



TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
CENTRAL CAMPUS, PULCHOWK

THESIS NO.: 070MSCS651

IMAGE SPLICING FORGERY DETECTION

**BY
ALIZA TANDUKAR**

A THESIS
SUBMITTED TO THE DEPARTMENT OF ELECTRONICS AND
COMPUTER ENGINEERING IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN
COMPUTER SYSTEM AND KNOWLEDGE ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING
LALITPUR, NEPAL

February, 2015

IMAGE SPLICING FORGERY DETECTION

by
Aliza Tandukar
070MSCS651

Thesis Supervisor
Dr. Dibakar Raj Pant
Head of Department

A thesis submitted in partial fulfillment of the requirement for
the degree of Master of Science in Computer System and Knowledge
Engineering.

Department of Electronics and Computer Engineering
Institute of Engineering, Central Campus, Pulchowk
Tribhuvan University
Lalitpur, Nepal

February, 2017

COPYRIGHT ©

The author has agreed that the library, Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk Campus, may make this thesis freely available for inspection. Moreover the author has agreed that the permission for extensive copying of this thesis work recorded herein or, in their absence, by the Head of Department, wherein this thesis was done. It is understood that the recognition will be given to the author of this thesis and to the Department of Electronics and Computer Engineering, Pulchowk Campus in any use of the material of this thesis. Copying of publication or other use of this thesis for financial gain without approval of the Department of Electronics and Computer Engineering, Institute of Engineering, Pulchowk Campus and author's written permission is prohibited.

Request for permission to copy or to make any use of the material in this thesis in whole or part should be addressed to:

Head
Department of Electronics and Computer Engineering
Institute of Engineering, Pulchowk Campus
Pulchowk, Lalitpur, Nepal



TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS
DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

Ananda Niketan, Pulchowk, Lalitpur, P.O. Box 1175, Kathmandu, Nepal.
Tel : 5534070, 5521260 extn. 315, Fax : 977-1-5553946, E-mail : doece@ioe.edu.np

Our Ref :

Departmental Acceptance

The thesis entitled "**Image Splicing Forgery Detection**", submitted by **Aliza Tandukarin** partial fulfillment of the requirement for the award of the degree of "**Master of Science in Computer System and Knowledge Engineering**" has been accepted as a bonafide record of work independently carried out by her in the department.

Dr. Dibakar Raj Pant

Head of Department

Department of Electronics and Computer Engineering

Pulchowk Campus

Institute of Engineering

Tribhuvan University

Nepal.



TRIBHUVAN UNIVERSITY
INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS
DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

Ananda Niketan, Pulchowk, Lalitpur, P.O. Box 1175, Kathmandu, Nepal.
Tel : 5534070, 5521260 extn. 315, Fax : 977-1-5553946, E-mail : doece@ioe.edu.np

Our Ref :

CERTIFICATE OF APPROVAL

The undersigned certify that they had read, and recommended to the Institute of Engineering for acceptance, a thesis report entitled "**Image Splicing Forgery Detection**" submitted by **Aliza Tandukar** in a partial fulfillment of the requirements for the award of the degree of "**Master of Science in Computer System and Knowledge Engineering**".

Supervisor, Dr. Dibakar Raj Pant

Head of Department

Department of Electronics and Computer Engineering

External Examiner: Mr. Subhash Dhakal

Department of IT, Ministry of Science and Technology

Committee Chairperson: Dr. Subarna Shakya

Professor

Department of Electronics and Computer Engineering

DATE OF APPROVAL: February, 2017

ACKNOWLEDGEMENT

First of all, I would like to express my sincere gratitude to the Department of Electronics and Computer Engineering for providing the opportunity to research and further increase my knowledge in the field of engineering through this thesis work which is a partial fulfillment for the degree of Master of Science in Computer Systems and Knowledge Engineering.

I would like to express the deepest appreciation to my supervisor, Head of Department **Dr. Dibakar Raj Pant** for his guidance throughout the period of this work. His invaluable support, understanding and expertise have been very important in completing this work. It was a great honor for me to pursue my thesis under his supervision.

I am grateful to our MSCSKE Coordinator **Dr. Aman Shakya, Dr. Sanjeeb Prasad Pandey, Prof. Dr. Shashidhar Ram Joshi, Prof. Dr. Subarna Shakya, Dr. Baburam Dawadi** and **Dr. Basanta Joshi** for their encouragement and guidance to this thesis defense period.

Likewise, I would like to extend my appreciation to all of my friends for their advice and encouragement during my thesis work.

Finally, a special thanks to my family for supporting me and encouraging me with their blessings to accomplish this work.

Aliza Tandukar

(070/MSCS/651)

ABSTRACT

The rapid development of digital technology has raised challenges for ensuring authenticity of digital images. Image splicing, which has constituted a menace to integrity and authenticity of images, is a very common and simple trick in image tampering. Image splicing creates a composite image by cropping and pasting regions from the same or different images. Spliced images could be so eye-deceiving that they are scarcely distinguished from authentic ones even without any post processing. Therefore, image-splicing detection is of great importance in digital forensics. The forged picture however leaves some clues which can be used to locate the manipulated regions. In this paper, an effective algorithm for revealing image-splicing forgery is proposed. Firstly the algorithm converts input RGB image into YCbCr color channel. The four-level Discrete wavelet transform on each color channel is applied, the sharp edges, which are traces of cut-paste manipulation, are high frequencies and detected from LH, HL and HH sub-bands. The four level inverse discrete wavelet transform is applied by removing low frequency components and considering only high frequency components. Afterwards difference between obtained chroma components and luminance component is calculated. The morphological operation is applied to reconstruct the boundaries of sharp edge regions. The obtained largest and second largest regions are compared to determine whether the image is forged or not based on noise inconsistency level. If the obtained difference is above 1dB the input image is forged image else original. If the image is forged one, the method defines the region having maximum area to be forged region. When a fake is confirmed, suspicious regions becomes objects to be considered. Then the quality measures of the obtained result has been evaluated by means of sensitivity, specificity and accuracy. The experimental results demonstrate the robustness of the algorithm in exposing image splicing forgeries with accuracy of 88%.

Keywords— Image forgery; Splicing; YCbCr color channel; Discrete Wavelet Transform (DWT); Inverse Discrete Wavelet Transform (IDWT); Chroma components; Image tampering.

Table of Contents

COPYRIGHT	ii
DEPARTMENTAL ACCEPTANCE	iii
CERTIFICATE OF APPROVAL	iv
ACKNOWLEDGEMENT	v
ABSTRACT	vi
List of Figures	ix
List of Tables	x
List of Abbreviations	xi
CHAPTER ONE: INTRODUCTION	
1.1 Background	2
1.2 Problem Statement	3
1.3 Objectives	4
1.4 Scope of the Work	4
1.5 Organization of Report	4
CHAPTER TWO: LITERATURE REVIEW	
2.1 Related Work	6
CHAPTER THREE: METHODOLOGY	
3.1 General	9
3.2 Proposed Method	9
3.2.1 Color space	9
3.2.2 Four Level decomposition using Wavelet Transform	10
3.2.3 Compute Difference between Chroma and Luminance Components	15
3.2.4 Edge detection	15
3.2.5 Morphological operation	17
3.2.6 Detecting whether the image obtained is forged or not	19
3.2.7 Locating the tampered region in forged image	20
3.3 Research Design	21
CHAPTER FOUR: EXPERIMENTS AND DISCUSSIONS	
4.1 Image Dataset	23
4.2 Results and Discussion	24
4.2.1 Different Steps of Proposed Algorithm	28

4.2.2. Performance Evaluation.....	31
CHAPTER FIVE: CONCLUSION	
5.1 Conclusion	34
5.2 Future Enhancement	34
REFERENCES	37
Appendix A.....	37
Appendix B	39
Appendix C.....	46

List of Figures

Figures	Page
Figure 1.1: The steps of image splicing	3
Figure 1.2: Example showing Forgery in Image (Taken from CASIA Database)	3
Figure 3.1: An RGB image and its YCbCr components.....	10
Figure 3.2: One-level decomposition of 2-D image.	11
Figure 3.3: Four-level decomposition of 2-D Image	12
Figure 3.4: Four level decomposition of Y- component.....	13
Figure 3.5: Analysis decomposition of 2-D wavelet transform.....	13
Figure 3.6: Synthesis Reconstruction of 2-D inverse discrete wavelet transform.....	14
Figure 3.7: Inverse Four-level decomposition of Y, Cb and Cr image respectively	14
Figure 3.8: Output obtained by computation	15
Figure 3.9: Output image after applying Sobel operation.....	17
Figure 3.10: Morphological Dilation of a Binary Image	18
Figure 3.11: Output image after applying dilation operation	19
Figure 3.12: Wiener Filtering	19
Figure 3.13: Copy-paste Forgery. The tampered region is identified by a red outline.....	20
Figure 3.14: Research Design	21
Figure 4.1: A sample of Original images from the database	23
Figure 4.2: A sample of forged images from the database	24
Figure 4.3: Experimental results of tampered images	26
Figure 4.4: Some unsuccessful cases of tampered images	27
Figure 4.5: (a)-(c) Sample 1 Input Image (d)-(j) overall process of proposed method	28
Figure 4.6: (a)-(c) Sample 2 Input Image (d)-(j) overall process of proposed method	29
Figure 4.7: Sample GUI 1 of Tampered Image (forged portion: flower)	30
Figure 4.8: Sample GUI 2 of Tampered Image (forged portion: ball).....	30
Figure 4.9: Experimental results of authentic images.....	31
Figure 4.10: Detection result on different levels of wavelet transforms.....	32

List of Tables

Tables	Page
Table 1: Edge detection convolution kernels	16
Table 2: Image neighborhood	17
Table 3: Structuring element to bridging gaps.....	18
Table 4: Description of the Evaluated Datasets	23
Table 5: Detection result on different level of wavelet transforms	32

List of Abbreviations

CASIA	Chinese Academy of Sciences Institute of Automation
DWT	Discrete Wavelet Transform
FN	False Negatives
FP	False Positives
HH	Sub-band of DWT containing high frequency components
HL	Sub-band of DWT containing horizontal components
HPF	High Pass Filter
IDWT	Inverse Discrete Wavelet Transform
LH	Sub-band of DWT containing vertical components
LL	Sub-band of DWT containing low frequency components
LPF	Low Pass Filter
TN	True Negatives
TP	True Positives
YCbCr	Luminance; Chroma: Blue; Chroma: Red

CHAPTER 1
INTRODUCTION

1. INTRODUCTION

1.1 Background

Modern information technology brings great convenience in our daily life; however, as every coin has two sides, "Seeing is not believing" [1]. The advent of sophisticated photo editing software has made it increasingly easier to manipulate digital images. Forged images have appeared in tabloid magazines, mainstream media outlets, scientific journals, political campaigns, courtrooms, and the photo hoaxes that land in our e-mail in-boxes. These doctored photographs are appearing with growing frequency and sophistication, and even experts often cannot rely on visual inspection to distinguish authentic images from forgeries [2]. It is important to develop a credible method to detect whether digital image is doctored or not. Often visual inspection cannot definitively distinguish the resulting forgeries from photographs. The modification of an image can be used for malicious purposes such as hide some important traces from an image. This modified image can result in transmission of incorrect information. As consequences, the integrity and authenticity of digital image is lost. Therefore, digital Image forgery detection techniques have emerged over past few years to regain trust in digital images.

Image forgery detection techniques are classified into two main categories: active and passive. Active techniques, detect the forgery by validating the integrity of a pre-embedded (i.e. by a camera) signature or watermark. Since many available cameras are not having the ability to embed such kind of signature [3], this approach has a limited scope. In contrast to active approaches, passive techniques do not need any watermark or prior information about images. They depend on the original characteristics of the image [4], which let them to be widely used and become a hot research topic in digital image forensics. Basically, passive techniques draw the highest attention as they require no collaboration on the part of the user through some types of watermarks or signature.

There are three different types of passive techniques in digital image forgery: Copy-Move, Image splicing and Image retouching image forgery.

In **Copy-move image forgery**, one part of the image is copied and pasted on other part of the same image. In other words, the source and destination of the modified image is originated from the same image.

In **Image splicing**, two images to create one tampered image or it is a technique that involves a composite of two or more images, which are combined to create a fake image.

In **Image Retouching**, the images are less modified. It just enhances some features of the image. For example by adding onto brightness, creating noise, creating clarity onto the base image etc.

Among these image manipulation techniques, image composition or image splicing is most common. The following Figure 1.1 shows one of the example forms of the image splicing process and its steps [5].

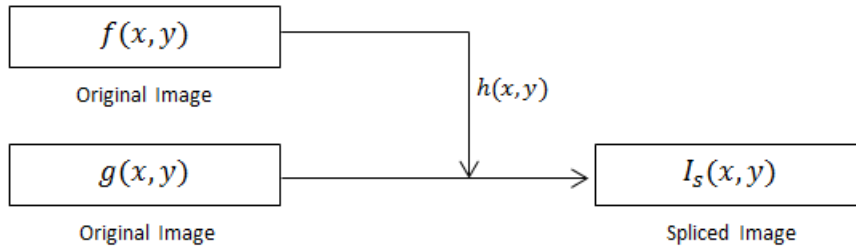


Figure 1.1: The steps of image splicing

As shown in figure 1.1, $f(x, y)$ and $g(x, y)$ are original images, $h(x, y)$ is a part of $f(x, y)$ which is inserted into $g(x, y)$ and generate spliced image $I_s(x, y)$ as shown below:

$$f(x, y) = f'(x, y) + h(x, y) \quad (1)$$

$$I_s(x, y) = g(x, y) + h(x, y) \quad (2)$$



Figure 1.2: Example showing Forgery in Image (Taken from CASIA Database)

As shown in Figure 1.2, by copying a spliced portion from the source image Figure(a) into a base image Figure (b), one can create a composite image Figure(c) or scenery to cheat others with the help of state-of-art image editing software, even non-professional users can perform splicing without much difficulty.

1.2 Problem Statement

With the rapid growth of cheap and high-resolution digital cameras, high-performance computers, and powerful image-processing software, it is getting easier to manipulate a digital image without leaving obvious visual traces. As a matter of fact, many tampered images have occurred in news coverage, scientific experiments, and even for legal evidences. We have always puzzled that which images are believable in our daily life. Spliced images could be so eye-deceiving that they are hardly distinguished from authentic ones. In addition, malicious image-splicing manipulation may mislead the public and persuade them to believe something that never exists. Image splicing techniques has increased which forms a serious threat to a security of digital images. Therefore, splicing detection is of fundamental importance in image tampering detection.

1.3 Objectives

- To design a method for copy paste image forgery detection using image chroma components of color channel which can better reflect the splicing introduced traces.
- To detect tampered traces from the forged image.

1.4 Scope of the Work

The scope of the thesis is on the implementation of image splicing detection in different images. A reliable splicing detection system for digital images will be useful in areas such as journalism, forensic investigation, criminal investigation, insurance processing, surveillance systems, intelligence services, and medical imaging.

1.5 Organization of Report

The report is divided into five chapters. A brief description of each chapter is presented below:

- **Chapter 1:** This chapter has described a brief introduction to image splicing forgery and the objectives. The definition of the problem has been included in this chapter.
- **Chapter 2:** The relevant literature studied and referred in the course of this research work has been included in this chapter.
- **Chapter 3:** This chapter includes the methodology used in thesis work. It explains method that is implemented for image splicing tampering detection.
- **Chapter 4:** This chapter includes the experimental results, evaluation and discussion on proposed method.
- **Chapter 5:** This chapter includes the conclusion of the thesis and future enhancement for future researches in the area.

CHAPTER 2
LITERATURE REVIEW

2. LITERATURE REVIEW

2.1 Related Work

Sheldon Sensenig[6] proposed a simple method of localizing a noise tampered region of a forged image. The method focuses on tiling an image with non-overlapping blocks and calculating noise features for each block based on noise estimation, de-noising algorithms and wavelet analysis. This technique was not capable of finding random noise that could be added across an entire image to conceal image tampering.

Wei Wang et al. [7] introduced passive color image splicing detection method based on gray level co-occurrence matrix (GLCM) of thresholded edge image of image chroma. Edge images were generated by subtracting horizontal, vertical, main and minor diagonal pixel values from current pixel values respectively and then thresholded with a predefined threshold T . The GLCMs of edge images along the four directions served as features for image splicing detection. Boosting feature selection is applied to select optimal features and Support Vector Machine (SVM) is utilized as classifier in our approach.

Y Zhang et al. [9] proposed a method where the local binary pattern operator is used to model magnitude components of two-dimensional arrays obtained by applying multisize block discrete cosine transform to test images. Then, all of bins of histograms computed from local binary pattern codes were served as discriminative features for image-splicing detection. After that, kernel principal component analysis was utilized to reduce the dimensionality of the proposed features to avoid the high computational complexity, high mutual correlation among the constructed features and possible overfitting for support vector machine classifier. Finally, support vector machine classifier was employed to distinguish spliced images from authentic images by using the final dimensionality-reduced feature set.

Archana V Mire et al. [11] proposed JPEG forgery detection based on 8x8 block Discrete Cosine Transform (DCT) transform to detect the shift of DCT block alignment. Differences of JPEG compression in an image can be caused by the splicing. The splicing detection was proposed by analyzing and suggesting solutions for cases making the differences in compression history including detections of Aligned Double JPEG, Non Aligned Double JPEG, Primary Quantization Table, JPEG ghost.

Mahdi Hariri et al. [12] introduced an image splicing forgery detection algorithm based on LBP, wavelet transform and PCA. The algorithm converts input RGB image into YCbCr color channel, afterwards chrominance component is divided into non-overlapping blocks. Secondly Local Binary Pattern (LBP) operator is performed, and wavelet transform is applied in all blocks. Finally, Principal Component Analysis (PCA) is used for all blocks and the output is fed to Support Vector Machine (SVM) classifier as features. The classifier detects whether input image is forged or not.

Harpreet Kaur et al. [13] introduced image forgery detection using steerable pyramid transform and LAB color space. The algorithm converts RGB image to LAB color space. SPT is applied to chrominance component; the output is a number of sub bands that are translation and rotation invariant. LBP is applied in each SPT sub band to obtain local texture descriptor. The algorithm annotates forged area and unforger area into two colors.

Upendra Ujjainiya et al. [14] proposed image forgery detection algorithm based on combination of two algorithms wavelet transform function and clustering algorithm using cluster selection technique. The wavelet transform function gives the texture feature of original and forged image. After extraction of feature of original and forged image generate pattern of cluster. The distribution of data using the partition clustering technique creates block of pattern. The process of standard deviation measures the block of difference of original and forged image. This algorithm reduces the value of false negative and improves the value of detection. But this technique used both original and forged image.

CHAPTER 3
METHODOLOGY

3. METHODOLOGY

3.1 General

The use of image splicing often changes image structure, which means sharp edges are usually introduced by splicing. The method detects image splicing artifacts based on the observation of image edges in chroma channels. Since, image splicing (splicing artifacts) can be regarded as detecting weak signal in the background of strong signal (image contents), detecting splicing artifacts in Y channel which preserves most of image contents is usually difficult task. In contrary, Cb and Cr channels contain chromatic information which is less related to image content. Therefore, detecting image splicing in chroma channels can be regarded as detecting weak signal in the background of weak signal which reduces detecting difficulties [7].

3.2 Proposed Method

3.2.1 Color space

The visibility of tampering traces varies in different color model. Image forgery detection techniques usually work in grayscale and RGB color systems. However, recent researches [7], [9] and [12] found that using chromatic channel rather than luminance or RGB enhanced the detection performance [9].

YCbCr color model represents colors in the form of luminance (Y) and chrominance (Cb and Cr) components. Cb represents the blue difference chroma component and Cr represents the red difference chroma component. Human vision perceives the luminance component in a better way than chrominance component. Therefore, most of the tampering traces, which could not be detected by naked eyes, are hidden in the chromatic channel.

YCbCr in Rec.ITU – RBT.601 – 6 is defined as a linear transform from R, G and B channels which is formulated in (3):

$$\begin{pmatrix} Y \\ Cb \\ Cr \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.117 \\ -0.299 & -0.587 & 0.886 \\ 0.701 & -0.587 & -0.114 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} + \begin{pmatrix} 16 \\ 128 \\ 128 \end{pmatrix} \quad (3)$$

The spliced regions will have sharp edges while the authentic objects in the image will have smooth edges. These spliced edges are more visible in chroma components.

Figure 3.1 shows color image and its Y, Cb and Cr color components:

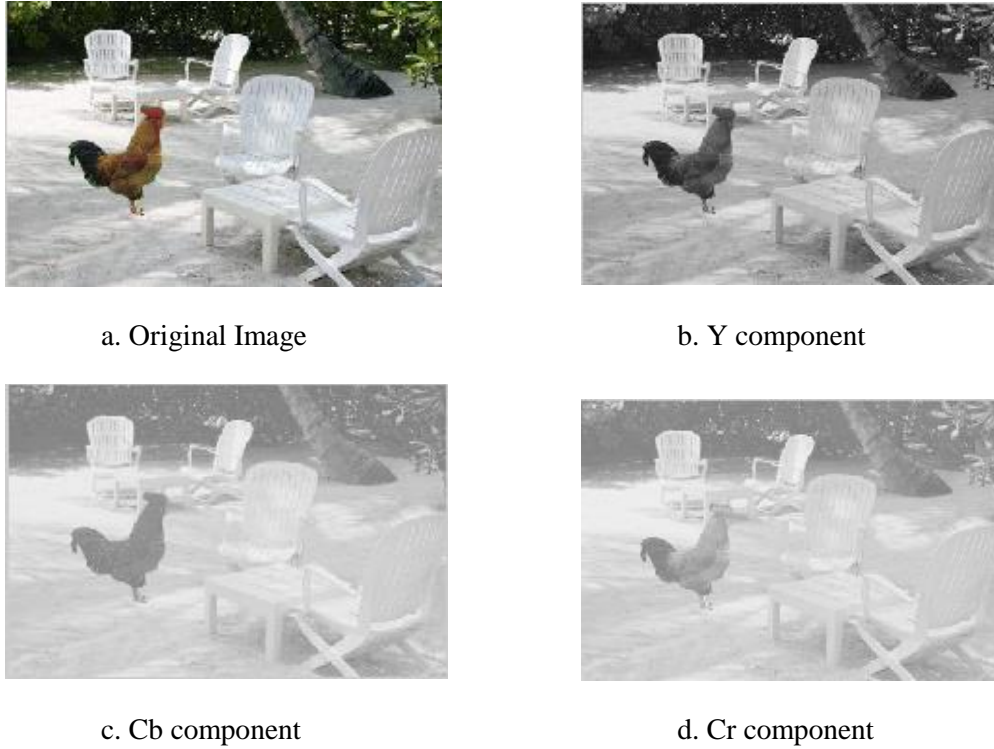


Figure 3.1: An RGB image and its YCbCr components.

3.2.2 Four Level decomposition using Wavelet Transform

In order to weaken the effect of smooth variation (image content), the discrete wavelet transform is introduced in this part. An image is represented as a two-dimensional array of coefficients, each coefficient representing the brightness level in that point. Most natural images have smooth color variations, with the fine details being represented as sharp edges in between the smooth variations. Technically, the smooth variations in color can be termed as low frequency variations and the sharp variations as high frequency variations. The low frequency components (smooth variations) constitute the base of an image, and the high frequency components constitute the edges which gives the detail of the image. Separating the smooth variations and details of the image can be done in many ways. One such way is the decomposition of the image using a Discrete Wavelet Transform (DWT).

The discrete wavelet transform (DWT) is an implementation of the wavelet transform using a discrete set of the wavelet scales and translations obeying some defined rules. The wavelets are made from an extension of modified capability called mother wavelet. DWT is basically an arrangement of filters: wavelet filter and scaling filter. The wavelet filter is a high pass filter and scaling filter is a low pass filter. The DWT has many variations, viz. Daubechies wavelet, Haar wavelet and so on. The method has utilized Daubechies wavelet for decomposition of image into levels.

The DWT of image $f(x,y)$ of width M pixels and height N pixels is done by defining the approximation and directional coefficients as below:

$$W_{\phi}(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} f(x, y) \phi_{j_0, m, n}(x, y) \quad (4)$$

$$W_{\Psi}^i(j_o, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} f(x, y) \Psi_{j_o, m, n}^i(x, y) \quad (5)$$

$$f(x, y) = \frac{1}{\sqrt{MN}} \sum_m \sum_n W_{\phi}(j_o, m, n) \phi_{j_o, m, n}(x, y) + \frac{1}{\sqrt{MN}} \sum_{i=H, V, D} \sum_{j=j_o}^{\infty} \sum_m \sum_n W_{\psi}^i(j, m, n) \phi_{j_o, m, n}^i(x, y) \quad (6)$$

where j_o is an arbitrary scale, $W_{\phi}(j_o, m, n)$ are approximation coefficients of image $f(x, y)$ at scale j_o and $W_{\psi}^i(j, m, n)$ are coefficients used to add the horizontal, vertical and diagonal details for scale $j \geq j_o$.

After applying one level and four level discrete wavelet transform, an image is decomposed in approximation, horizontal, vertical and diagonal part as shown in Figure 3.2 and Figure 3.3 respectively:

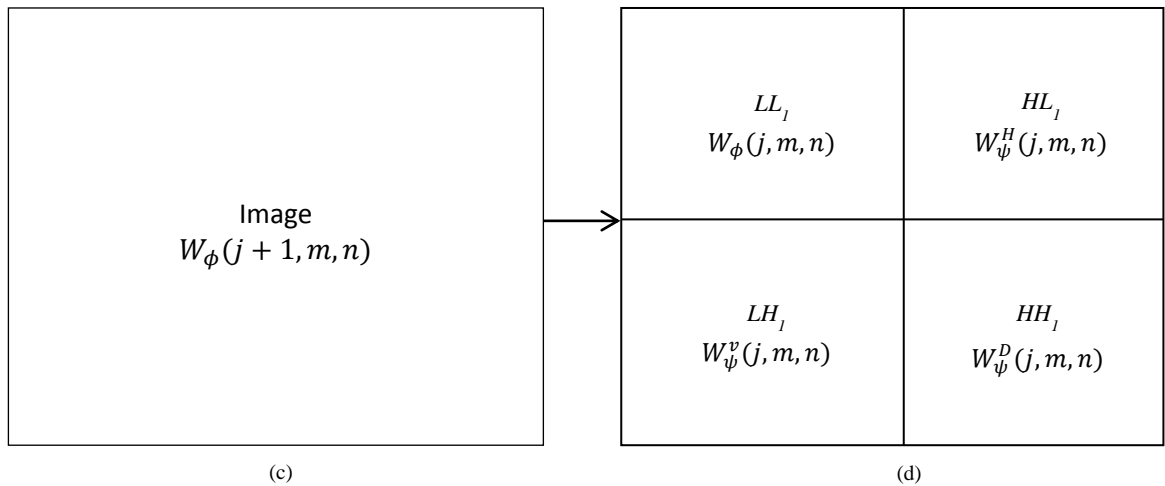
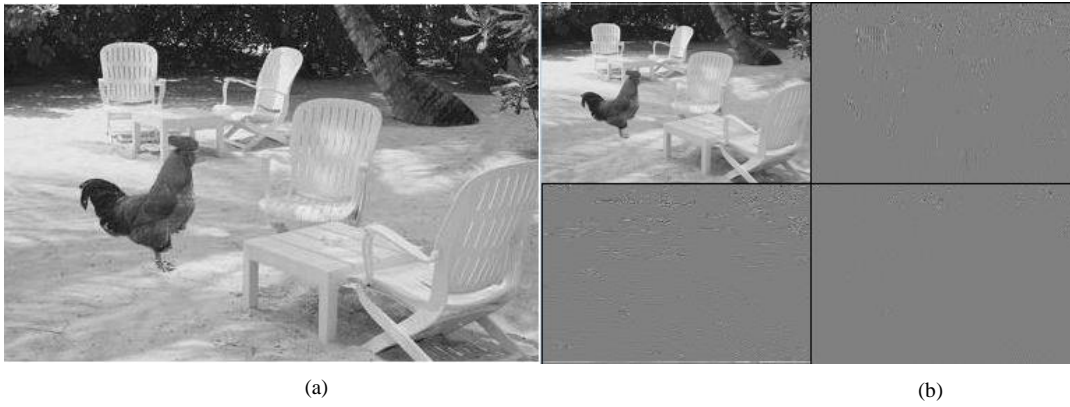


Figure 3.2: One-level decomposition of 2-D image.

(a) The original image, (b) A one-level DWT. (c), (d) Positions of corresponding sub-bands

As a result of decomposition, we get the estimates: sub-band low- low (LL), flat sub-band low-high (LH), vertical sub-band high-low (HL) and diagonal sub-band high-high (HH) for each component. The LL image is considered a reduced version of the original as it retains most details. The LH image contains horizontal edge features, while the HL contains vertical edge features. The HH contains high frequency information only. In wavelet decomposition, only the LL can be decomposed once again in same manner, thereby producing even more sub-bands. This can be done up to any level, thereby resulting in a pyramidal decomposition as shown in Figure 3.3.

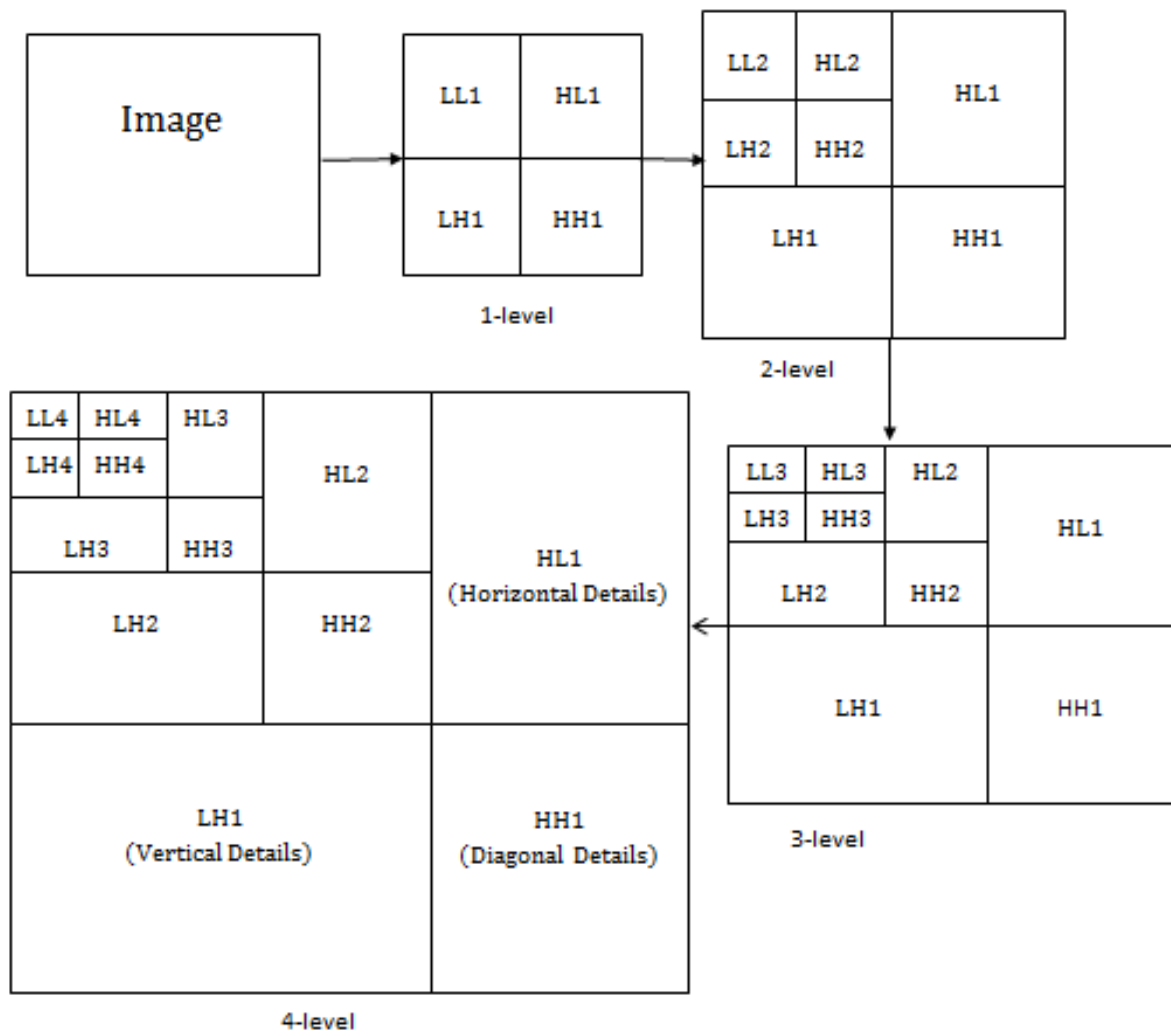


Figure 3.3: Four-level decomposition of 2-D Image

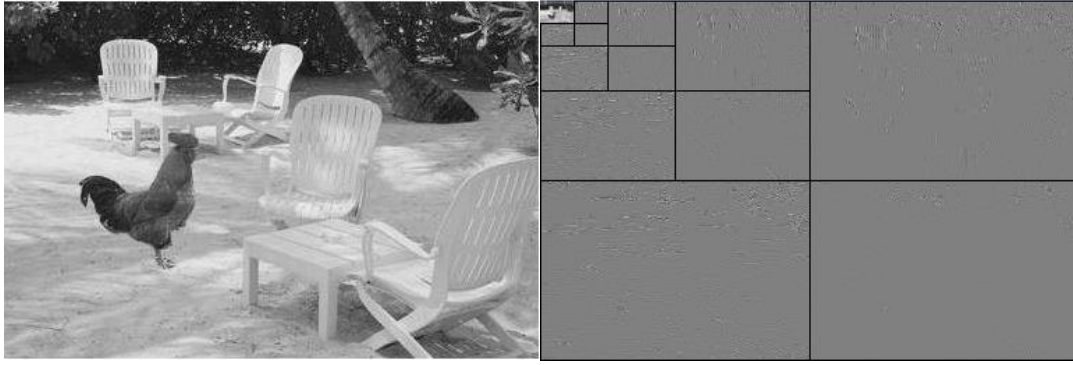


Figure 3.4: Four level decomposition of Y- component

The Schematic diagram of 2-D wavelet transform for one level analysis is shown below in Figure 3.5:

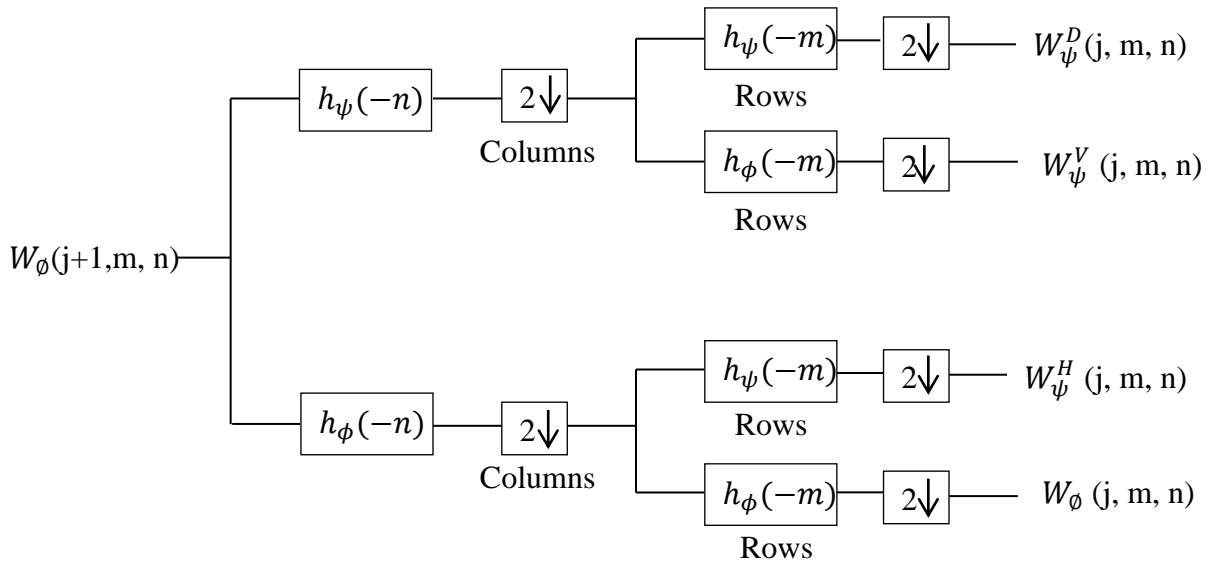


Figure 3.5: Analysis decomposition of 2-D wavelet transform

In this method, four-level discrete wavelet transform is applied on each color channel. The sharp edges which are the traces of cut-paste manipulation are higher frequencies and are detected in detail sub-bands i.e. LH, HL and HH sub-bands of decomposition. Therefore, the three sub-bands are considered to detect the edges. Also, the low frequencies in LL sub-band of fourth level decomposition are ignored by setting them to zero. Therefore, to reconstruct the original image with lower frequency removed utilize the process known as inverse discrete wavelet transform.

Just as a forward transform is used to separate the image data into various classes of importance, a reverse transform is used to reassemble the various classes of data into a reconstructed image. A pair of high pass and low pass filters is used here also. This filter pair is called the Synthesis Filter pair. The filtering procedure is just the opposite - start from the topmost level, apply the filters column wise first and then row wise, and proceed to the next level, till we reach the first level.

The schematic diagram of 2-D inverse wavelet transform for one level analysis is shown below in Figure 3.6:

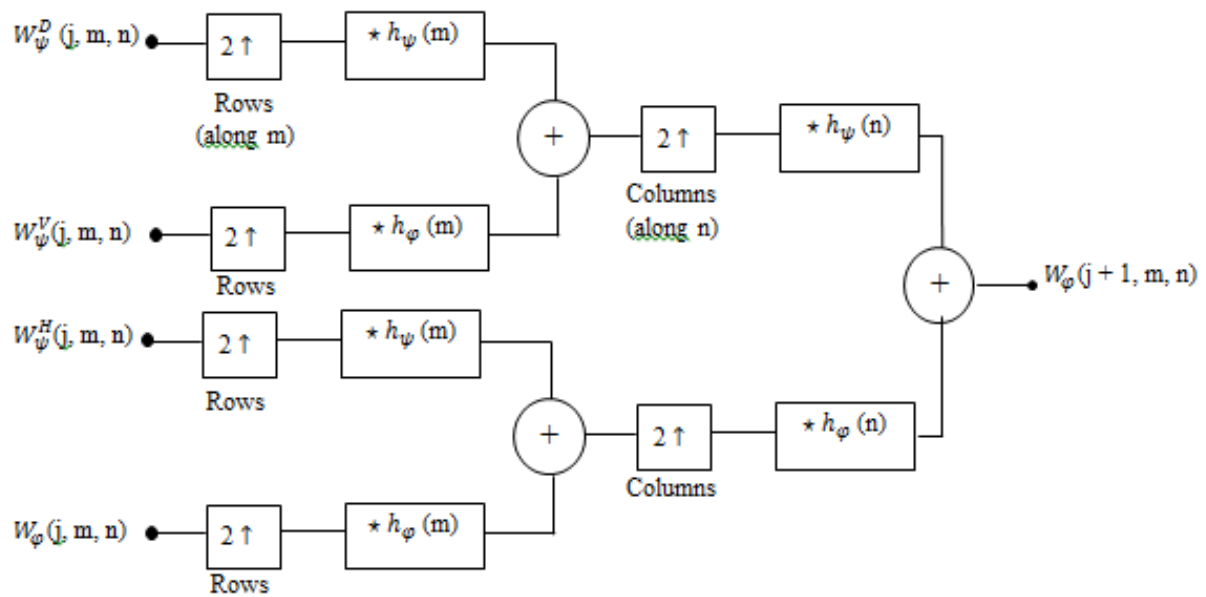


Figure 3.6: Synthesis Reconstruction of 2-D inverse discrete wavelet transform

The output obtained from inverse discrete wavelet transform consists of high frequency components i.e. sharp edges, boundaries as shown in figure 3.7 below.



Figure 3.7: Inverse Four-level decomposition of Y, Cb and Cr image respectively

3.2.3 Compute Difference between Chroma and Luminance Components

The spliced regions will have sharp edges while the authentic objects in the image will have smooth edges. The Sharpness of edges can be the traces of cut-paste manipulation. On computing the difference between chroma components and luminance components can better reflect the splicing edges. Therefore, the method computes difference between chroma components and luminance components as shown below:

$$\text{Output Image} = -Y + Cb + Cr \quad (7)$$



Figure 3.8: Output obtained by computation

From Figure 3.8, we find that in the output obtained by difference between chroma and luminance component original image edges are much smoother than the splicing introduced edges (say the contour of hen) and even some of original image edges are disappeared. Based on this observation, the method makes use of output image obtained from difference between chroma and luminance components for further processing steps.

3.2.4 Edge detection

Edge detection refers to the process of identifying and locating sharp discontinuities in an image. The discontinuities are abrupt changes in pixel intensity which characterize boundaries of objects in a scene. Classical methods of edge detection involve convolving the image with an operator (a 2-D filter), which is constructed to be sensitive to large gradients in the image while returning values of zero in uniform regions.

The Sharpness of edges can be the traces of cut-paste manipulation. Therefore, edge detection with highest sharpness are collected, considered and tested. Based on this observation, the method make use of output image obtained from difference between chroma and luminance components for further processing steps by a convolution of obtained image and a Sobel kernel. The Sobel operator is an algorithm for edge detection in images. Therefore, on applying Sobel operator we can search the suspicious region having edges with highest sharpness as shown in Figure 3.9 (c).

The Sobel operator performs a 2-D spatial gradient measurement on an image and so emphasizes regions of high spatial frequency that correspond to edges. An image gradient is a change in intensity (or color) of an. An edge in an image occurs when the gradient is greatest and the Sobel operator makes use of this fact to find the edges in an image. The Sobel operator calculates the approximate image gradient of each pixel by convolving the

image with a pair of 3×3 filters. These filters estimate the gradients in the horizontal (x) and vertical (y) directions and the magnitude of the gradient is simply the sum of these 2 gradients as shown in Table 2. One kernel is simply the other rotated by 90° , where the central pixel in each row and column is weighted by 2 to provide smoothing.

-1	0	1	1	2	1
-2	0	2	0	0	0
-1	0	1	-1	-2	-1
$\frac{\partial f}{\partial x}$			$\frac{\partial f}{\partial y}$		

Table 1: Edge detection convolution kernels

These kernels are designed to respond maximally to edges running vertically and horizontally relative to the pixel grid, one kernel for each of the two perpendicular orientations. The kernels can be applied separately to the input image, to produce separate measurements of the gradient component in each orientation. These can then be combined together to find the absolute magnitude of the gradient at each point and the orientation of that gradient.

The gradient of an image is given by:

$$\nabla f = \left[\frac{\partial f}{\partial x}, \frac{\partial f}{\partial y} \right] \quad (8)$$

Typically, edge strength is given by gradient magnitude which is computed as:

$$\|\nabla f\| = \text{mag}(\nabla f) = \sqrt{(\partial f / \partial x)^2 + (\partial f / \partial y)^2} \quad (9)$$

To simplify computation, this quantity is approximated sometimes by using absolute values as below:

$$\text{mag}(\nabla f) = \left| \frac{\partial f}{\partial x} \right| + \left| \frac{\partial f}{\partial y} \right| \quad (10)$$

The angle of orientation of the edge (relative to the pixel grid) giving rise to the spatial gradient is given by:

$$\theta = \tan^{-1} \left(\frac{\frac{\partial f}{\partial y}}{\frac{\partial f}{\partial x}} \right) \quad (11)$$

Often, this absolute magnitude is the only output the user sees, the two components of the gradient are conveniently computed and added in a single pass over the input image.

where, A is an input image, B is the structuring element and \hat{B} is the reflection of B and $(\hat{B})_z$ is the shifting of \hat{B} by z. This equation is based on obtaining the reflection of B about its origin and shifting the reflection by z. Hence, dilation of A with B is a set of all displacement, Z such that (B) and A overlap by at least one element. Dilation adds pixel to the boundaries of objects in an image. The number of pixels added depends on the shape size of the structuring element.

Based on this interpretation the equation can be rewritten as:

$$A \oplus B = \{ z \mid [(\hat{B})_z \cap A] \subseteq A \} \quad (13)$$

By applying dilation of A by the structuring element B defined in Table 3, repairs gap in boundaries which are traces of cutting and pasting.

1	1	1
1	1	1
1	1	1

Table 3: Structuring element to bridging gaps

The following Figure 3.13 illustrates the dilation of a binary image. Note how the structuring element defines the neighborhood of the pixel of interest, which is circled. The dilation function applies the appropriate rule to the pixels in the neighborhood and assigns a value to the corresponding pixel in the output image. In the Figure 3.10, the morphological dilation function sets the value of the output pixel to 1 because one of the elements in the neighborhood defined by the structuring element is on.

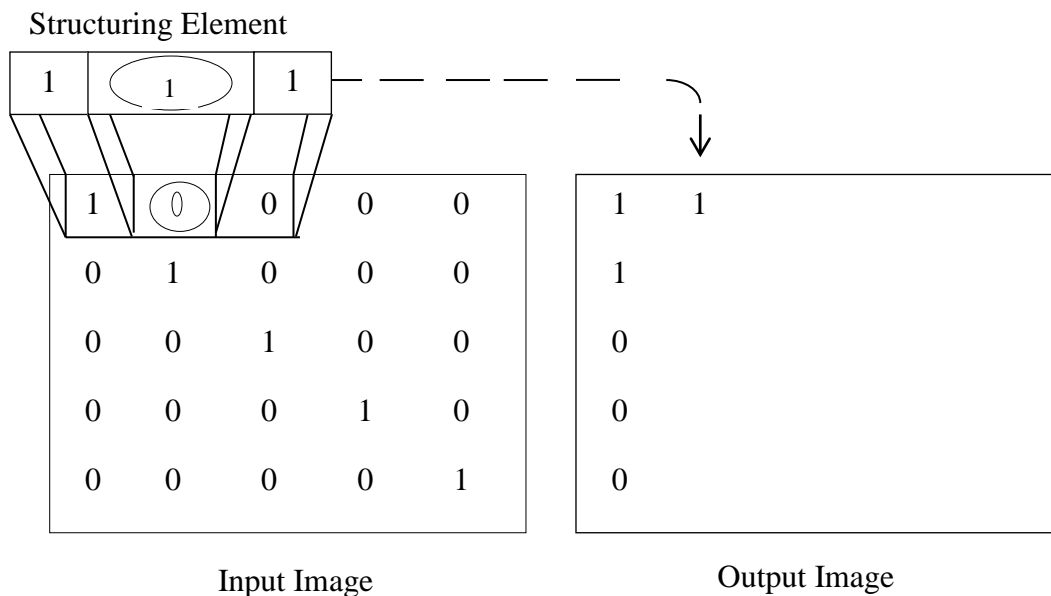


Figure 3.10: Morphological Dilation of a Binary Image

Figure 3.11(b) shows the obtained image after applying dilation operation to image obtained using edge operation Figure 3.11(a). Then, the obtained binary image holes are filled as shown in figure 3.11(c).

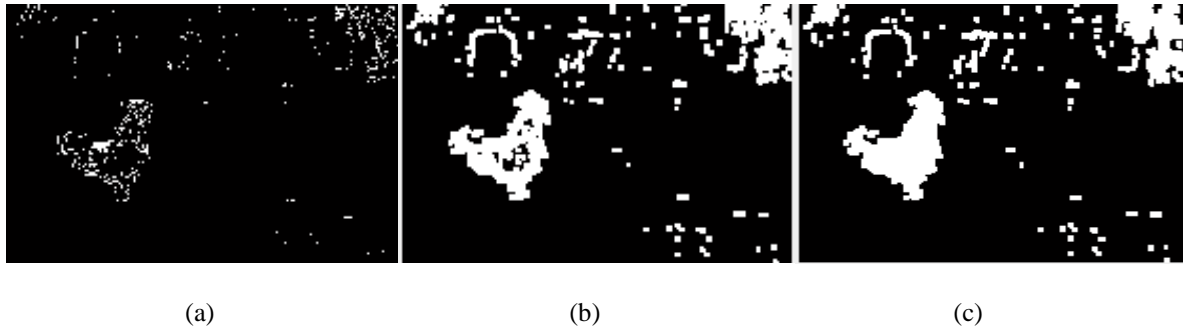


Figure 3.11: Output image after applying dilation operation

(a)Original Image, (b) Dilation Operation, (c) Filling Holes

3.2.6 Detecting whether the image obtained is forged or not

The image noise is defined as the random deviation of the brightness/ contrast and the color information. The image noise is basically produced by the camera sensor while the image is being photographed. It is an unwanted by-product of the image capture that adds forged information in the image. Every image is supposed to have a noise as a by-product of the capturing process. But, noise is typically fairly uniform throughout an authentic image. So, the inconsistency in the noise can be used to detect whether the image is forged or not.

The purpose of Wiener filter is to filter out noise that has corrupted an image. It is based on statistical approach. Wiener filter minimizes mean square error between filtered image $\hat{f}(x, y)$ and original image $f(x, y)$.

$$e^2 = E \left\{ (f(x, y) - \hat{f}(x, y))^2 \right\} \quad (14)$$

where, E is the expected value operator and f is the un-degraded image.

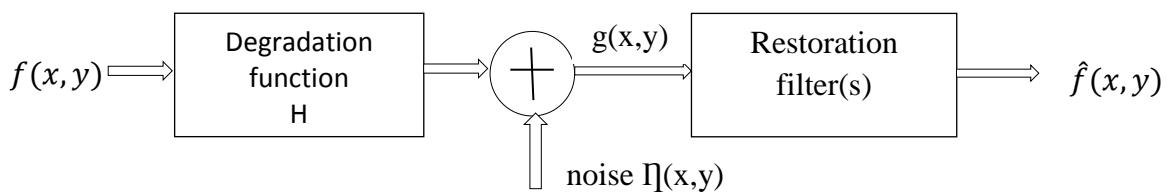


Figure 3.12: Wiener Filtering

The wiener2function applies a Wiener filter which is a type of linear filter to an image adaptively, tailoring itself to local image variance. Where the variance is large, wiener2 performs little smoothing. Where the variance is small, wiener2 performs more smoothing. This approach often produces better result than linear filtering. The adaptive filter is more selective than a comparable linear filter, preserving edges and other high frequency parts of an image. In addition, there are no design tasks; the wiener2 function handles all preliminary computations, and implements the filter for an input image. Wiener2, however, does require

more computations time than linear filtering. Wiener2 works best when the noise is constant-power (“white”) additive noise, such as Gaussian noise.

After applying morphological operation we obtain connected regions. Among the connected regions we take two larger area sections of the image. The random noise may be introduced in the tampering process as a means of concealing the tampered region. Therefore, for each section, 3 x 3 Wiener filter is applied and the filtered image is subtracted from the selected regions. This difference will result us the noise present in that section.

The mean of the absolute value of this subtraction is given in equation:

$$f = \frac{\sum_{i=1}^n |p_i - w_i|}{\text{no.of pixels}} \quad (14)$$

where, p_i is a given pixel in the area and w_i is the corresponding pixel in the filtered region and n is the total number of pixels.

If the calculated noise is below threshold value T , it will be the section of same image which means original image else forged image.

3.2.7 Locating the tampered region in forged image

Afterwards, if the image obtained is forged one, the method finds region with maximum area and define that region as spliced region of image. The method again performs edge detection basically to create a red lining on selected region.

Figure 3.13 shows the output obtained based on proposed method:



Figure 3.13: Copy-paste Forgery. The tampered region is identified by a red outline.

3.3 Research Design

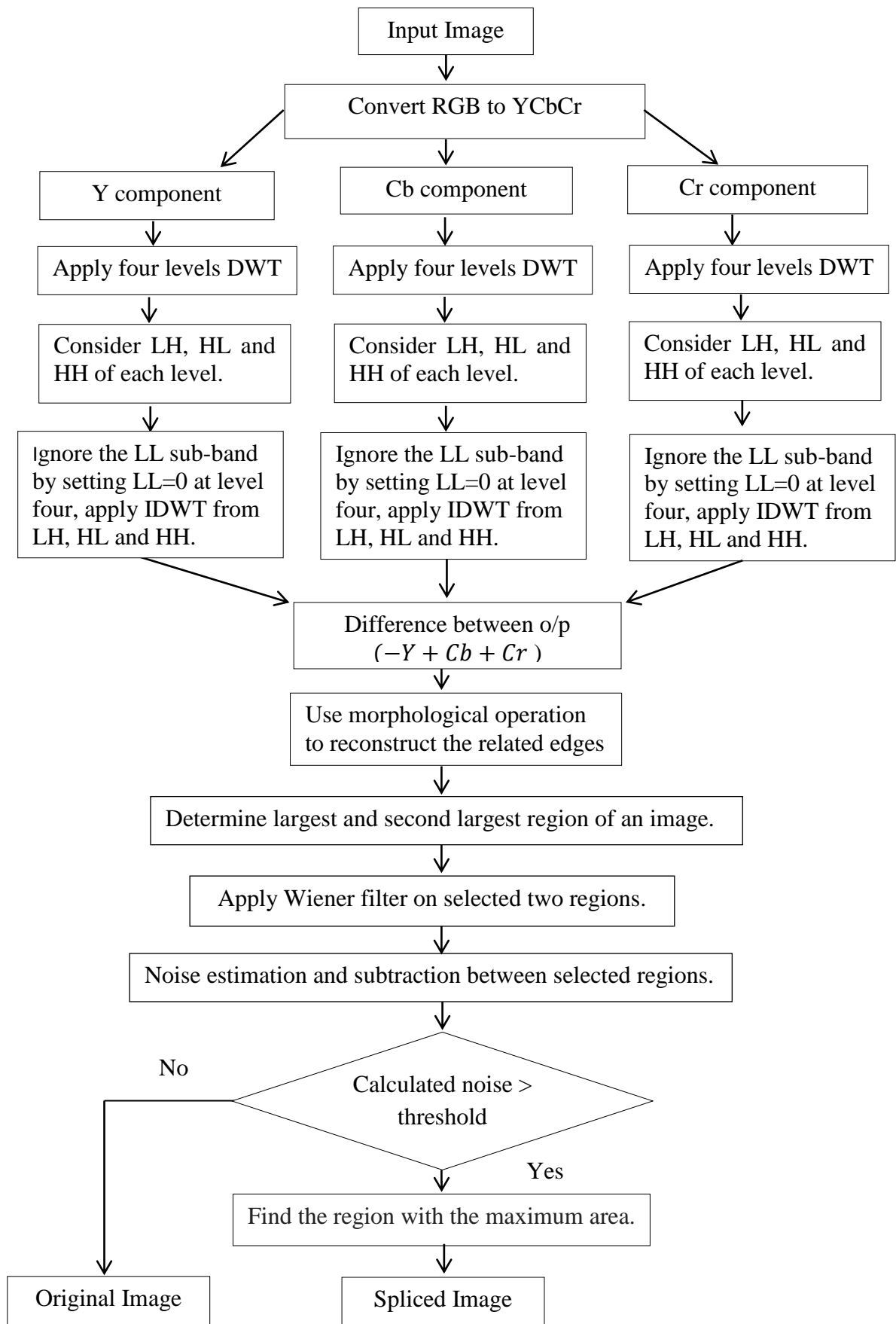


Figure 3.16: Research Design

CHAPTER 4
EXPERIMENTS AND DISCUSSIONS

4. EXPERIMENTS AND DISCUSSIONS

4.1 Image Dataset

The proposed method is evaluated using two benchmark databases: CASIA Tampered Image Detection Evaluation Database Version 1.0 (CASIA TIDE v1.0) [16] and CASIA TIDE v2.0 [17]. It is an image dataset designed to evaluate copy-move and image splicing detection methods.

Table below provides a description of these datasets.

Table 4: Description of the Evaluated Datasets

Dataset	No. of Images			Image Type	Image Size
	Authentic	Tampered	Total		
CASIA v1.0	800	921	1,721	jpg	384x256 To 256x384
CASIA v2.0	7,491	5,123	12,614	jpg tif bmp	240x160 To 1152x768

Figure 4.1 below shows some of authentic images from both datasets:



Figure 4.1: A sample of Original images from the database

Figure 4.2 below shows some of forged images from both dataset:



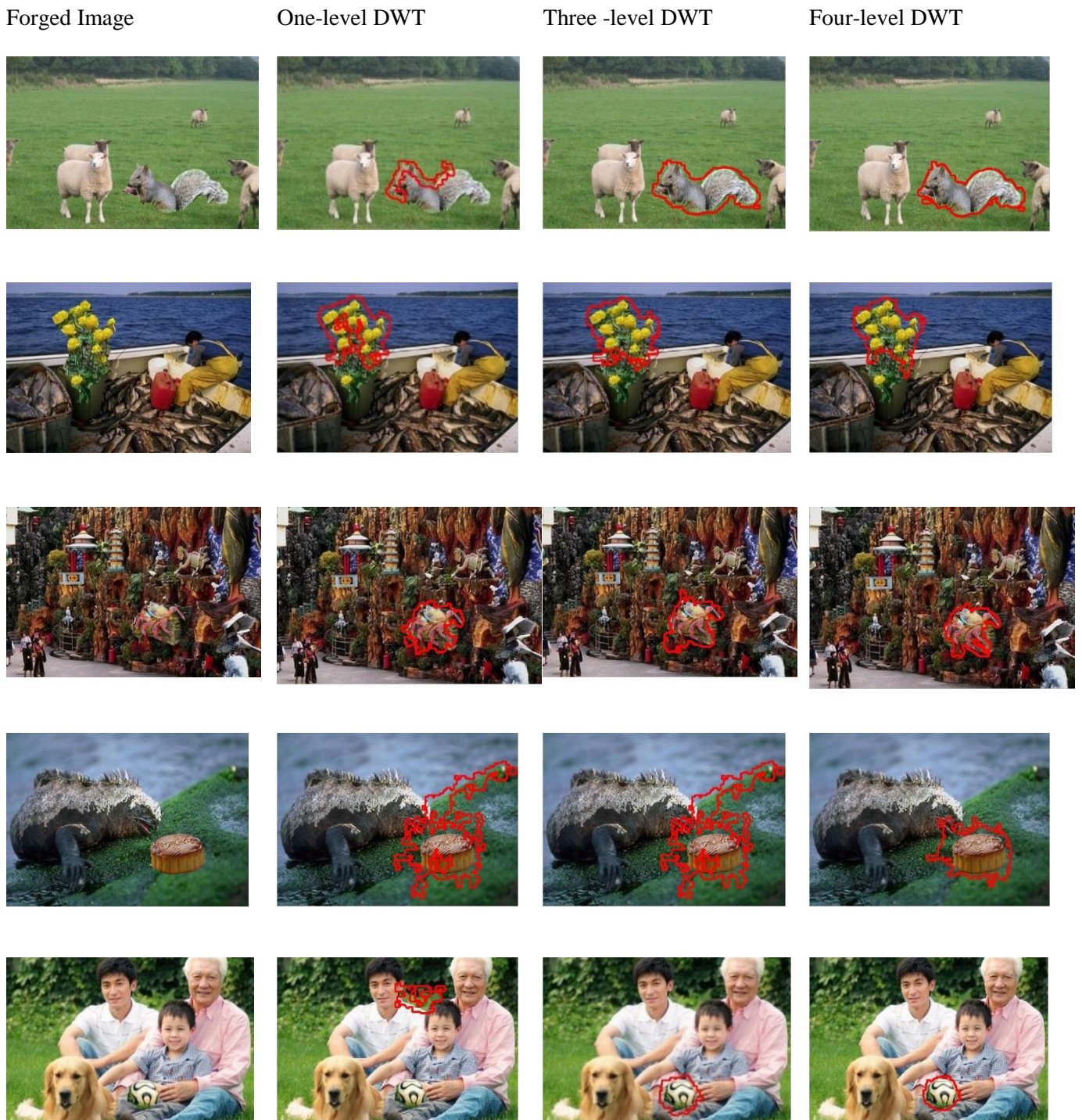
Figure 4.2: A sample of forged images from the database

4.2 Results and Discussion

Firstly the color image is converted to YCbCr color space. Figure 4.4 shows each level of decomposition, the four-level of decomposition lead us to better results. Therefore, a counterfeit is firstly defined from the sharpness of edges and boundaries presented by high frequencies at the three sub-bands LH, HL and HH of four-level DWT decomposition which are traces of cutting and pasting. To detect the cutting/pasting parts, the low frequencies in LL sub-band are ignored by setting them to zero. Therefore, Inverse discrete wavelet transform from these four sub-bands shows an image with only edges and boundaries. Then difference between obtained chroma components and luminance component was performed to obtained suspicious edges. The morphological operation is applied to reconstruct the boundaries of forged regions afterwards detect whether the input image is forged or not based on noise present in the image. If the image is forged one, define the region having maximum area to be forged region. When a fake is confirmed, suspicious regions becomes objects to be considered.

Figure 4.3 and Figure 4.4 shows the positive and negative experimental results respectively:

Experimental Positive Results:



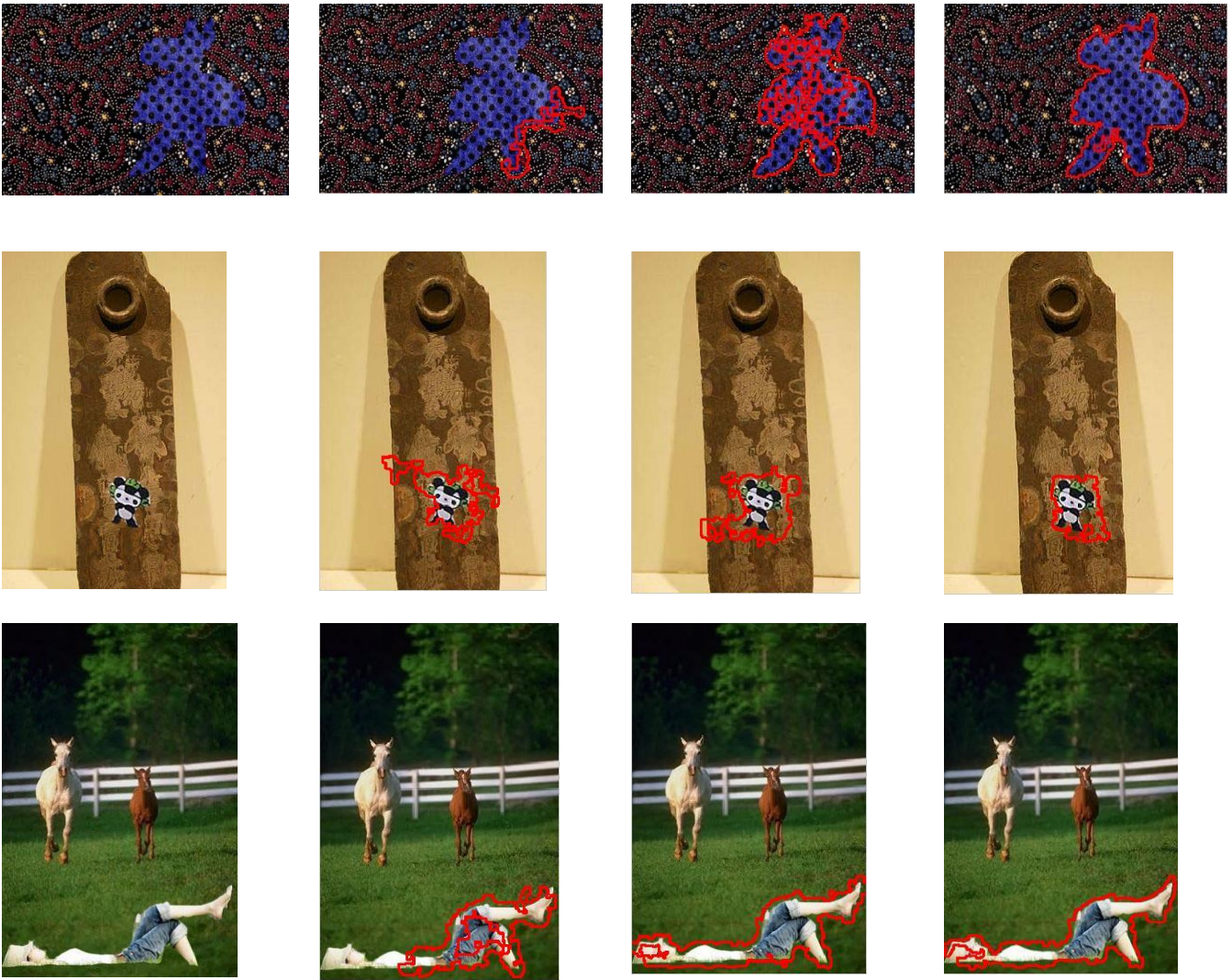


Figure 4.3: Experimental results of tampered images

Figure 4.3 shows experimental results of tampered images. First column shows tampered images from CASIA database. Second column, third and last column are first, third and fourth level decomposition using discrete wavelet transform respectively. Last column showed the detection of more accurate tampered region locations given by our algorithm. Therefore, fourth level of decomposition showed better result than other level of decomposition.

Experimental Negative Results:

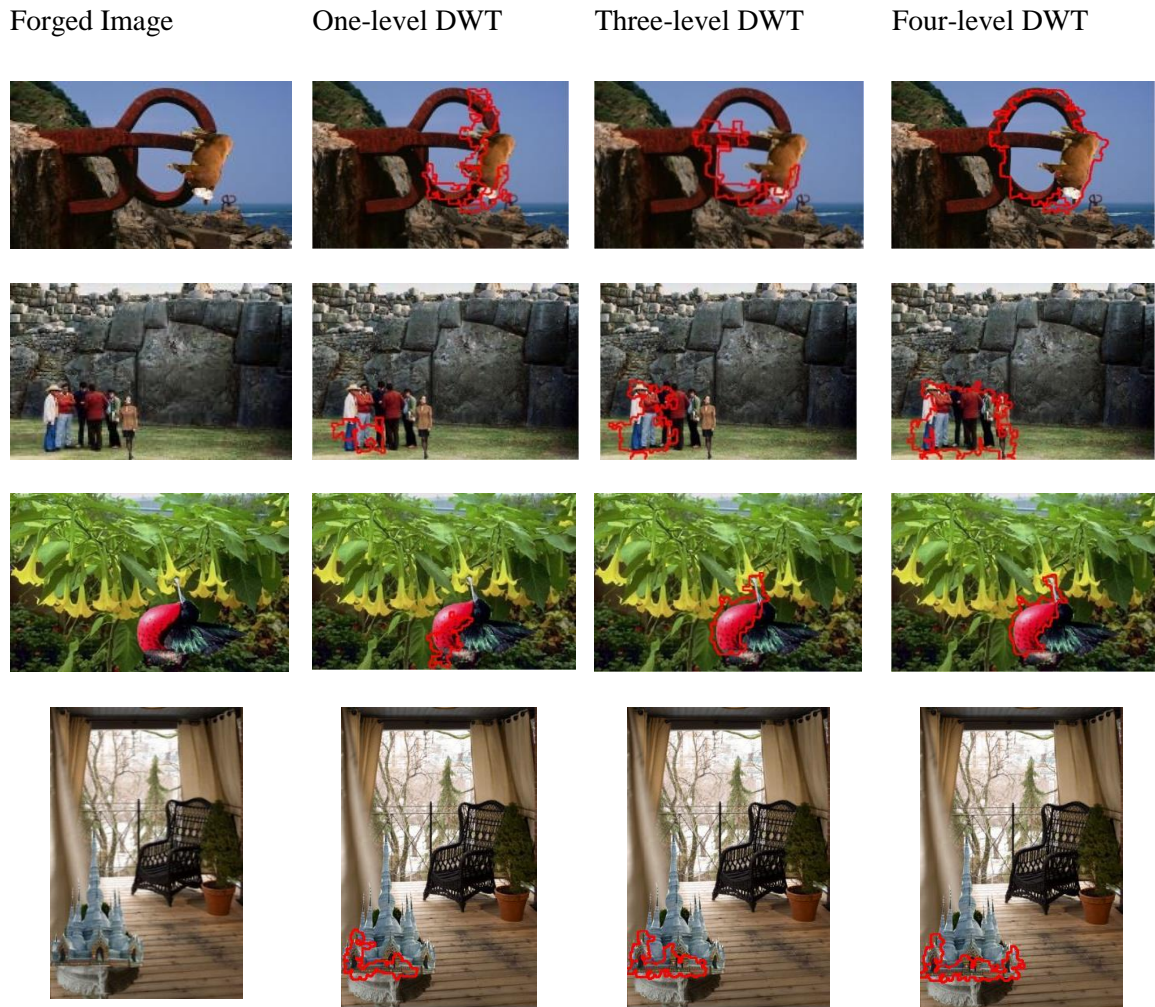


Figure 4.4: Some unsuccessful cases of tampered images

Figure 4.4 shows unsuccessful experimental results of tampered images from CASIA dataset. First column shows tampered images from CASIA database. Second column, third and last column are first, third and fourth level decomposition using discrete wavelet transform respectively. However for each level of decomposition the output obtained was not able to detect exact tampered region locations.

4.2.1 Different Steps of Proposed Algorithm

The output obtained at different steps of proposed algorithm has been shown and described below:

Example 1:

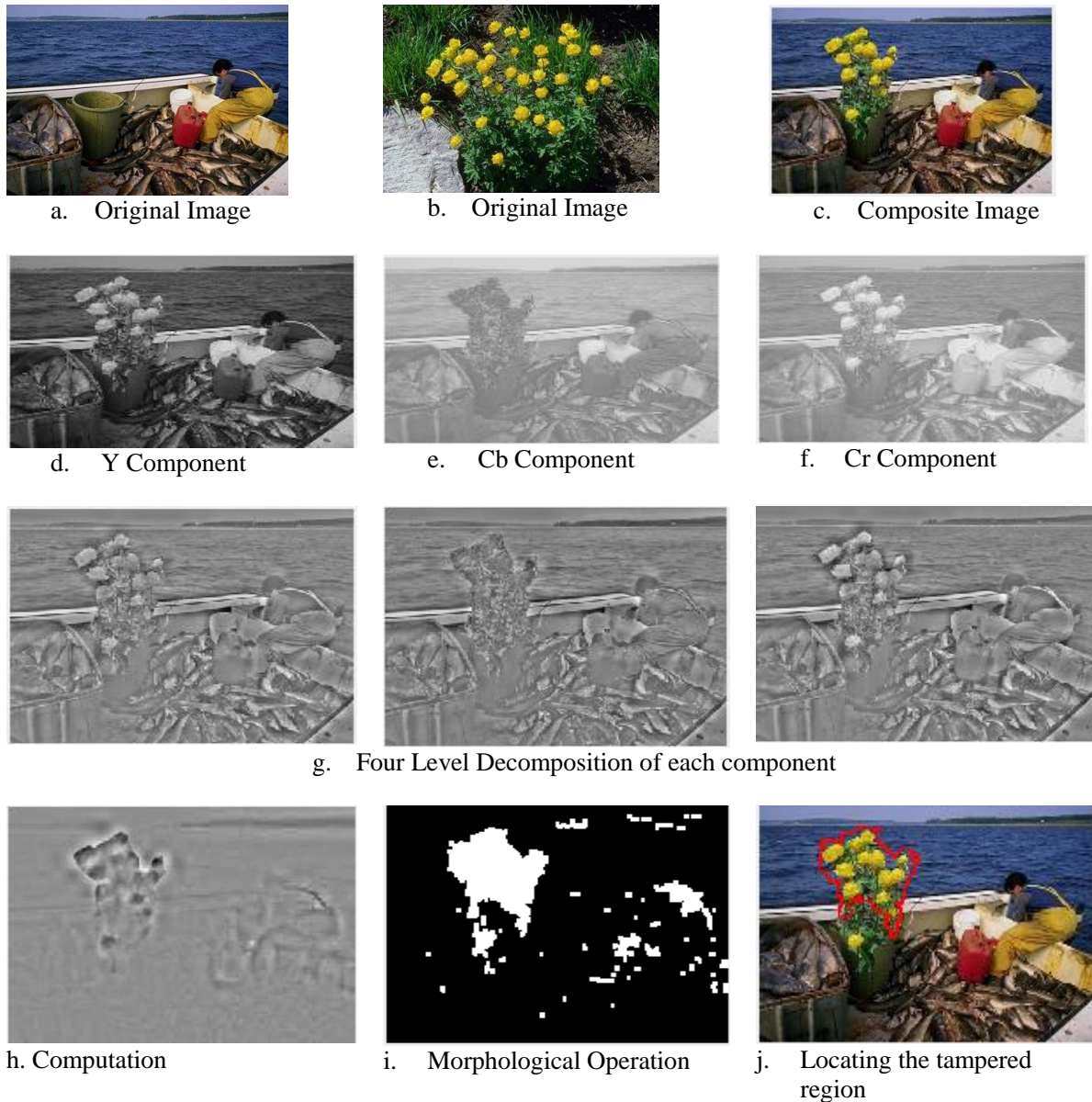


Figure 4.5: (a)-(c) Sample 1 Input Image (d)-(j) overall process of proposed method

In above figure, figure (a), (b) is the sample image of dimension 384×256 . Figure (c) shows composite image (figure a as base image and a portion of flower from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCBCR components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting portion of flower as a tampered region.

Example 2:

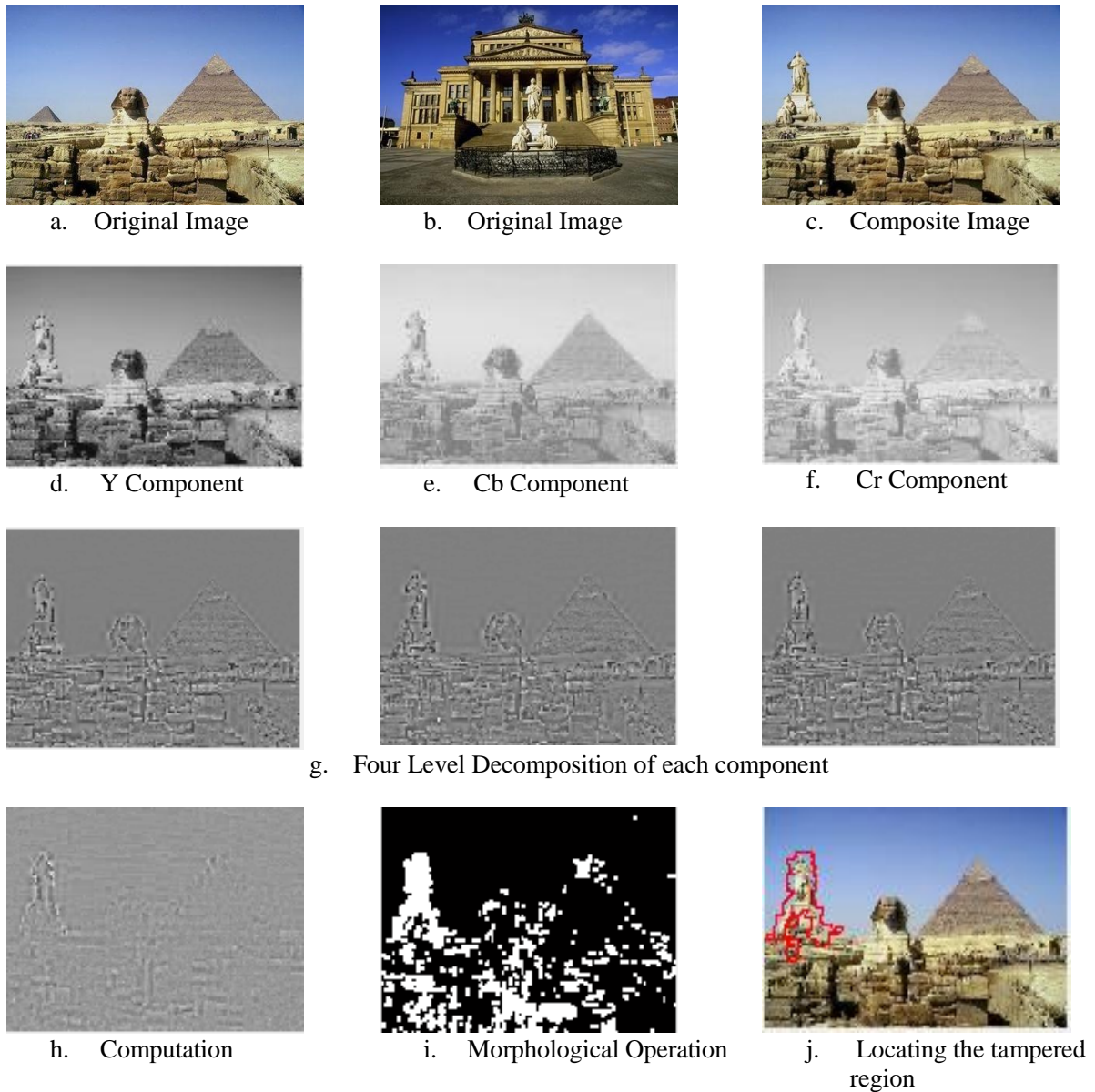


Figure 4.6: (a) -(c) Sample 2 Input Image (d)-(j) overall process of proposed method

In above figure, figure (a), (b) is the sample image of dimension 384×256 . Figure (c) shows composite image (figure a as base image and a statue from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCBCR components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting statue as a tampered region.

Example 3:

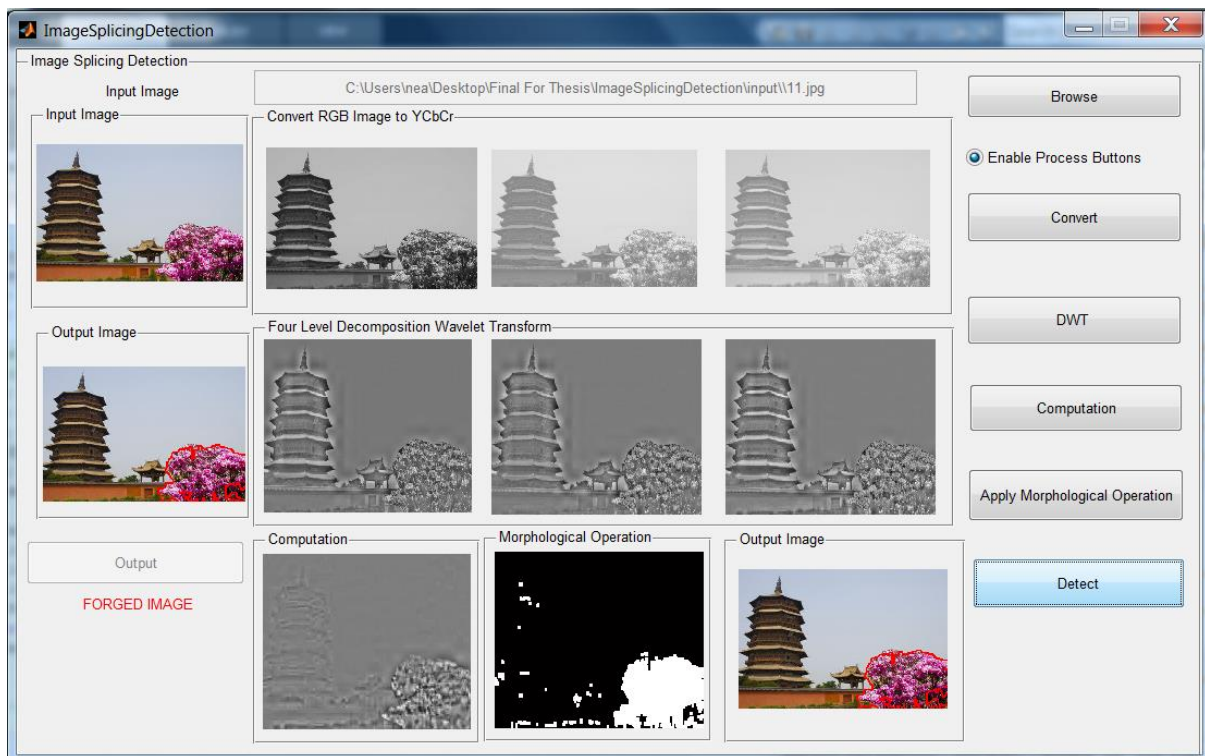


Figure 4.7: Sample GUI 1 of Tampered Image (forged portion: flower)

Example 4:

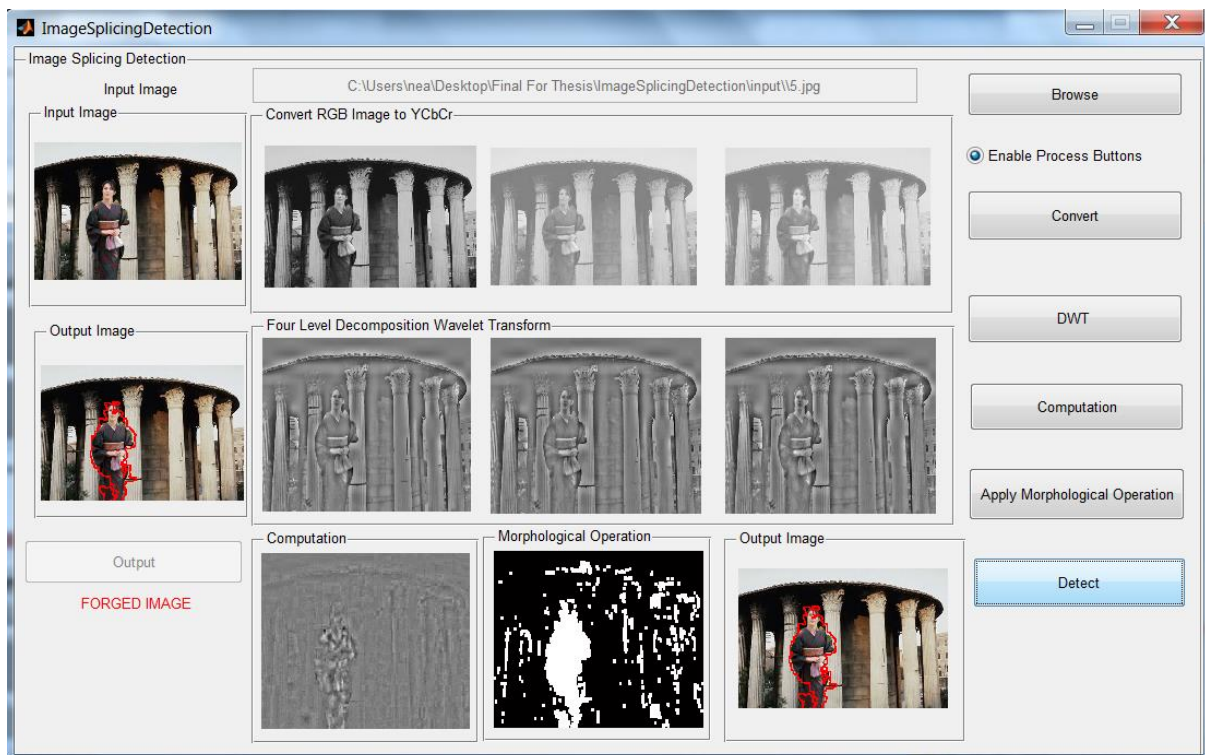


Figure 4.8: Sample GUI 2 of Tampered Image (forged portion: girl)

Example 5:

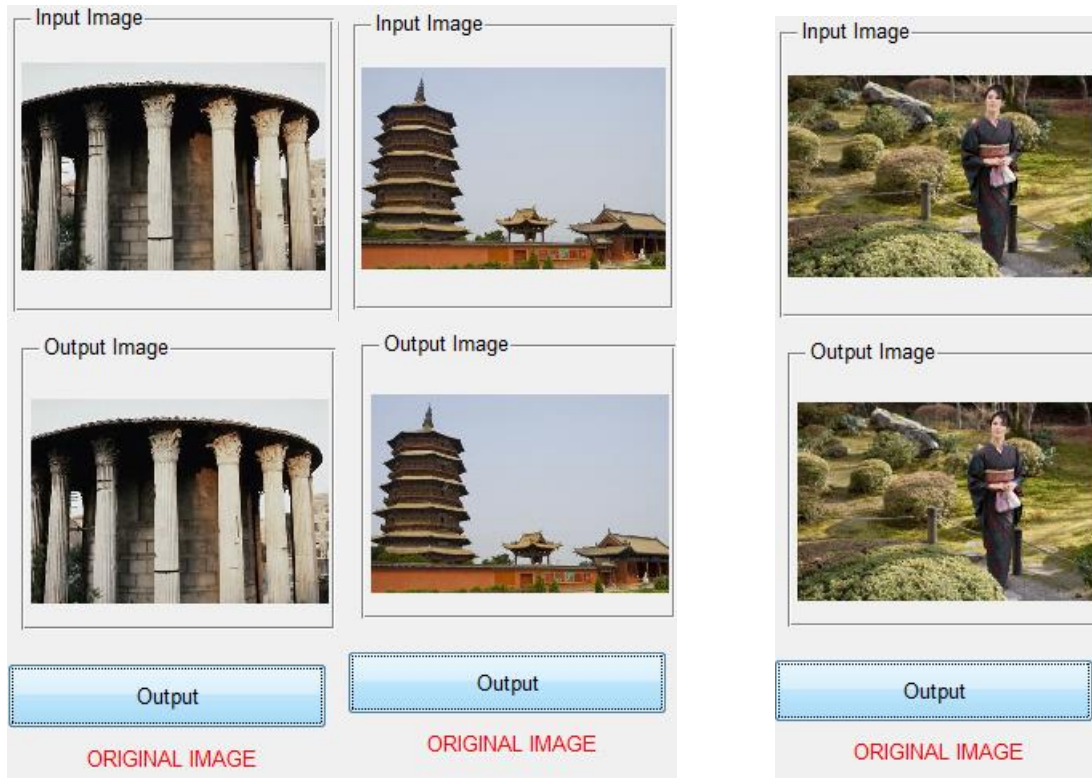


Figure 4.9: Experimental results of authentic images.

4.2.2. Performance Evaluation

Testing of the tamper detection algorithms is done on a database of images. The main objective of performance evaluation is to know how efficient the detection algorithm in detecting tampering is. Three parameters called precision (p), recall (r) and accuracy are used to evaluate the feasibility of the proposed method, which is defined in (i), (ii) and (iii). Sensitivity indicates, how well the test predicts forged images and Specificity measures how well the test predicts the original images. Whereas Accuracy is expected to measure how well the test predicts both categories

As a quality measure, the method used sensitivity, specificity and accuracy defined as:

$$\begin{aligned} \text{Sensitivity} &= \frac{TP}{TP+FN} & (i) \\ &= \text{Correctly Selected} / \text{Correctly Selected} + \text{Mistakenly Rejected} \end{aligned}$$

$$\begin{aligned} \text{Specificity} &= \frac{TN}{TN+FP} & (ii) \\ &= \text{Correctly Rejected} / \text{Correctly Rejected} + \text{Mistakenly Selected} \end{aligned}$$

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+Tp+TN} \quad (\text{iii})$$

$$= (\text{Correctly Selected} + \text{Correctly Rejected}) / (\text{Correctly Selected} + \text{Mistakenly Selected} + \text{Correctly Rejected} + \text{Mistakenly Rejected})$$

With TP = true positive rate; number of tampered images, which are classified as tampered, FP= false positive rate; number of authentic images, which are classified as tampered ones, TN= true negative rate; number of authentic images, which are classified as authentic; FN= false negative rate; number of tampered images, which are classified as authentic.

Table 5: Detection result on different level of wavelet transforms

Level	True Positive rate	False Positive rate	True negative Rate	False Negative rate	Sensitivity	Specificity	Accuracy
1	56	25	48	21	72.73%	65.75%	69.33%
2	66	19	48	17	79.52%	71.64%	76%
3	74	13	48	15	83.15%	78.69%	81.33%
4	84	8	48	10	89.36%	85.71%	88%

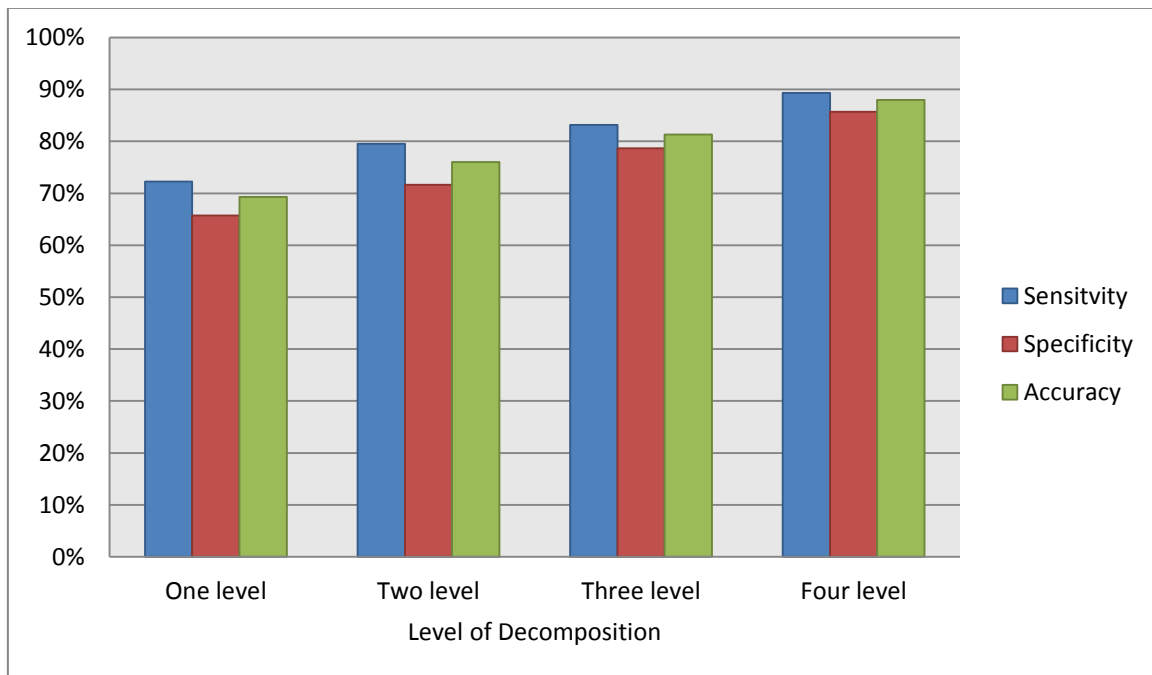


Figure 4.10: Detection result on different levels of wavelet transforms

These results show that using difference between luminance and chromatic component enhances the detection rate of image forgeries. As high frequency information, such as edges, becomes pronounced in chroma components of the tampered image and DWT further weakens the effect of low frequency variations i.e. image content and causes to discriminate the tampering.

CHAPTER 5
CONCLUSION

5. Conclusion

5.1 Conclusion

Image splicing forgery detection is a method to detect the manipulations in an image caused by copy-paste operation. This research has proposed a passive color image splicing detection method based on the analysis of image chroma component. Image splicing detection is the problem of weak signal (splicing introduced edges) detection in the background of strong signal (image content). In the process, the method removed image content and preserved the splicing introduced edges. Therefore, the method obtains edge image of chroma component, the problem has been changed to detection of signal in the background of weak signal which is an easier way to deal with.

In this thesis, the aim of the splicing detection is different from an edge detector. Instead of finding the entire boundary, only suspicious edge points due to splicing are labeled. These points may not be continuous. A counterfeit is firstly defined from the sharpness of the edges and boundaries presented by chroma components and high frequencies at the three sub-bands LH, HL and HH of four levels DWT decomposition which are traces of cutting and pasting. The output obtained from chroma components and luminance components decomposition is subtracted to remove stronger signal from the background of weak signal. When a fake portion is confirmed, suspicious regions becomes objects to be considered.

Finally, the experimental results have showed effectiveness of the proposed method. For this, sensitivity, specificity and accuracy are calculated for spliced images and analyzed the results. Our study indicates that the difference between chroma components and luminance components are better suited for image forgery detection than luminance or gray scale color channel. The method shows the consistency over CASIA datasets with sensitivity 89%, specificity 86% and accuracy 88%.

5.2 Recommendation

The method makes use of noise calculation feature to differentiate between original and forged image. This method can result in incorrect detection when two images with same noise are used. Further enhancement of this work can be done by experiment with large number of real data set. Different noise estimation features such as histogram analysis of selected region or mean or median calculations can be added to increase the accuracy of the method.
















REFERENCES

- [1] H. Farid, (2009). "Seeing is not believing" IEEE Spectrum.
- [2] O'Brien, J.F. and Farid H. (2012). "Exposing Photo Manipulation with Inconsistent Reflection"
- [3] H. Farid. "A Survey of image forgery detection." IEEE Signal Processing Magazine, vol. 26, pp. 16-25, 2009.
- [4] B. L. Shiva Kumar and Lt. Dr. Santhosh. "Detecting copy-move forgery in Digital images: A survey and analysis of current methods," Global Journal of Computer Science and Technology, vol. 10, no. 7, 2010.
- [5] Zhen zhang, Ying zhou, Jiquankang & Yaan ren. "Study of digital image splicing detection". <http://zhangzhen660126.com>, China.
- [6] Sheldon Sensenig, (2010). "Localizing Tampered Image Regions Through Image noise features".
- [7] Wei Wang, Jing Dong and Tieniu Tan, (2010). "Effective Image Splicing Detection Based on Image Chroma", International Conference on Image Processing.
- [8] Zhongwei He, Wei Lu, Wei Sun, Jiwu Huang (2012). "Digital image splicing detection based on Markov features in DCT and DWT domain, Pattern Recognition" 45(12), 4292-4299 (2012).
- [9] Y Zhang, Ch Zhao, Yiming Pi, Shenghong Li, Shilin W, (2013). "Image-Splicing Forgery Detection Based On Local Binary Patterns Of DCT Coefficients", Security And Communication Networks, Published Online In Wiley Online Library.
- [10] Zahra Moghaddasi, Hamid A. Jalab, RafidahMd Noor, and Saeed Aghabozorgi (2014) , "Improving RLRN image splicing detection with the Use of PCA and kernel PCA", The Scientific World Journal · September 2014
- [11] Archana V Mire, Dr. S. B. Dhok, Dr P. D. Porey , Dr N. J. Mistry, (2014). "Digital Forensic of JPEG Images", IEEE Fifth International Conference on Signals and Image Processing, Jeju Island, Korea, 8-10 Jan. 2014.
- [12] Mahdi Hariri, Fahime Hakimi and Farhad GharehBaghi, (2015). "Image splicing forgery detection using local binary pattern and discrete wavelet transform", IEEE 2015, 2nd International Conference on Knowledge-Based Engineering and Innovation.

- [13] Harpreet Kaur, Kamaljit Kaur (2015). "Image Forgery Detection Using Steerable Pyramid Transform and LAB Color Space", International Journal of Advanced Research in Computer Science and Software Engineering.
- [14] Upendra Ujjainiya, Shaila Chugh, (2016). "Digital Image Forgery Detection Based on Texture Feature and Clustering Techniques", International Journal of Computer Applications, vol. 147 – No.11.
- [15] Tu Huynh-Kha, Thuong Le-Tien, Synh Ha-Viet-Uyen, Khoa Huynh-Van, Marie Luong (2016). "A Robust Algorithm of Forgery Detection in Copy-Move and Spliced Images", (IJACSA) International Journal of Advanced Computer Science and Applications.
- [16] "CASIA Tampered Image Detection Evaluation Database (CASIA TIDE v1.0)"
Internet: <http://forensics.idealtest.org/casiav1/>.
- [17] "CASIA Tampered Image Detection Evaluation Database (CASIA TIDE v2.0) "
Internet: <http://forensics.idealtest.org/casiav2/>.

Appendix A

FigureA.1 below shows the process of image splicing that involves two images to create a composite image.

S.N	Base Image (Authentic)	Image from which crop portion is obtained (Authentic)	Composite Image (Forged)
1.			
2.			
3.			
4.			
5.			

6.



FigureA.1: A sample of creation of forged images

Figure A.1 shows creation of forged images using two different authentic images from CASIA dataset. Second column indicates the base authentic image, third column indicates authentic image from which a portion is cropped and pasted in base image and final column indicates composite image.

Appendix B

Dataset Test Image 1:

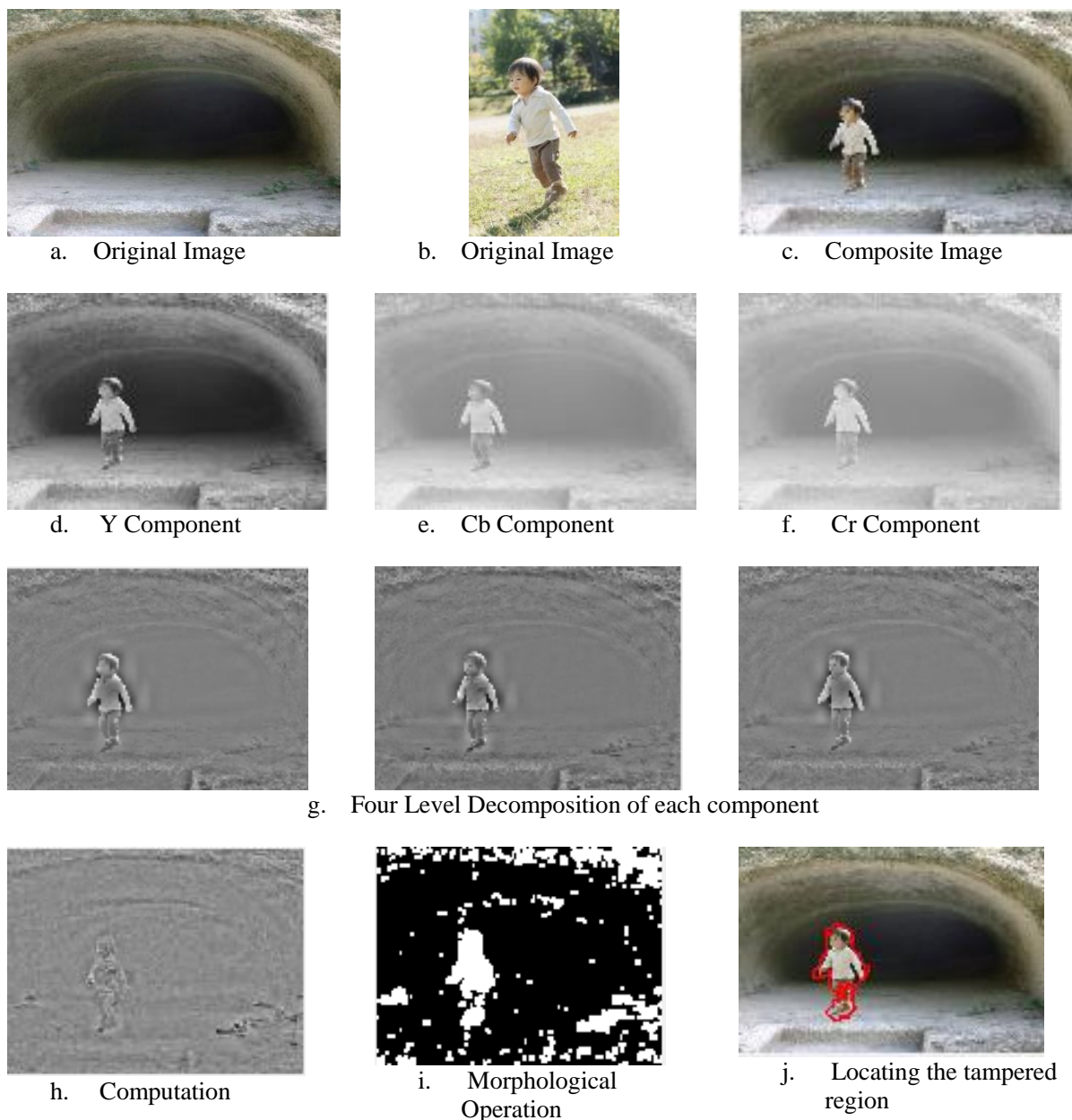


Figure B.1: Experimental result of Dataset Test Image 1

In above figure, figure (a) is the sample image of dimension 384×256 and figure (b) of dimension 256×384 . Figure (c) shows composite image (figure a as base image and a boy from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCBCR components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting boy as atamperedregion.

Dataset Test Image 2:

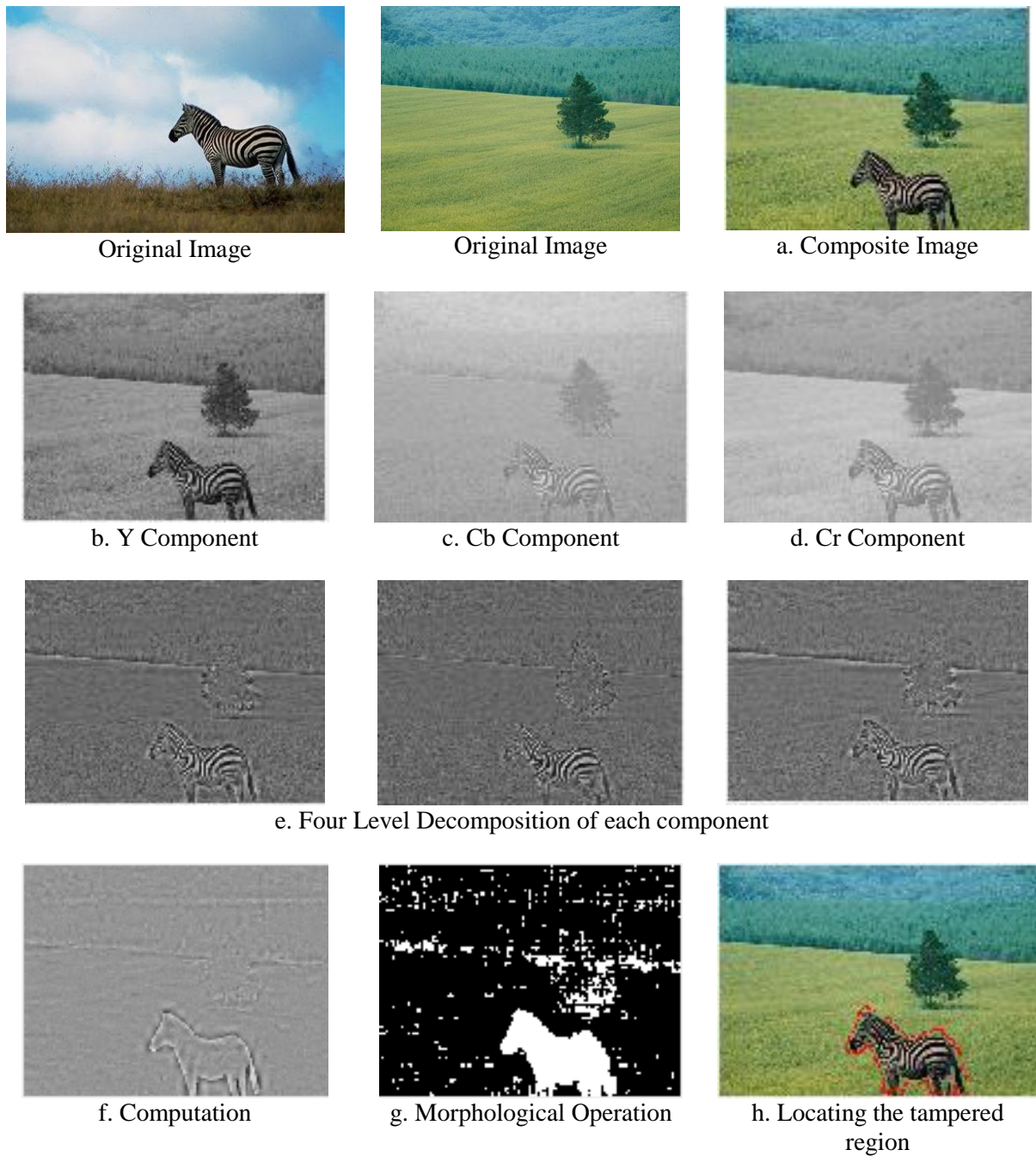


Figure B.2: Experimental result of Dataset Test Image 2

In above figure, figure (a),(b) is the sample image of dimension 384×256 . Figure (c) shows composite image (figure a as base image and a boy from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCbCr components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting boy as atamperedregion.

Dataset Test Image 3:

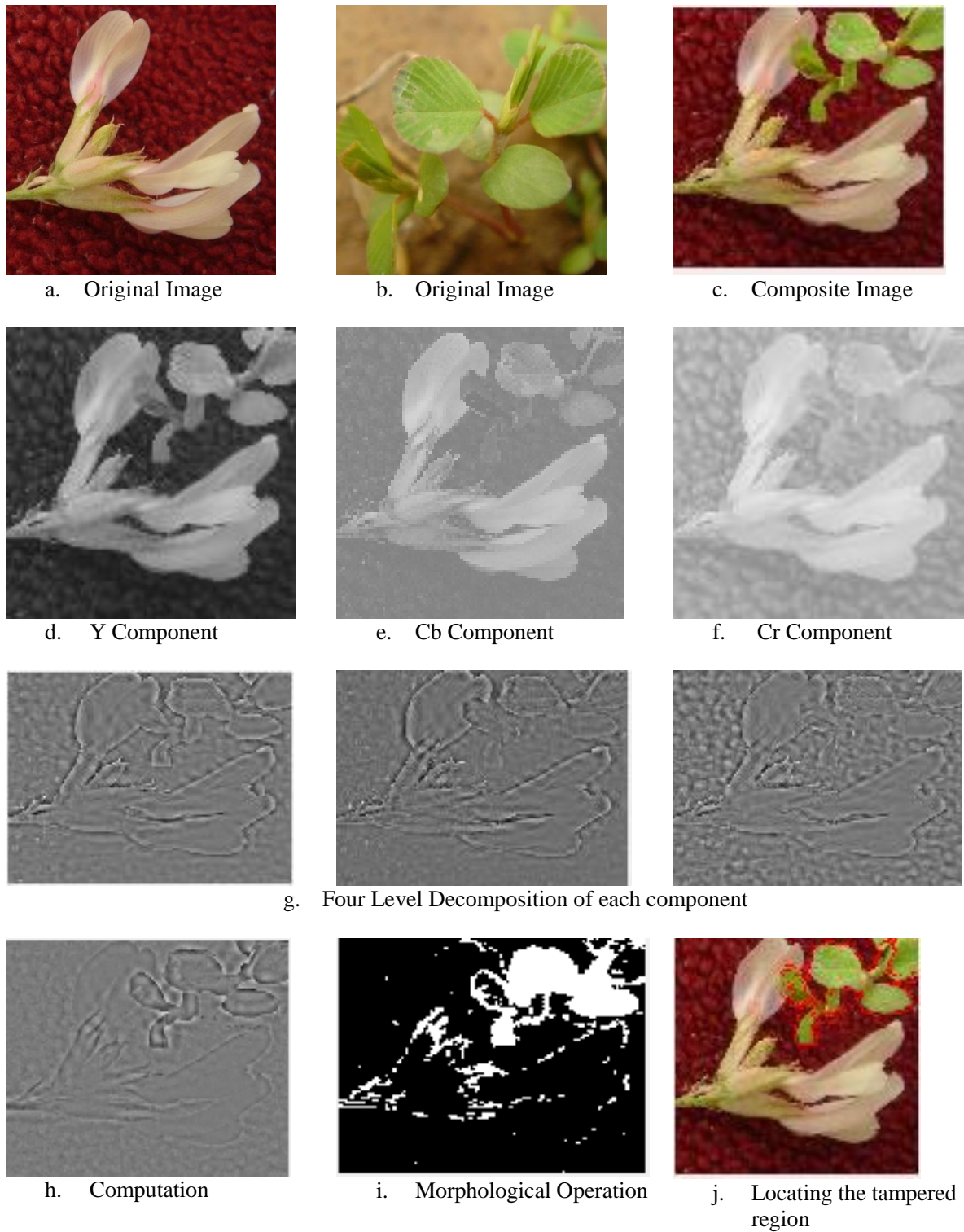


Figure B.3: Experimental result of Dataset Test Image 3

In above figure, figure (a) is the sample image of dimension 384×256 and figure (b) of dimension 500×500 . Figure (c) shows composite image (figure a as base image and leaf from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCBCR components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting leaf as a tampered region.

Dataset Test Image 4:

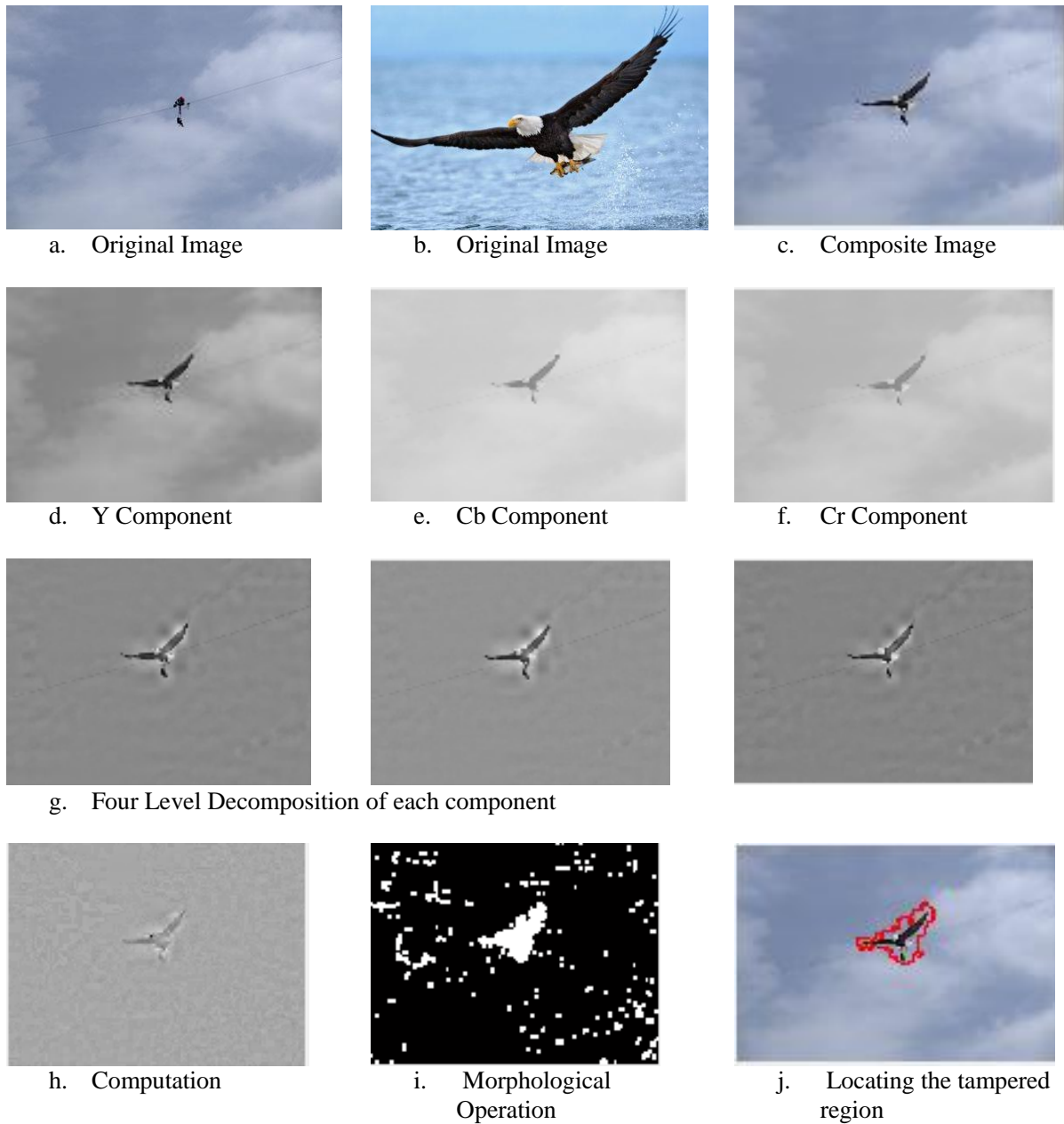


Figure B.4: Experimental result of Dataset Test Image 4

In above figure, figure (a), (b) is the sample image of dimension 384×256 . Figure (c) shows composite image (figure a as base image and a bird from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCBCR components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting bird as a tampered region.

Dataset Test Image 5:

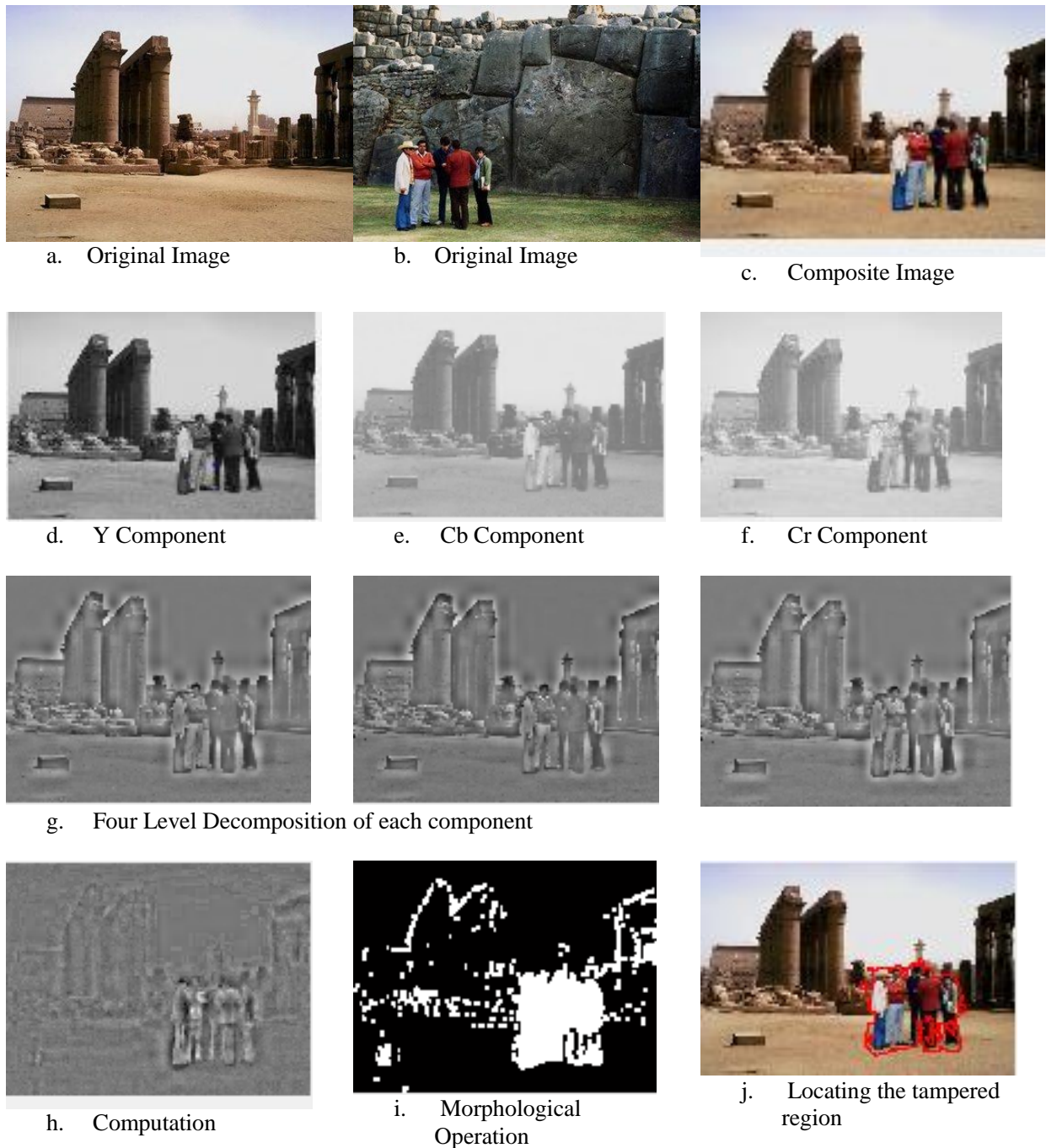


Figure B.5: Experimental result of Dataset Test Image 5

In above figure, figure (a), (b) is the sample image of dimension 384×256 . Figure (c) shows composite image (figure a as base image and group of people from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCBCR components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting group of people as a tampered region.

Example 6:

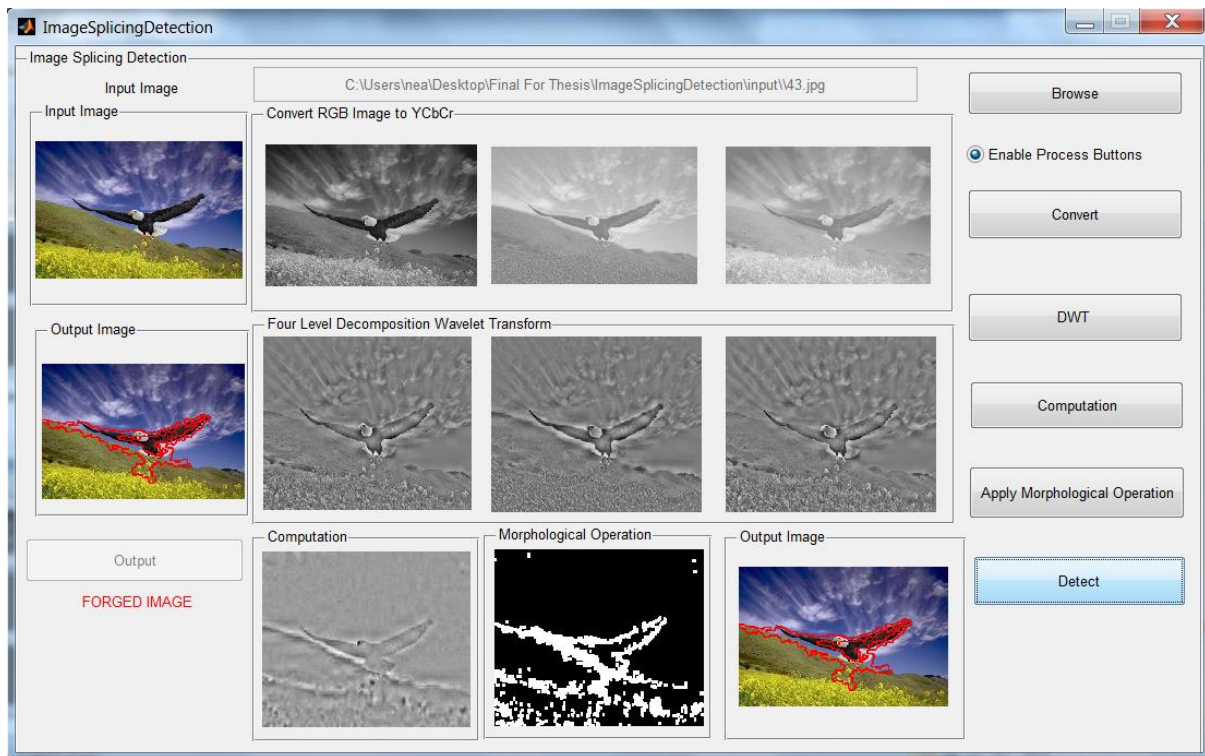


Figure B.6: Sample GUI 1 of Tampered Image (forged portion: bird)

Example 7:

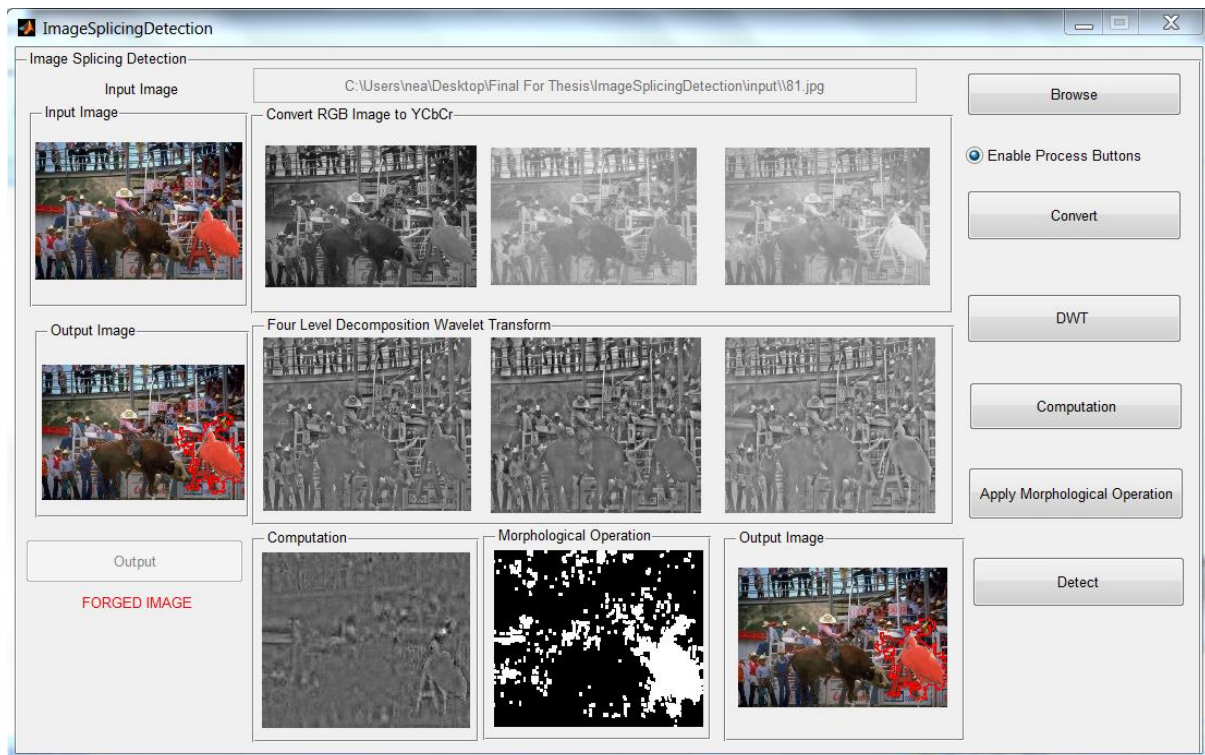


Figure B.7: Sample GUI 2 of Tampered Image (forged portion: bird)

Example 8:

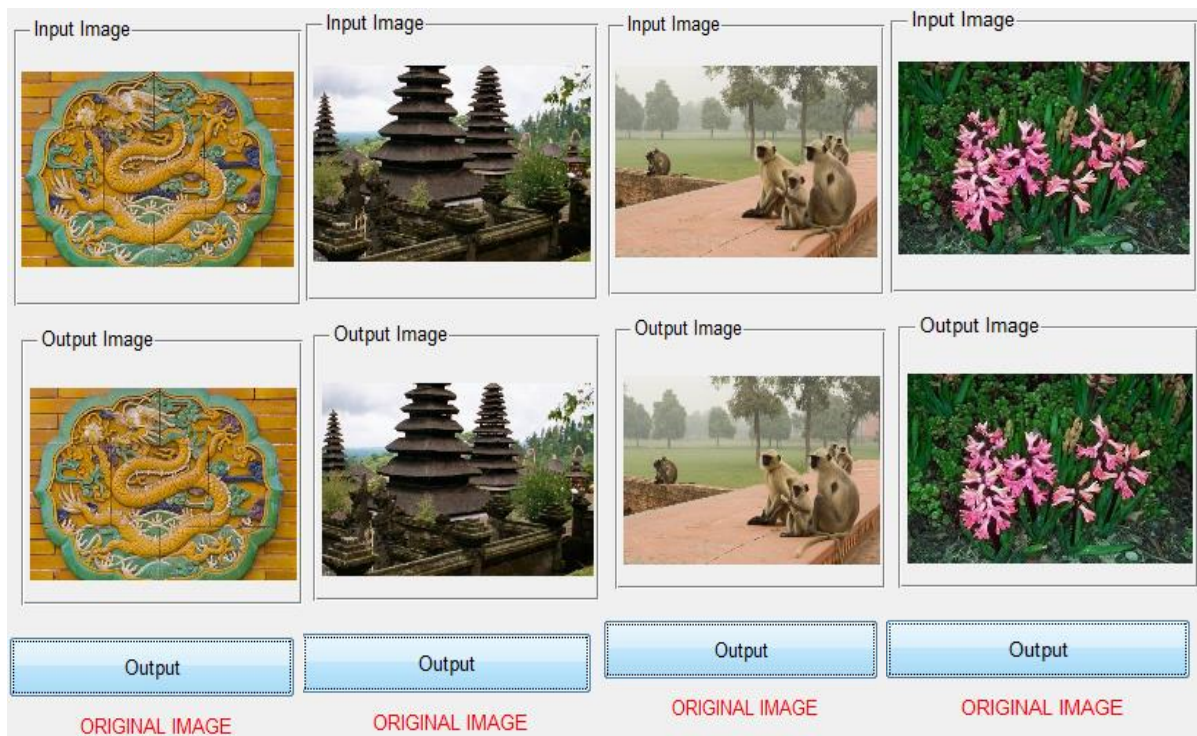


Figure B.8: Experimental results of authentic images.

Appendix C

After the multiple experiments with the simulated images, the real images were tested. These images are created using Adobe Photoshop

Real Test Image 1:

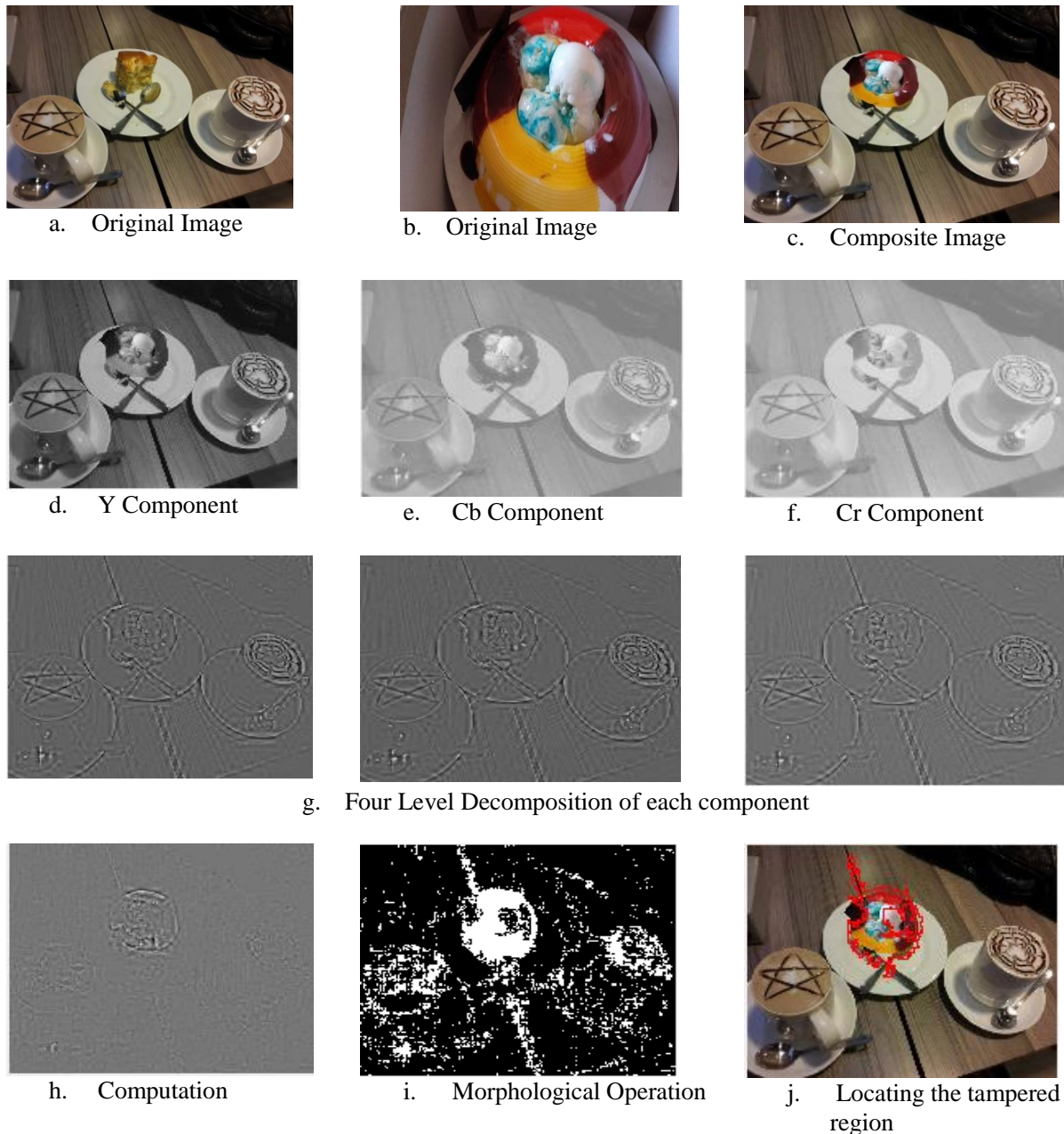


Figure C.1: Experimental result for Real Test Image 1

In above figure, figure (a) is the sample image of dimension 1024×768 and figure (b) of dimension 410×230 . Figure (c) shows composite image (figure a as base image and a cake from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCBCR components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting cake as a tampered region.

Real Test Image 2:

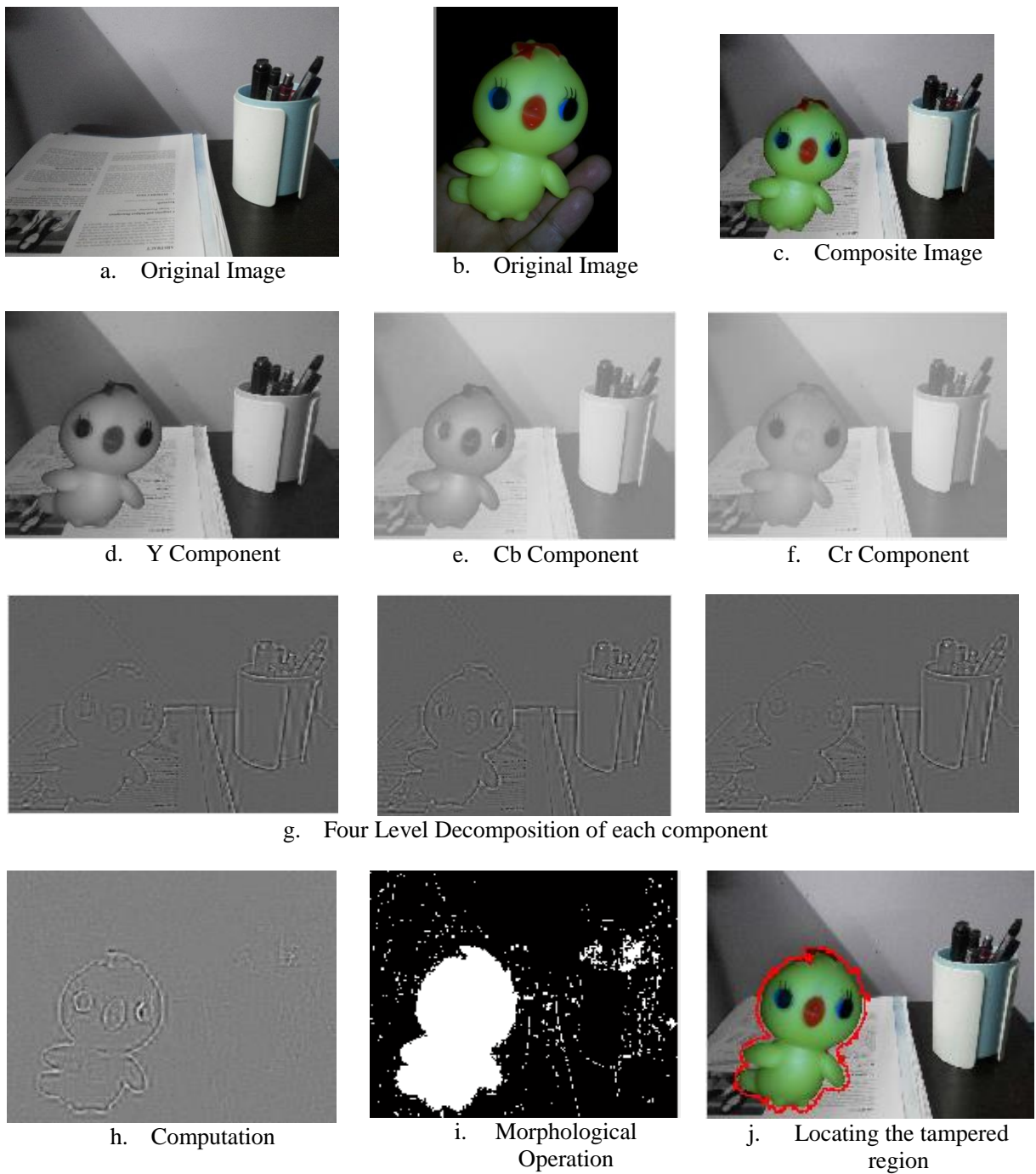


Figure C.2: Experimental result for Real Test Image 2

In above figure, figure (a) is the sample image of dimension 1024×768 and figure (b) of dimension 410×230 . Figure (c) shows composite image (figure a as base image and a duck from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCbCr components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting duck as a tampered region.

Real Test Image 3:



a. Original Image



b. Original Image



c. Composite Image



d. Y Component



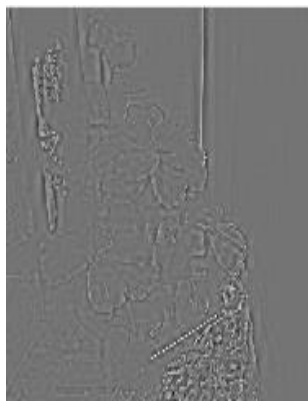
e. Cb Component

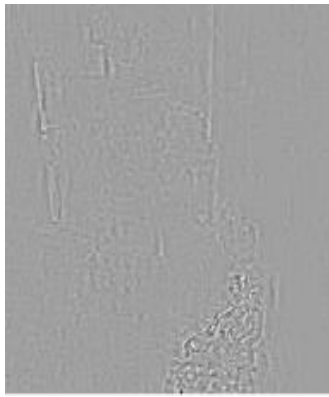


f. Cr Component



g. Four Level Decomposition of each component

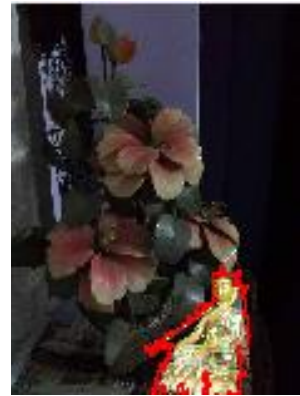




h. Computation



i. Morphological Operation



j. Locating the tampered region

Figure C.3: Experimental results for Real Test Image 3

In above figure, figure (a) is the sample image of dimension 768×1024 and figure (b) of dimension 768×1024 . Figure (c) shows composite image (figure a as base image and a Buddha from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCbCr components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting Buddha as a tampered region.

Real Test Image 4:

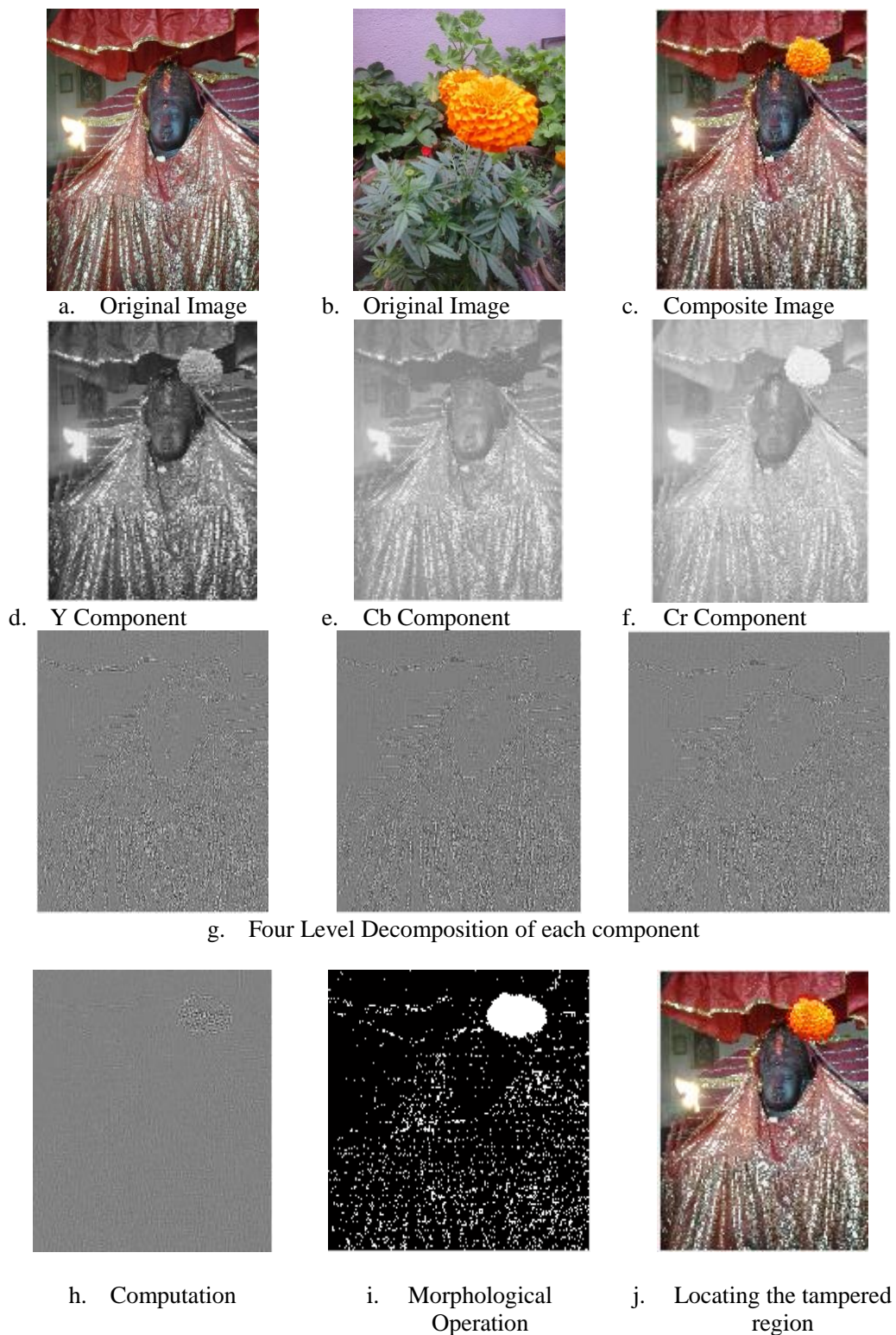


Figure C.4: Experimental results for Real Test Image 4

In above figure, figure (a) is the sample image of dimension 1536×2048 and figure (b) of dimension 768×1024 . Figure (c) shows composite image (figure a as base image and a flower from figure b). Figures (d), (e), (f) shows conversion to YCbCr components, (g) shows four level decomposition of YCbCr components (h) shows difference between chroma and luminance components, (i) shows morphological operation and (j) shows final output image detecting flower as atamperedregion.

Real Test Example 5:

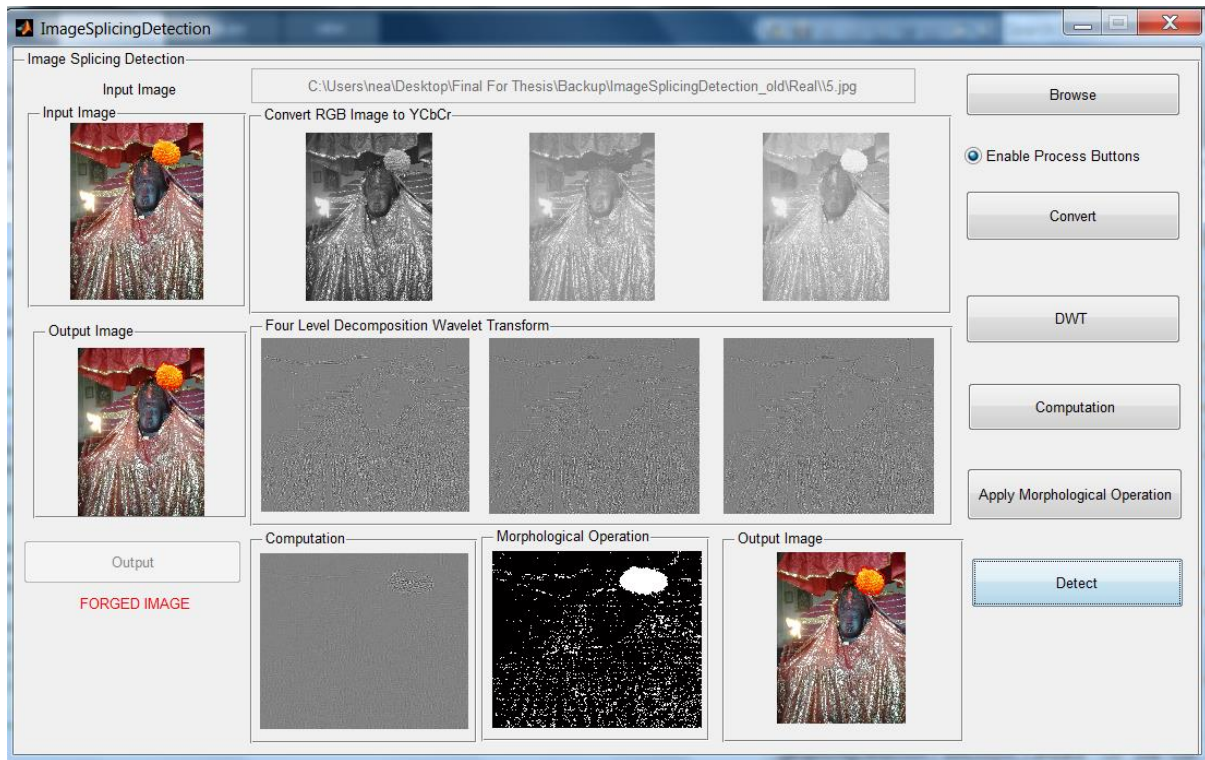


Figure C.5: Sample GUI results for Real Test Image 5

Real Test Example 6:

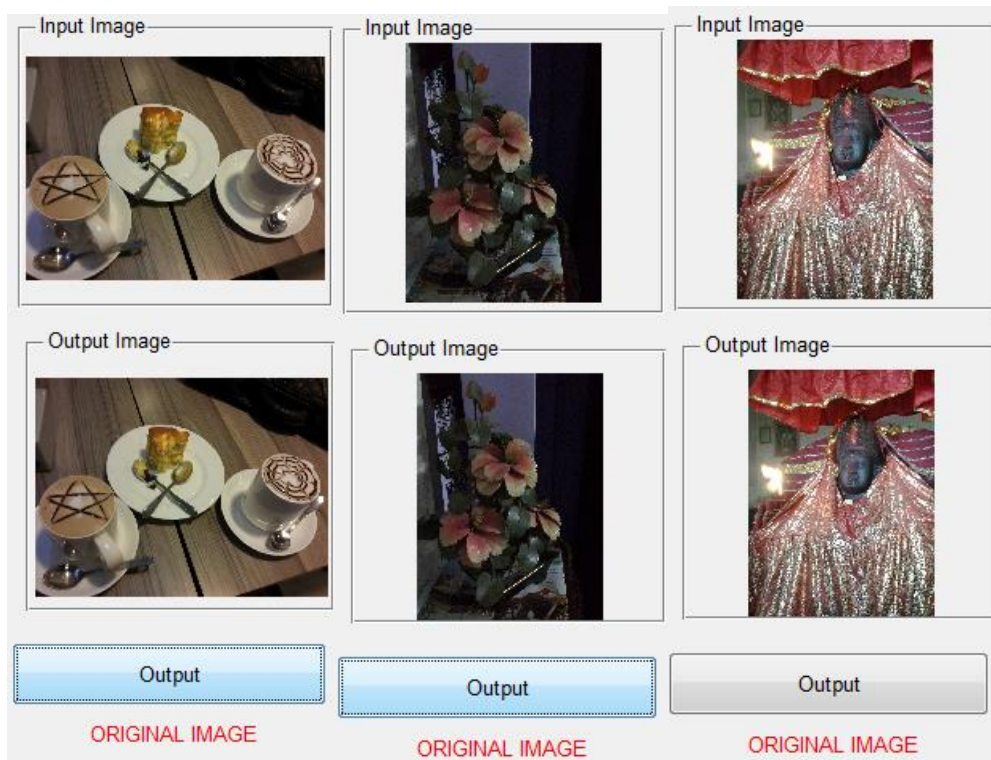


Figure C.6: Experimental results of real authentic images.