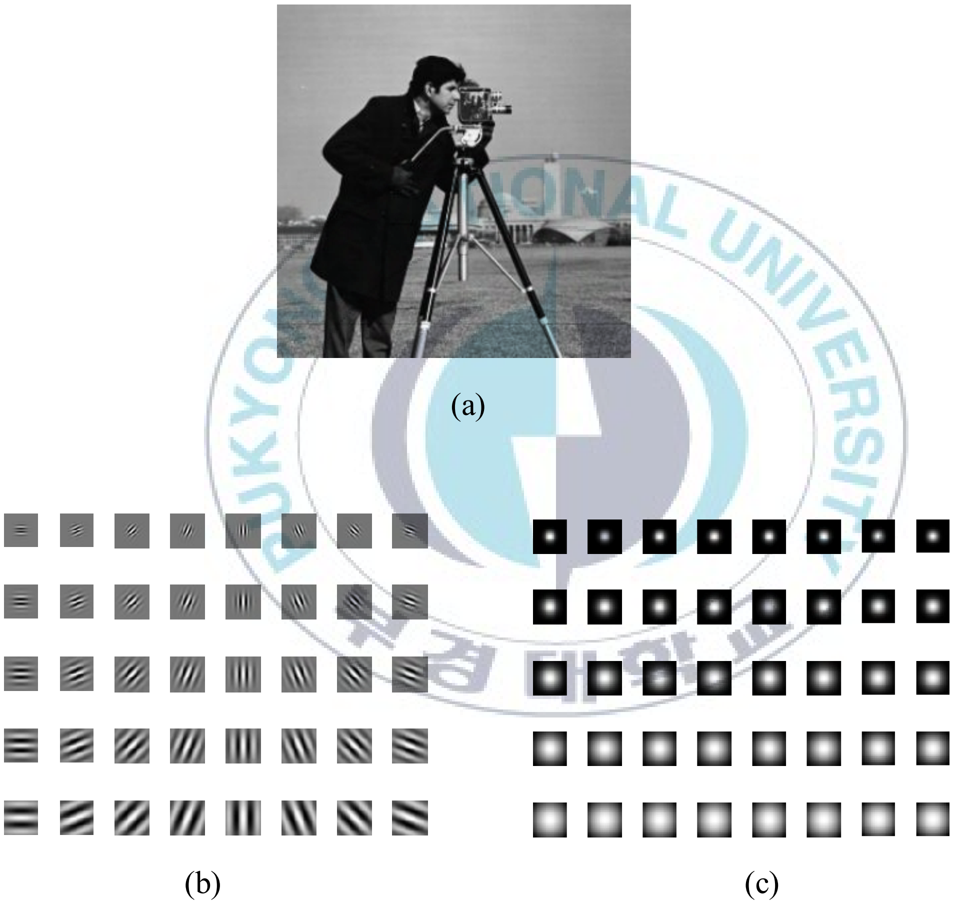
where f is the frequency of a sinusoidal plane wave, θ is the anti-clockwise rotation of the Gaussian envelope and sinusoid, γ is the spatial width of the filter along the plane wave, η and the spatial width perpendicular to the wave, the spatial coordinates $\left(x,y\right)$ of the image.

The filter described in Equation (3.1) is applied to an image function $\xi\left(x,y\right)$ such as shown in Figure 4. will get the filter out results for different parameters such as different rotation angles and/or frequencies. This filtering convolution operation can be stated as

$$\gamma_\xi\left(x,y;f,\theta\right)=\psi\left(x,y;f,\theta\right)*\xi\left(x,y\right), \qquad (3.2)$$

where $\xi(x,y)$ is the input image, (x,y) the translation, θ the rotation and f the scale. The response of the Gabor filter in Equation (3.2) is the low-level Gabor feature.

When the Gabor filter is applied to the object image shown in Figure 4(a), the Gabor images of frequency and magnitude as shown in Figure 4(b-c). Thus image analysis by the Gabor functions is much more edge information from the original image and similar to perception in the human visual system.


(a)

(b)

(c)

Figure 4: Gabor Feature Extraction. (a) object image, (b) the real part of the resulting image, and(c) the magnitude.

3.1.2. Gabor Space

According to the definition of Equation (3.2), assume the image is rotated by ϕ, scaled by a and amplified by c , then

$$c\gamma_{\xi}\left(ax, ay; \frac{f}{a}, \theta-\phi\right)=r\left(x, y; f, \theta\right), \tag{3.3}$$

The $r=\left(x, y; f, \theta\right)$ in Equation (3.3) is called a Gabor feature at coordinate $\left(x, y\right)$. Assume the index m denotes different interesting frequency and then covering the frequencies of interest from f_0 to f_{m-1} and the orientations from to θ_0 to θ_{n-1}.

In the selection of discrete rotation angles θ_k, the orientations must be spaced uniformly, that is,

$$\theta_k=\frac{k2\pi}{n}, \quad k=\{0,\ldots,n-1\}, \tag{3.4}$$

where θ_k is the k th orientation and n is the number of orientations that are going to be used.

In the selection of discrete frequency f_k, exponential sampling must be used, that is,

$$f_k=a^{-k}f_{\max}, \ k=\{0,\ldots,m-1\}, \tag{3.5}$$

where f_k is the k th frequency, $f_0=f_{\max}$ is the highest frequency desired, and a is the frequency scaling factor ($a>1$) and $a=\sqrt{2}$ for half octave spacing.

Then it can construct a matrix G focus on an image location $\left(x_0, y_0\right)$ by using Equation (3.2) and parameters from Equation (3.4) and Equation (3.5) as follows:

$$G=\begin{pmatrix} r\left(x_0, y_0; f_0, \theta_0\right) & \cdots & r\left(x_0, y_0; f_0, \theta_{n-1}\right) \\ \vdots & \ddots & \vdots \\ r\left(x_0, y_0; f_{n-1}, \theta_0\right) & \cdots & r\left(x_0, y_0; f_{m-1}, \theta_{n-1}\right) \end{pmatrix}, \tag{3.6}$$

3.2. MultiScale Autoconvolution

In forgery detection or other areas, we have to consider the methods which are invariant to affine transform under different geometric transformation. Some of them have been publish like Fourier Mellin transform [18], Sift, MSA [19]….However, if we have to consider the time complexity and the recognition accuracy they are not good as MSA.

Let start by defining the spatial affine transformation and affine invariance [20].

Definition 1. Define the affine transformation $A = A\{T, t\}$ by

$$x' = A(x) = Tx + t \ , \qquad (3.7)$$

where $t, x \in \ {}^2$and T is a 2 ×2 nonsingular matrix whose elements belong to and is a translation vector. Any such transformation is invertible with inverse $A^{-1}(x) = T^{-1}x - T^{-1}t$.

Definition 2. Suppose $f(x): \ {}^2 \rightarrow \ , f \geq 0$ is an image intensity function corresponding to a gray-scale image in ^{2}.We may apply an affine transformation A to this image, which gives a new gray-scale image in ^{2} with image function f'.

$$f'(x) = f \circ A^{-1}(x) = f\left(T^{-1}x - T^{-1}t\right), \qquad (3.8)$$

where f' the A transformed version of f.

Definition 3. A feature I, extracted from the function f, is said to be affine invariant if it produces the same value for f and then A transformed version of f for any affine transformation A.

Let $f(x): \ {}^2 \rightarrow$ with $f \geq 0$ be an image intensity function in $L^1\left(\ {}^2\right) \cap L^2\left(\ {}^2\right)$ and let $p(x) = \dfrac{1}{\|f\|_{L^1}} f(x)$ be the normalized version of f, so that $f_{\ 2}\, p(x)dx = 1$.

Then, $p(x)$ is a probability density function and we may take X_0, X_1 and X_2 to be independent random variables with values in ^{2} so that $px_j(x_j) = p(x_j)$.(we write px for the probability density function of a random variable X).Consider three samples (x_0, x_1, x_2) of these random variables as a basis for the following transformation :

$$u = \alpha(x_1 - x_0) + \beta(x_2 - x_0) + x_0, \qquad (3.9)$$

where (α, β) are the coordinates for u in the space spanned by the vectors $X_1 - X_0$ and $X_2 - X_0$ and with the origin at X_0. Now let $A\{T, t\}$; to be an affine transformation as in Definition 1. If one takes the A transformed versions of the sample points X_0, X_1 and X_2, that is X'_0

$$x_0' = Tx_0 + t \ , \ x_1' = Tx_1 + t, \ x_2' = Tx_2 + t,$$

and defines another transformation by

$$u' = \alpha(x_1' - x_0') + \beta(x_2' - x_0') + x_0', \qquad (3.10)$$

It can be rewritten as

$$\begin{aligned} u' &= \alpha(Tx_1 - Tx_0) + \beta(Tx_2 - Tx_0) + Tx_0 + t \\ &= Tu + t. \qquad (3.11) \end{aligned}$$

One can also see that the points u and u' are connected by A if they have the same coordinate values (α, β) in the corresponding spaces.

Now, recall that the points x$_0$, x$_1$, and x$_2$ were samples of the random variables $X_0, X_1,$ and X_2 and define a new random variable

$$U_{\alpha,\beta} = X_0 + \alpha(X_1 - X_0) + \beta(X_2 - X_0), \qquad (3.12)$$

which has U as the corresponding sample. Similarly, we can define

$$U'_{\alpha,\beta} = X'_0 + \alpha(X'_1 - X'_0) + \beta(X'_2 - X'_0), \qquad (3.13)$$

where $X'_0 = TX_0 + t$, $X'_1 = TX_1 + t$, and $X'_2 = TX_2 + t$ hence, $U'_{\alpha,\beta} = TU_{\alpha,\beta} + t$.

Substituting $X = U'_{\alpha,\beta}$, we get

$$f'\left(U'_{\alpha,\beta}\right) = f\left(T^{-1}U'_{\alpha,\beta} - T^{-1}t\right),$$

$$= f\left(T^{-1}\left(TU_{\alpha,\beta} + t\right) - T^{-1}t\right) = f\left(U_{\alpha,\beta}\right), \tag{3.14}$$

where $f\left(U_{\alpha,\beta}\right)$ and $f'\left(U'_{\alpha,\beta}\right)$ are equal as random variables. This gives a method of obtaining affine invariant features of an image function f: The expected value of $f\left(U_{\alpha,\beta}\right)$, or any of its moments, or the expected value of $g\left(f\left(U_{\alpha,\beta}\right)\right)$ for a measurable function g, do not change in an affine transformation of f. Thus, we introduce the following affine invariant features and single out one of them as the MSA transform of f.

3.2.1 Definition of MSA

Let f be a function in $L^1(\ ^2) \cap L^2(\ ^2)$ with $f \geq 0$ and let $p(x) = \frac{1}{\|f\|_{L^1}} f(x)$ be the corresponding probability density function. Take $X_0, X_1,$ and X_2 to be independent random variables with values in $\ ^2$ so that $pX_j\left(x_j\right) = p\left(x_j\right)$. For $\alpha, \beta \in$, define a new random variable

$$U_{\alpha,\beta} = X_0 + \alpha\left(X_1 - X_0\right) + \beta\left(X_2 - X_0\right),\ F\left(\frac{1}{2}, \frac{1}{2}\right) = 1. \tag{3.15}$$

The K^{th} moment of $f\left(U_{\alpha,\beta}\right)$ is defined as $F^K(\alpha,\beta) = E\left[f\left(U_{\alpha,\beta}\right)^k\right]$ and the MSA transform of f is defined as the first moment, $F(\alpha,\beta) = E\left[f\left(U_{\alpha,\beta}\right)\right]$.

3.2.2 Advantages of MSA

Here, we shall present some important advantages of the MSA transform. The value of the MSA transform $F(\alpha,\beta)$ and the moment $F^K(\alpha,\beta)$ are invariant against any affine transformation $A(x) = Tx + t$, where $t \in {}^{2}$ and T is a 2×2 nonsingular matrix whose elements belong to .

Multiscale Autoconvolution can be generalized to cover a group of transforms that are invariant against other linear transformations of the image coordinates.

3.3 Proposed Method

In this section we are proposing a new approach based texture analysis using MSA and Gabor features to detect the forgery inside an image. This proposed approach is designed to be more robust and efficient. To reach such result we first start by improving the properties of the feature textures which at the end of extraction will give the best feature vectors are needed for a better decision during the forgery detection.

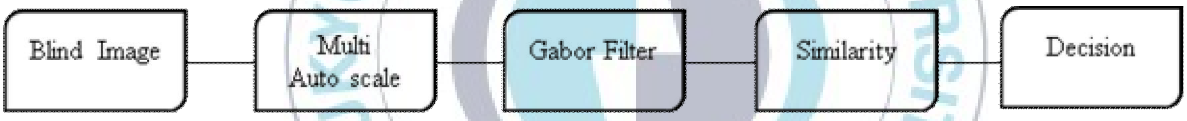


Figure 5: Proposed Algorithm

Here we explain step by step our proposed algorithm following the Figure 5:

- **Input image**: Let’s consider a blind image $I(x, y)$ that we divide in $M \times N$ size.
- **Multi autoscale:** we take the image and convert it in grayscale by apply the MSA.

$$I^{'}(x) = I \circ A^{-1}(x), \tag{3.16}$$

where $I'(x)$ is the image transformed in gray scale, $I(x)$ the original image and $A^{-}(x)$the invers of the affine transform A (see Equations (3.7) and (3.8)).This will give a new gray-scale image in with image function. At the same time, we apply a function $F(\alpha, \beta)$which produces a convolution of $I(x,y)$ with a variable scale $U_{\alpha,\beta} \in$ $_{,} f$ the characteristic function of a set in ^{2} and $E\left[f\left(U_{\alpha,\beta}\right)\right]$ the MSA transform of f as the first moment.

$$F(\alpha,\beta) = E\left[f\left(U_{\alpha,\beta}\right)\right], \tag{3.17}$$

Different scales levels will be sorted as shown in Figure 6.

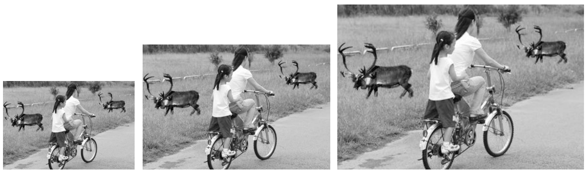


Figure 6: Extraction of Scale Levels by MSA.

This technique is used multiple times, it creates a stack of successively smaller images, with each pixel containing a local average that corresponds to a pixel neighborhood on a lower level of the pyramid.

- **Gabor filter:** Based on the three previous scales we will compute Gabor on each level scale to extract texture features. We will work by just shifting one pixel right of the previous one. So we have $(M'-M+1)\times(N'-N+1)$ blocks.

where M' and N' are respectively the column and row working on and $M+1$ and $N+1$ are the shifted column and row. Here we will describe one row for Gabor feature matrix.

$$c\gamma_{\xi}\left(ax, ay; \frac{f}{a}, \theta-\phi\right) = r(x, y; f, \theta), \tag{3.18}$$

The $r(x,y,f,\theta)$ Gabor features at coordinates (x,y). The index m will denote different frequency from f_0 to f_{m-1} and orientation from θ_0 to θ_{n-1}. Then we have a matrix G (Gabor feature matrix) on an image location (x_0, y_0).

$$G = \begin{pmatrix} r(x_0, y_0; f_0, \theta_0) & \cdots & r(x_0, y_0; f_0, \theta_{n-1}) \\ \vdots & \ddots & \vdots \\ r(x_0, y_0; f_{n-1}, \theta_0) & \cdots & r(x_0, y_0; f_{m-1}, \theta_{n-1}) \end{pmatrix}, \tag{3. 19}$$

The matrix G called Gabor feature matrix at location (x_0, y_0). The feature keypoints will be considered if, for each center block (x_τ, y_τ), block image location satisfies this condition $g(x_\tau + u, y_\tau + v) = 1$,

$$g(\mathrm{x}_\tau + \mathrm{u}, \mathrm{y}_\tau + \mathrm{v}) = \begin{cases} 1, G_{\max}(x_\tau + u, y_\tau + v) > Threshold_{\max} \,\&\, G_{\max}(x_\tau + u, y_\tau + v) > \Delta G_{avg}(x_\tau + u, y_\tau + v), \\ 0, Otherwise. \end{cases} \tag{3.20}$$

For the matching process we need to transform the feature keypoints we sorted in feature vectors. Consider the vector F is the block descriptor then compute:

We know that the according to three previous scales (N_1, N_2 and N_3) Figure 7, we have different features depending on the size reduction have been transform during the scale transformations. We will refer to the initial image to sort the optimal features that we need. A feature selection will first sort lexicographically all the feature textures and then grouping the pairs by using a threshold similarity.

- **Similarity measures:** Let vector F be a feature for object image $I(x, y)$ and every block of the image $I'(x, y)$ under inspection has a feature vector F'_i, $i = 1, \ldots (M' - M + 1) \times (N' - N + 1)$. The process is to find the similar feature between the bloc descriptor. Let first localize vectors on all duplicate pairs. For two duplicated blocks ,let compute the Euclidian distance:

$$Dist(A, B) = \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}, \tag{3.21}$$

where, $A(x_1, y_1)$ and $B(x_2, y_2)$ are the coordinates of the two suspicious pairs.

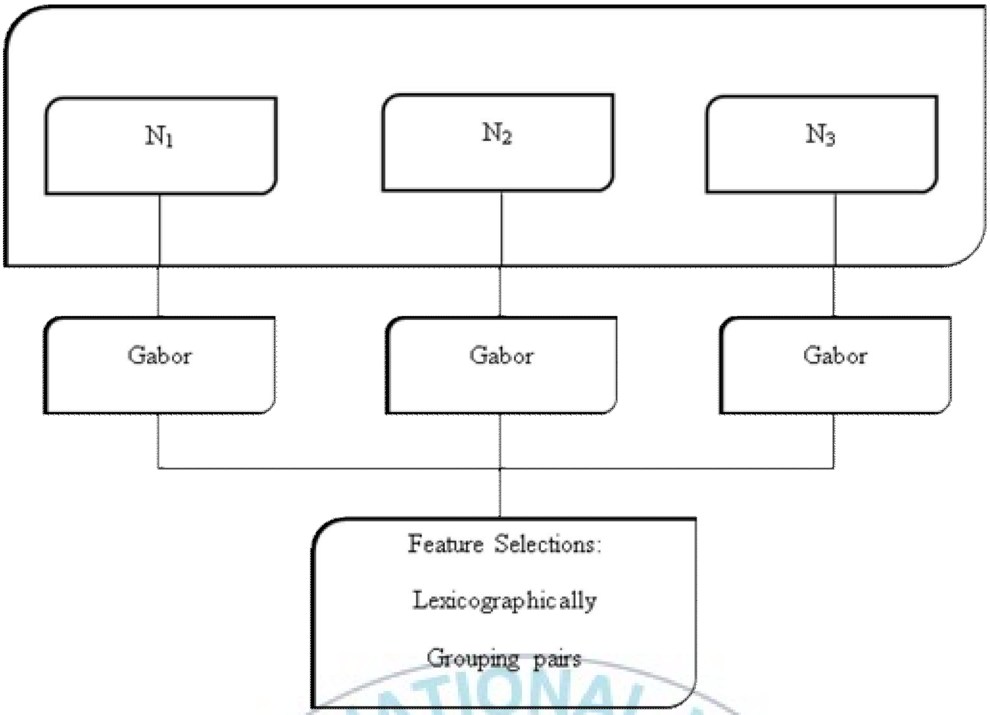


Figure 7: Feature Extractions

Taking account that similar neighbor regions can be assigned to be pair, we discard them now by avoiding wrong matching, and compute :

$$\begin{cases} \left|A(x_1,y_1)-I(x_\tau,y_\tau)\right| \leq Dist(A,B), \\ \left|B(x_2,y_2)-I(x_\tau,y_\tau)\right| \leq Dist(A,B), \end{cases} \tag{3.22}$$

where $A(x_1,y_1)$ and $B(x_2,y_2)$ are coordinates of the suspicious region from the image $I(x,y)$, $I(x_\tau,y_\tau)$ is coordinates of the neighborhood region in $I(x,y)$ and $Dist(A,B)$ the distance between the two pairs A and B.

If we Find that the similar vectors are less than a threshold T_r ,the vector under consideration (if it is A)will be discarded. Otherwise the two blocks vectors are marked as duplicated regions.

Chapter 4

Experimental Results

In this section, we present the experimental results of our proposed method. We simulated our method under a PC Intel (R) Pentium(R) Dual CPU E2160 1.80GHZ, RAM: 4.00GB (2.75 GB usable), and window 7. We used Matlab version R2011a.We evaluated our method by using two dataset .The dataset CASIA V.1.0 which has 800 authentic images, 921 forged color images of 459 copy-move forged and the rest are spliced. We only selected among those images the 459 copy-move forged and the authentic in our work. For the detection performance, we applied some geometric transformations such rotation, scaling, JPEG compression. The size of the image we used is 398×256 pixels, with a JPEG format. The forged imaged are obtained by randomly selecting an image area and copy-pasting it over the image after having applied different attacks such as translation, scaling, rotation or combination of them.

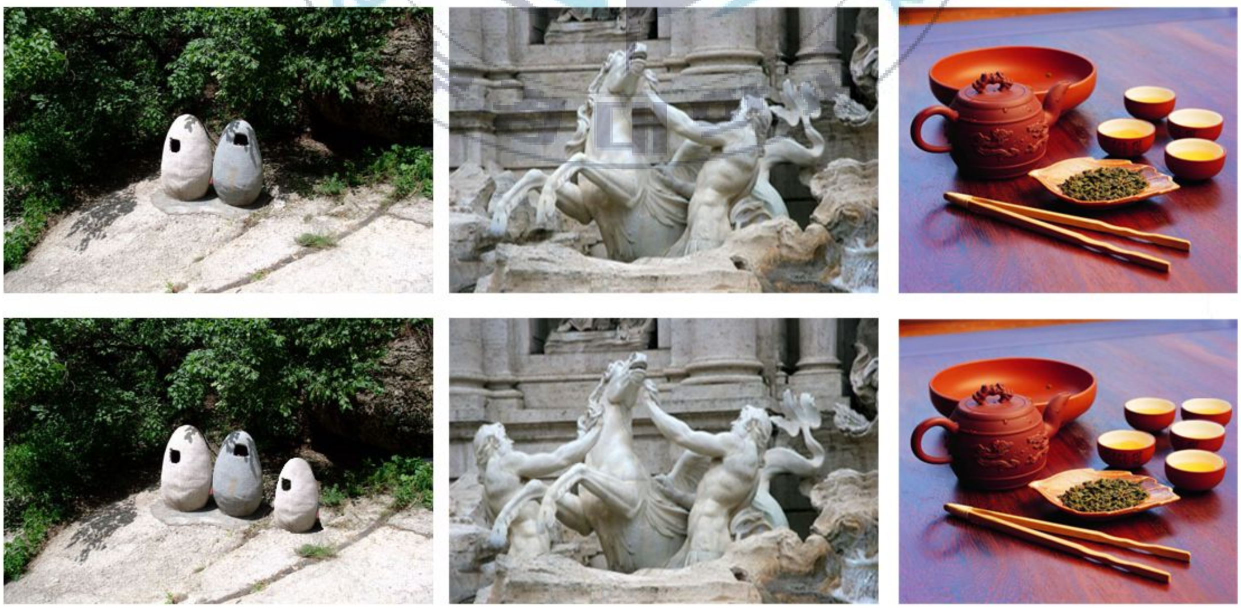


Figure 8: Example Images for Authentic (top row) and Forged Version (bottom row) from Dataset CASIA V.1.0.

4.1 Parameters Settings

The range of frequency information the Gabor filter extracted is defined by the number of scales of the filter, while the directional information is specified by the number of orientations of the filter. The lager the number of scales, the more information from low frequency bands will be extracted. Based on paper [23] published by Yi Jin and Qiu-Qi Ruan where experiences have been done on when the number of orientations varies and the number of scales fixed and another when number of scales varies and the number of orientations is fixed. Gabor filters of five scales and eight orientations are chosen to be used in our following experiments for it reaches the top of the accuracy rate detection.

Methods	Parameters	Features
Gabor [24]	$\theta = 8, \lambda = 5$	Mean and standard deviation of the magnitude
Method [4]	$\alpha = 4, \beta = 3$	60 features
Proposed Method	$\theta = 8, \lambda = 5$	40 features

Table 1: The settings of Parameters

4.2 The Evaluation of the Detection Performance

We quantify the accuracy of detection, with the true positive ratio (TPR) and the false positive ratio (FPR) as follows:

$$TPR = \frac{|\Omega_1 \cap \Omega_2| + |\overline{\Omega_1} \cap \overline{\Omega_2}|}{|\Omega_1| + |\overline{\Omega_2}|}, \tag{4.1}$$

$$FPR = \frac{|\Omega_1 \cup \Omega_2| + |\overline{\Omega_1} \cup \overline{\Omega_2}|}{|\Omega_1| + |\overline{\Omega_1}|} - 1, \tag{4.2}$$

where Ω_1 and Ω_2 are the original region and the detected tampered region, while $\overline{\Omega_1} and \overline{\Omega_2}$ are the forged region and the detected tampered region respectively. The threshold parameters are chosen by highest true positive ratio with corresponding lowest false ratio. The threshold values, similarity is set to 0.3.

4.3 Detection Performance

4.3.1 The Robustness Against Post-Processing Operations

The advantage of our proposed method is that it can resist against geometrical transformations and image processing operations and detect copy move forgery. We have tested our method on dataset CASIA V.1.0. We reach to detect distorted regions with a mixture of post-processing operations. For instance as shown in Figure 8, the copied regions are rotated or scaled and other compressed with JPEG. For the results, we present in Figure 11 by comparing with the Gabor [24] that our proposed method has quite high accuracies at low false matching.

4.3.2 The Performance Comparisons

In this section we are evaluating a comparison of then performance of our method previous work in copy move forgery detection with Gabor [24] and a DCT method [4]. Parameters we used in evaluation are presented in Figure 9. The purpose of this testing is to show the performance off features that we have employed. The accuracies of the features extracted with our method have better performance that the other two methods.

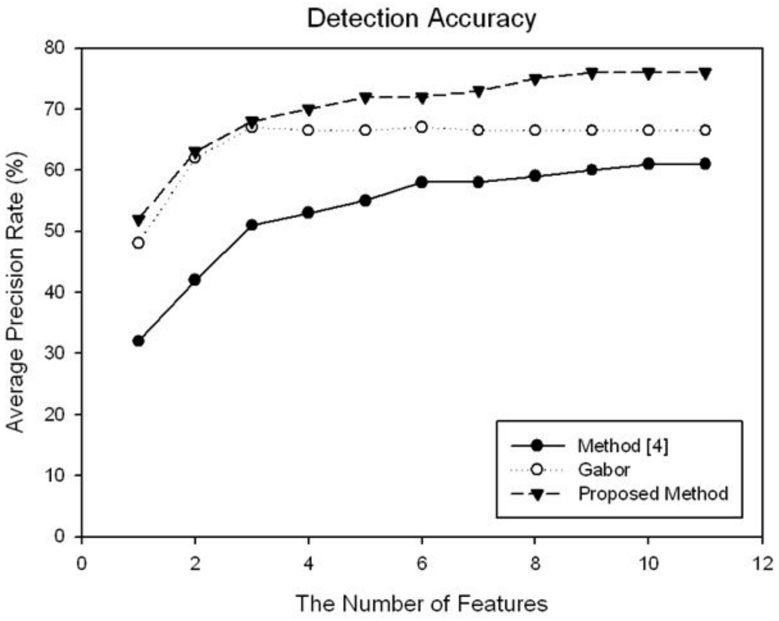


Figure 9: Detection Accuracy

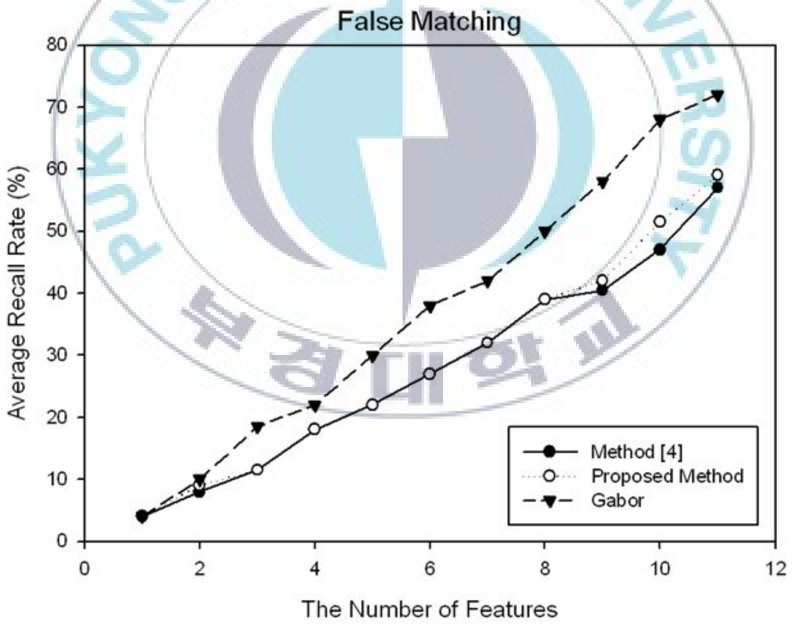


Figure 10: False matching

4.4 Discussion

In this thesis, we proposed forgery detection based on Gabor filter by first enhancing the quality of the image and making the texture feature more robust against different operations and attacks that we can find in image forgery detection. In presence of forgery detection, we know that the key of the detection is the way the features are extracted and the matching features. The proposed method has also taken account of that process by analyzing the texture of the image that have been initially divide in different blocks. And with the features vectors that are robust against operations such as scaling, rotation, illumination, affine transform, occlusion, and so on. We matched them by using two thresholds respectively similarity threshold and the distance threshold for better and efficient forgery detection. We have noticed that the method proposed has a problem to detect images with small regions copied and pasted in corner of the image.

Chapter 5

Conclusion

Digital image forensics can be defined as the science that the aim is to analyze an digital image content, to give a report such as the extract information can be trust or useful to the scene represented in that specific digital image. The fact that nowadays, with the easy access of the internet and the development of many softwares, the manipulations of the tools makes the trust and the authentication process more difficult for this area. In response to these challenges, digital image forensics has carefully started a study of the cause of forgery and the challenge that face the image. Based on that, different approached and algorithms have been developed to determine the authenticity of the image. Two kind of techniques have been proposed: active and passive techniques .The problem with the active method is that it needs the information about the original image, which bring an delicate issue because most on the case we don't have it. The passive method was been then proposed as a solution of that problem. The advantage of this passive method is that depending of the information you have, it is easy to detect the forgery. Some algorithms have been proposed like the forgery can be detected by analyzing the trace left by source device, others by analyzing the uniformity of the image or by analyzing the contents itself of the image and use that information to detect the forgery.

In this thesis, challenges and types of forgery have been discussed. Additionally methods and algorithms have been presented which have brought out the motivation of this work. As the texture can generate useful information about the image, we proposed a technique based on texture analysis to get the informations that we will use during the detection process.

Although, the proposed method shows a considerable performance, image forgery detection is a huge area with different manner of tampering. For that reason, we still have a work to do by developing a lot of algorithm for better authentication.

References

[1] Babak, M. and Stanislav, S.,“ Blind methods for detecting image fakery, ” IEEE Aerospatial Electronic System Magasin,Vol.4, pp. 18–24,2010.

[2] Ren,Y., Ping, X.-J., He,Z.Y. and Zhang, S.-Z,“A survey on Passive-Blind Image Forgery By Doctor Method Detection ,” International Conference on Machine Learning and Cybernetics,Vol.6, pp.3464-3467,2008.

[3] Granty, R. E. J., Aditya, T. S. and Madhu, S. S.,“Survey on Passive Methods of Image Tampering Detection,” Proceedings of the International Conference on Communication Computational Intelligence,pp.431-436,2010.

[4] Wandji, N. D.,Xingming, S. and Kue, M. F.,“Detection of copy-move forgery in digital images based on DCT,” International Journal of Scientific and Research Publications, Vol.3,2013.

[5] Shivakumar, B.L.and Baboo, S.S.,“Detecting copy-move forgery in digital images: a survey and analysis of current methods,” Global J. Computer Science Technology,Vol.10, pp. 61–65,2010.

[6] Shaid, S.,Z.,M.,“Estimating optimal block size of copy-move attack detection on highly textured image”,Thesis Submitted to the University of Technology, Malaysia,2009.

[7] Amerini, I., Ballan ,L., Caldelli ,R., Bimbo A., D., and Serra ,G.,“A SIFT-based Forensic Method for Copy-Move Attack Detection and Transformation Recovery,” IEEE Transactions on Information Forensics and Security,Vol.6,no. 3, pp. 1099–1110,2011.

[8] Bashar, M., Noda ,K., Ohnishi, N. and Mori, K.,“Exploring Duplicated Regions in Natural Images,” IEEE Transactions on Image Processing, Image Processing ,pp. 1,2010.

[9] Christlein,V., Riess, C., Jordan ,J.,Riess, C., R. and Angelopoulou, E.,“An Evaluation of Popular Copy -Move Forgery Detection Approaches,” IEEE Transactions on Information

forensics and security,Vol.7, N0.6,pp. 1841-1854,2012.

[10] Krawtez, N., “A pictures worth digital image analysis and forensics,” Black Hat Briefings, Available at www.hackerfactor.com/papers/bh-usa-07-krawetz-wp.pdf. , pp. 1–31, 2007.

[11] Ali Qureshi, M. and Deriche, M.,“A Review on Copy-Move Image Forgery Detection Techniques,” 11th International, Multi-Conference on Systems, Signals & Devices (SSD), pp.1-5,2014.

[12] Amerini,I., Ballan, L., Caldelli, R., Del Bimbo, A. and Serra, G.,“A sift-based forensic method for copy-move attack detection and transformation recovery, ” IEEE Transactions on Information Forensics and Security ,Vol.26, no.2, pp.1099-1110,2011.

[13] Farid, H.,“Image Forgery Detection,” IEEE Signal Processing Magazine,Vol.26,no.2, pp.16-25,2009.

[14] Farid, H.,“Image Forgery Detection,” IEEE Signal Processing Magazine,Vol.26,no.2,pp.16-25,2009.

[15] Pann, X. and Lyu, S.,“Region duplication detection using image feature matching,” IEEE Transactions on information Forensics and Security ,Vol. 5, no. 4, pp. 857-867,2010.

[16] Lin, H.-J., Wang, C.-W., Kao, Y.-T. and aI.,“Fast copy-move forgery detection,” WSEAS Transactions on Signal Processing,Vol. 5, no. 5, pp. 188-197,2009.

[17] Ardizzone, E.,Bruno ,A. and Mazzola ,G.,“Copy-move forgery detection via texture Description,” Proceedings of the 2nd ACM workshop on Multimedia in forensics, security and intelligence. NY, USA: ACM, pp. 59-64,2010.

[18] Gotze ,N., Drue ,S. and Hartmann ,G.,“Invariant object recognition with discriminant features based on local fast-Fourier Mellin transform,” in Proc. International Conference of Pattern Recognition,Vol. 1, pp. 948–951,2000.

[19] Resnick,J.,“The Radon Transform and Some of Its Applications,”IEEE Transaction on Acoustics Speech and Signal Processing,Vol.33, pp. 338-339,1985.

[20] Rahtu, E., Salo, M. and Heikkila, J.,“ Affine Invariant Pattern recognition using Multiscale Auto convolution,” IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol.27, no.6, pp. 908-918,2005.

[21] Wang, T., Tang, J., Zhao, W., Xu, Q. and Luo B.,“Blind Detection of Copy-Move Forgery Based on Multi-Scale Autoconvolution Invariants,” Pattern Recognition Communications in Computer and Information Science,Vol.321, pp. 438-446,2012.

[22] Kyrki, V. and Kamarainen, K.,K.,“Simple Gabor Feature Space for Invariant Object Recognition,” Pattern Recognition Letters,Vol. 25, pp. 311–318,2004.

[23] Jin,Y. and Ruan, Q. ,“Gabor –Based Improved Locality Preserving Projections for Face Recognition,” Computing and Informatics,Vol. 1, pp. 153-156,2007 .

[24] Hsu, C.,H. and Wang, M.,S.,“Detection of Copy-Move Forgery Image Using Gabor Descriptor,” IEEE Anti-Counterfeiting Security ,pp. 1-4,2012.

Acknowledgement
(감사의 말씀)

I want to first of all thank God for all the blessing and strength he has given me to go through this course to completing my Master thesis. It was not easy but it is a refreshing feeling to get to this point.

From the very first day I arrived in Busan, Republic of Korea, I knew it would be a journey that I will never forget. A spectacular one for that matter undertakes my Master program at the Pukyong National University. Not forgetting the amazing culture shock that was bound to hit me as a foreigner, I was received warmly by Professor Kyung Hyune Rhee.

I would like at the same time to thank Dr. Chul Sur, and Dr. Yong-Ho Park for their variable helps and guidance since starting my research. Their thoughtful comments and encouragement on my research are highly appreciated.

Also special thanks to the chairman of my thesis committee, Professor Man- Gon Park, and other members, Professor Chang- Soo Kim and Professor Kyung Hyune Rhee, for their valuable comments, and assistance that have greatly enhanced my thesis. Besides, I would like to appreciate the other professors and secretaries of the department of Information Security and the department of IT Convergence and Application Engineering in PKNU for their help.

This project wouldn't have been possible if not for the great support and guidance of all the LISIA (Lab of Information Security and Internet Application) Members. My deep knowledges to the following colleagues in LISIA: Dr Munkbataar Doyodorj and Sonia Carol Kouayep who had help me in many ways, to the rest of the lab members, Lewis NKENYEREYE, Otieno Mark Brian, Myeong Hak Heo, Kaung Myat Sam. I will forever be grateful and owe it all to all of you for bringing a big change to my life as an academic and social person as a whole.

I dedicate this thesis to my parents NEMEYE Sylvestre and NGENZEBUHORO Suzanne, all my sisters and brothers in law, to rest of my family, friends and those who have been praying for me, special thought to Ferdinand BANKUWIHA because without them I will not be where I am right now.

Sheilha NININAHAZWE

October 21, 2014