Detection of Image Forgery using LBP and DCT Techniques

Shalini D V[1], Dr. Suresh D S[2]
[1, 2] Department of ECE
[1, 2] CIT Gubbi, Tumakuru.

Abstract- *A digital image plays a very crucial role for an insurance claim, as illustrative information for a news item and as evidence in judiciary system. Nevertheless, the development of effective image editing tools that effortlessly change the image contents without leaving any visible indications of such alterations makes the genuineness of the digital image suffer from dangerous threats. This has led to demonstration and proposal of various methods to check that the digital images are genuine. To detect the digital image forgery, active methods require pre-embedding of a digital signature or watermark. Generally, all digital cameras can embed such watermark or signature and thus the need of passive methods that depend completely on the features of the digital image were required. There are various passive techniques that exist and meet these difficulties, but there are no satisfactory solutions so far.*

This paper proposes a passive technique for Image Forgery Detection system that is designed to detect the most common types of forgery like, splicing and copy-move. Image splicing is most common type of forgery, in which forgery is carried out through copying a small part from one base image and pasting to some other image. Whereas in copy-move forgery, copied part is pasted somewhere else in the same base image to either hide or add objects. The proposed system in this work is established on Local Binary Pattern (LBP) and Discrete Cosine Transform (DCT). Firstly, the chrominance component of original input image is divided up into overlapping blocks. After that, for each block, Local Binary Pattern (LBP) is computed and modified into frequency domain using 2 Dimensional Discrete Cosine Transform (DCT). At last, Standard Deviations are computed for frequency coefficients of all blocks respectively and hence used as the features. A Support Vector Machine (SVM) is utilized for classification. Experimental results of different benchmark image forgery databases demonstrate that the detection accuracy of proposed technique in this work is up to 89%. MATLAB R2014b tool is used to implement the proposed system.

I. INTRODUCTION

Images have acquired the fame of being explicit evidence. Image editing tools such as Photoshop, GIMP etc., are very popular, the indication of tampering on the digital images is highly challenging to reveal. Therefore, nowadays the digital images are losing their genuineness and are considering their genuineness for granted. It is getting challenging in electronic media, in legal cases, in financial institutions and in medical profession etc.,

By the introduction of digital technology, uses of the digital images have increased in our lifestyle; and hence, the tampering of the digital images has become easy and ascertainable. We live in an era, where anything can be falsified with aid of technology. Digital technology has begun to decay because of image forgeries and counterfeiting.

Digital image plays a very significant purpose in the fields like journalism, insurance processing and criminal investigation. In all these fields, the digital images are utilized as confirmative evidence or as authentication of some event. Sometimes, people in these professions attempt to forge the basic original image to regulate the result of the case. Nowadays, manipulating of digital image has become effortless and comfortable with the accessibility of sophisticated software and developing hardware. Thus, detection of such kind of manipulation signs is not only essential but also crucial.

The digital images forgeries are created by most common method called as Image Splicing. In Image Splicing method, image forgery is carried out through copying a small part from one base image and then, pasting it to some other image or pasting somewhere else in the same base image to either hide or add objects. Generally, some part of processing is carried out on the copied part either after (e.g. blurring and adding noise) or before (e.g. scaling and rotation) pasting, to eliminate irregularities those show image as tampered and to make editing less provable.

1. Existing System

There are various existing systems which use different kind of techniques to detect image forgery. From literature, it can be observed that these existing system use algorithms based on chain Markov and DCT (Discrete Cosine Transform).In chain Markov method features vector is

extracted from Markov stationary distribution of the chroma channel to represent the edge information, but accuracy level is lower with JPEG images on which compression QF is low.

2. Problem Statement

The primary problem in existing system is only one method is used to detect image forgery and that too the complexity is also high and few methods fail to detect images of JPEG type. And also, accuracy level is very low which is in turn computationally expensive. Apart from this existing system fail to detect if tampering occurred in compressed images.

1.3 Objective of Proposed system

In this work, an effort is made to detect forgery images, which accomplishes high accuracy as compared to previously proposed methods. In proposed system, techniques like, DCT and LBP are combined to achieve higher results and those results are compared by employing them separately. This proposed image forgery detection system aids the user as a way to check whether the image is original or tampered.

II. LITERATURE SURVEY

In 2004, Popescu and Farid [3] introduced a technique by usage of Principal Component Analysis (PCA) for representing image-segments i.e. overlapping of square blocks. Regular detection system accuracies were found to be 50%.

In 2010, QianruZheng, Wei Sun and Wei Lu [4] suggested a digitally spliced image detection technique established on the basis of edge blur assessment. Experiment depict that the suggested method was efficient and the categorization accuracy reached up to 62%.

In 2003, Fridrich et al [14] recommended a method to identify tampered images. The author suggested a method for detection of copy-move digital image forgery by usage of Discrete Cosine Transform (DCT) through overlapping of blocks and their lexico-graphical representation to evade the calculation burden. Balance of complexity and performance of system was found to be best by employing block matching algorithm.

III. IMAGE FORGERY DETECTION

In today's world, one can easily falsify a digital image by removing or adding some features within the image, which effects in very high numbers of image forgeries. With enhancing applications of the digital imaging, various kinds of soft wares' were brought in for the image processing.

Software like those could do change in the image by altering blocks of digital; image without depicting the consequence of the alteration in the image forgery. Alterations like those can't be observed by human naked eyes. Henceforth, confirmation of genuineness of images has become a difficult and challenging task. A digital image could be falsified with a broad diversity of manipulating methods such as scaling, cropping, blurring, rotation, filtering, resampling, etc. Detection technique of image forgery is essential in various fields for defending forgery and protecting copyright. The confirmation of genuineness of images is demanded in applications such as glamour, media, forensic, scientific, military, etc.

3.3 Types of Digital Image Forgery

There are various categories of digital image forgery. Each example falls into one of three major classes, depending upon the process employed in the image's creation. These classes consists of

1. Image Retouching
2. Image Splicing
3. Copy-Move

Image Retouching

Image Retouching is a potentially least-destructive and extremely common kind of digital modification. Rather than totally altering the subject of the photo, retouching is reduction or enhancement of certain characteristics in the image (Figure3.2).The most common exploiters of this technique are magazines and other photo heavy publications. By changing the images that are used in their articles or on their cover pages, such publications can make the contents of the photos seem more attractive and promote buyers to purchase the publication, ignoring the ethical problems of such an activity.

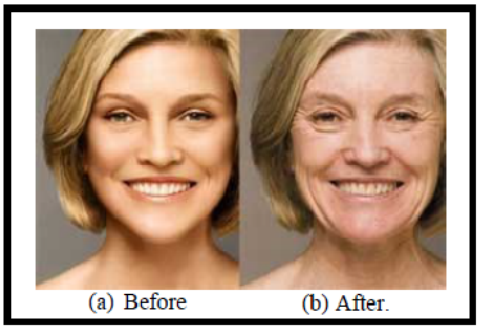

Figure 3.1: Example of Image Retouching Forgery

Image Splicing

Image Splicing is a kind of image forgery, which is much more aggressive technique than the retouching. It is nothing but creating totally new image through copying a component from one base image and then pasting to some other one.

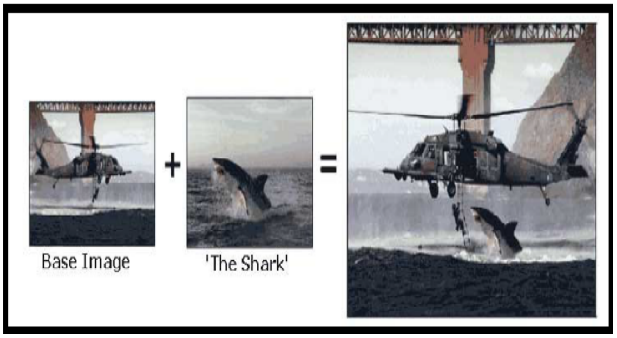

Figure 3.2: Exampleof Image splicing Forgery

In Figure 3.3, there is an introduction of a breaching Great White Shark into the basic image of the helicopter rescue operation. In addition to that, the basic image is rotated to make the image more credible, and surely more memorable and dramatic.

Copy-Move

Copy-move is a resemblance to the former category. Dissimilar to Image Splicing, a copy of an area of a digital image is pasted in the same image. The difference lies in employing the base image itself as both recipient and source of the copied component. The primary aim of copy-move forgery method is to either hide or add objects in a digital image. Blurring border of the pasted regions makes the editing less provable, elimination of abnormalities that could show the picture as tampered.

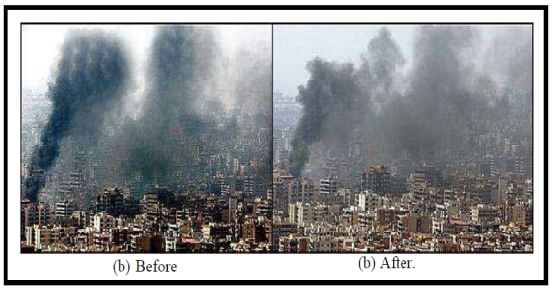

Figure 3.3:Example 1of Copy-Move Forgery

3.4 Approaches for image forgery Detection

Detection techniques for image forgery are categorized into two types -

1. Active Approach
2. Passive Approach

Active Approach

A digital image needs few preprocessing operations like signature generation or watermark embedding during creation of a digital image in a camera, which will restrict the use in practice. Furthermore, there are lakhs of digital images in cyber space without watermark or digital signature. In situation like these, active approach cannot be utilized to find out the genuineness of the image. More categories of active methods consists digital signature and data hiding techniques. The most commonly utilized form of data hiding is the use of digital watermarks. Data hiding refers to secondary data embedded inside the image data.

Digital watermarking comprises of entering the hidden data when the picture is taken, usually from the camera used, providing it to be detected and checked by a software. Watermarks are usually indivisible from the remaining data, that they are part of and alter along with an image. One main limitation of digital watermarks is that, the potentiality of placing watermark in an image must be present in the device, and it can only be entered with particular authorization. The insertion of a watermark can also reduce the quality of the image.

Digital signatures draw out some unique characteristics from the image and encode them into a new string of data, uniquely to that image. This data can then be utilized to find out the picture individually. This approach has similar drawbacks as watermarking.

Passive Approach

The image forensics functions in the lack of signature or watermark. These methods operate on the presumption that “though digital forgeries may leave no visual clues that indicate tampering, they may alter the underlying statistics of an image.”

The suggested system is established based on passive methods for forgery detection; it requires no earlier data about the original image. Passive detection methods focus on the particular are noticeable alterations that forgery techniques bring in to the tampered image. Visual means cannot detect alterations like these, particularly if a high-quality program changes the image.

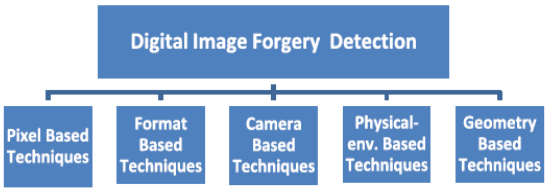

Figure 3.5: Digital Image Forgery Detection Techniques

Figure 3.5 shows the flow chart of classification of passive approach digital image for forgery detection techniques.

Pixel-Based Image Forgery Detection Techniques

Pixel-based techniques stress upon the number of pixels of an image. This technique is used to find statistical abnormalities inserted at the pixel stage. This method is evenly classified into four kinds as Resampling, Cloning, Splicing and Statistical.

Format Based Image Forgery Detection Techniques

This detection technique is established upon the digital image formats and operates primarily in the JPEG file format. Whenever the digital image is in compressed form, then it becomes highly challenging to detect image forgery, but this method can detect image forgery in a compressed form of image. This method can be categorized into 3 kinds namely, Double JPEG, JPEG Quantization, and JPEG Blocking.

Camera-Based Image Forgery Detection Techniques

When a digital image is taken from a digital camera, an image goes from digital camera sensors to the memory and then it experiences a sequence of processing stages which include color correlation, quantization, white balancing, gamma correction, JPEG compression and filtering. This sequence of processing stages from capturing to the saving the digital image in the memory may change depending upon the digital camera artifacts and model features. It uses artifacts inserted by camera sensor, lens or on-chip post–processing. This method can be categorized into 4 kinds namely, sensor noise, Chromatic Aberrations, Camera Response and Color filter Array.

Physical Environment-Based Image Forgery Detection Techniques

This technique unambiguously detects abnormalities in the 3-dimensional interaction of camera, physical objects, and light. Lighting is highly significant for action of capturing any image. This method operates on basis of available light present when an image is taken. This method is classified into three classes namely, Light Direction 3D Light Direction 2D and Light Environment.

Geometry-Based Image Forgery Detection Techniques

This method makes the assessment of objects in the whole world and their relative locations with respect to the camera. This method can be categorized into 2 groups namely, Metric Measurements and Principal Point.

This method can be categorized into 2 groups namely, Metric Measurements and Principal Point.

3.5 Advantages of Image Forgery Detection

1. Identification and authentication of images are possible.
2. Facts and evidences present in images can be revealed by forgery detection.
3. Copyrights of image can be protected.

IV. PROPOSED SYSTEM

This chapter presents the system design of the proposed Image Forgery Detection System. Image Forgery Detection System (IFDS) is a type of a Pattern Recognition System (PRS) that intent to allot one of pre-intended classes to an unknown input pattern (object). In IFDS, the pattern is an image. The classes are specified as authentic and tampered. The combination of LBP and DCT are used to detect forgery images. The design of the proposed system is shown in Figure 5.1.The crucial constituents of this system are-

1. Preprocessing
2. Feature extraction
3. Classification
4. Evaluation

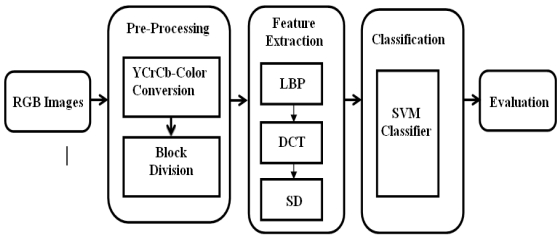

Figure 5.1: Design of the Proposed System

4.1 Preprocessing

Preprocessing is defined as the process of enforcing image enhancement methods either to separate patterns of

interest from the background or to decrease the noise in the data. In addition to that, it comprises the translation of the image between the other different color systems. Actually, this process is application dependent.

The tampering traces vary in different color model. Image forgery detection techniques are generally utilized gray scale and RGB color systems. In this stage, RGB color image is transformed to YCbCr, Cb components are extracted from YcbCrsince using chromatic channel instead of luminance or RGB enhanced the detection performance. YCbCr color model represents RGB colors in form of chrominance (Cb and Cr) and luminance (Y) components. Equation (3.1) defines the formula used for computing Y, Cb and Cr channels from different contributions of R, G and B channels.

$$\begin{pmatrix} y \\ cb \\ cr \end{pmatrix} = \begin{pmatrix} 0.299 & 0.587 & 0.177 \\ -0.299 & -0.587 & 0.866 \\ 0.701 & -0.587 & -0.114 \end{pmatrix} \begin{pmatrix} R \\ G \\ B \end{pmatrix} + \begin{pmatrix} 16 \\ 128 \\ 128 \end{pmatrix}$$

Y channel is the weighed sum of R, G and B and it holds the gray scale information and much more color content than the blue difference channel (Cb) and the red difference one (Cr).Human color vision comprehends the luminance component much better than the chrominance one.

Therefore, most of the tampering traces are hidden in the chromatic channel which cannot detected by naked eyes. Figure 5.2 shows Y,Cb and Cr component of an RGB image. The Cb components are distributed into 8x8 overlapping blocks and the processed block is fed to feature extraction step has input.

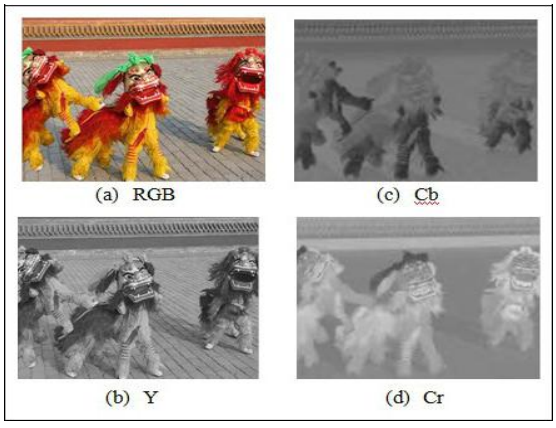

Figure 4.2: An RGB image and its YCbCr components.

4.2 Feature Extraction

Feature extraction is defined as the process of detecting a new representation of the data (image) in terms of features. The fundamental idea is to extract separate features that represent the data well. Reducing the dimensionality and avoiding redundancy of the data are two necessities for good features.

In this system Local Binary Pattern (LBP), DCT (Discrete Cosine Transform) and Standard Deviation(SD) is computed to every block and used as feature vector for further classification step. The last stage is to detect the changes, which artifacts make in the local frequency distribution of the LBP block. This can be carried out by transfer of LBP block into frequency domain using DCT and then use standard deviation to evaluate the frequency alters in each DCT coefficient. The resulted set of standard deviations is used as feature vector. The details of feature extraction step are depicted in figure 5.3.

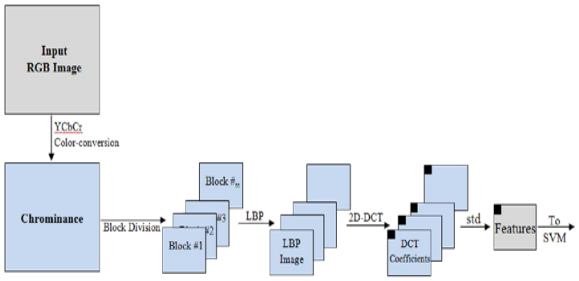

Figure 4.3: The details of feature extraction step.

4.2.1 Local Binary Pattern (LBP)

LBP is a local operator that separates different kinds of textures. The original LBP operator defines a LBP code (label) for each pixel of a digital image. To calculate the LBP code, a 3x3 vicinity of a pixel is set at threshold by its intensity value. If the neighbor's pixel value is less than that of the center, it will hold binary digit '0'; otherwise it will hold '1'. The neighbors' binary digits are concatenating to build a binary code. The LBP code is the decimal value of that binary code. Figure 5.3 shows the LBP code computation process. Later, the neighborhood size of LBP operator was expanded.

The LBP operator is defined as follows and denoted by

$$LBP_{P,R} = \sum_{i-1}^{P-1} S(P_i - P_C)\, 2^i$$

Where P is the neighborhood and R is radius and is the center pixel value, and the threshold formula is defined as follows

$$S(P_i - P_C) = \begin{cases} 1 & (P_i - P_C) \geq 0 \\ 0, & (P_i - P_C) < 0 \end{cases}$$

Whenever the manipulating is carried out, the basic master texture of a digital image is deformed. Because of the

capability of LBP to capture the texture deviations, it is a very effective tool for detection of image forgeries.

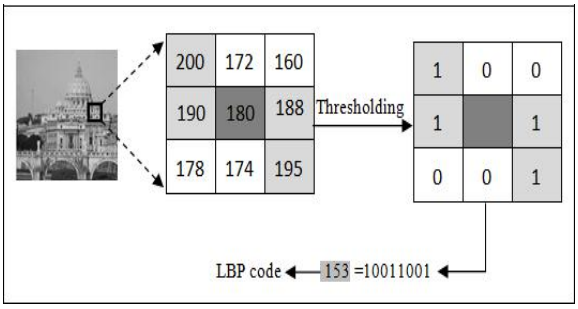

Figure 4.4: LBP code computation process.

4.2.2 Discrete Cosine Transform (DCT)

Discrete Cosine Transform (DCT) corresponds to a digital image as a sum total of cosine of various frequencies. It changes the digital image from spatial domain to frequency domain. The frequency domain renders a best representation, where in information is visually important than others. DCT consists of attribute that it focuses on information in only low frequency coefficients. Therefore, DCT often used in image compression such as JPEG.

DCT changes an array of coefficients of frequencies from an array of pixel values. The top-left side coefficient presents the low frequency coefficient information and called as DC, whereas, other coefficients provide the high frequency coefficient information (AC components). The bottom-right side coefficient presents the highest frequency.

4.3 Classification

Classification is nothing but the process of allotting an unknown data sample to one of the predetermined classes. A classifier is always modeled using data with known classes. This process comprises of two phases: testing phase and training phase. In training phase, the system is learning to find a mapping between the features extracted from the images in the training set and their classes. In the testing phase, the system employs the learned model and the features extracted from new images (i.e. testing set) to assign them to classes. Figure 6.3 shows Training and Testing Phases Classification.

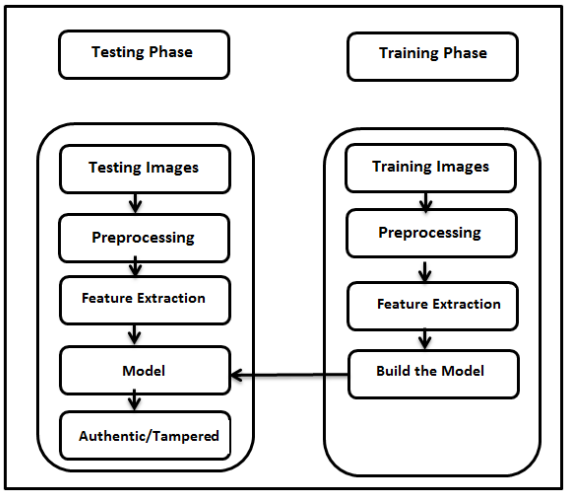

Figure 4.5: The Training and Testing Phases Classification

Since proposed system concentrates on feature extraction instead of design of the best classifier, the selection scheme for the classification algorithm is so depends upon the other existing works. SVM classifier is employed to classify the images and a RBF kernel is chose both training and testing is carried out in this phase. Ten- fold grid exploring is utilized to choose parameters for classifier.

4.3.1 Support Vector Machine Classifier (SVM)

Support Vector Machines are monitored learning models with related learning algorithms which analyze data utilized for classification. SVM's are established upon the main conception of decision planes which determine decision boundaries. A decision plane is nothing but a plane which distinguishes a set of objects having distinct class memberships.

Working of SVM Classifier finds out the decision boundaries in training phase and hence their methods could provide better generality in the high dimensional input spaces. The conception of decision planes those define decision boundaries that differentiates a set of objects having distinct class memberships, this concept is the crucial one as SVM classification is established based on this. Classification with SVM abides both multiclass and binary targets that search the vectors i.e. "support vectors" which selec-t the separators which provide the widest separation of classes.

4.4 Evaluation

In this work to keep the track of the performance during the validation of the classifier function is used. It creates and optionally updates the classifier performance object which accumulates the results of the classifier.

Accuracy measures the percentage of the images that are rightly classified by the classifier.

The accuracy of the classifier is evaluated using the below mentioned formulae:

$$\text{Accuracy} = \frac{\text{Correctly Classified Samples}}{\text{Classified Samples}} \times 100$$

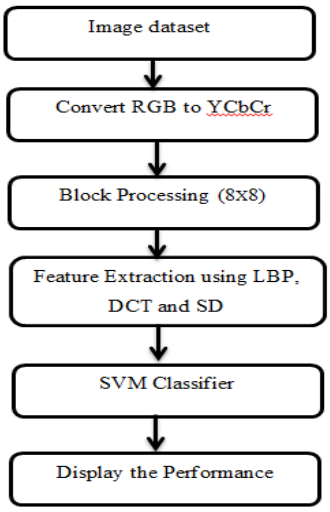

Figure 4.6: Flow Chart of Proposed System

V. IMPLEMENTATION DETAILS

This chapter presents the experimental settings and conditions, which are utilized to conduct the experiments. Also, it offers an overview of datasets namely, "CASIA Tampered Image Detection Evaluation Database Version 1.0 (CASIA TIDE v1.0)" and "CASIA Tampered Image Detection Evaluation Database Version 2.0."

5.1 System Details

The proposed system is developed using MATLAB R2014b programming tools on a PC with Windows 7 and the following details:

1. **Processor**: Intel(R) Core(TM) i3- CPU M380 @ 2.53 GHz 2.53 GHz
2. **Installed Memory (RAM):**3.00 GB(2.87GB usable)
3. **System Type:** 64-bit operating system

5 .2 Datasets Used

The proposed system in this project work is assessed using two benchmark datasets namely, CASIA Tampered Image Detection Evaluation Database Version 1.0 (CASIA TIDE v1.0) [17] and CASIA TIDE v2.0 [18] Detailed descriptions of these datasets are presented below.

CASIA Tampered Image Detection Evaluation Database Version 1.0

CASIA Tampered Image Detection Evaluation Database Version 1.0 (CASIA TIDE v1.0) was developed at the "Chinese Academy of Science" by their "Institute of Automation's National Laboratory of Pattern Recognition". In order to render a standard platform for researchers to compare and contrast the effectiveness of various image-tampering detection algorithms, it uses a dataset composed of natural color image detection evaluations and realistic tampering operations. Figure 6.1 shows examples of authentic images (1st row) and their forgeries (2nd row).

Brief description

The CASIA v1.0 database contains 1725 JPEG images that are 374 by 256 pixels each. These are separated into two groups, a tampered set and an authentic set. There are about 800 images that have not been forged, and 921 that have been tampered to some degree. Figure 5.1 shows examples of authentic and tampered images of this database.

Figure 5.1: Authentic images examples (row 1) and Forged Images (row 2)

Authentic images

Most of the authentic pictures were taken from the Corel image database, but some have been acquired through use of a digital camera. These images are further separated into the classes of Nature, Architecture, Animal, Article, Plant, Character, Scene, and Texture, depending on the subject of the image.

Tampered images

The authentic pictures form the basis for the forged images. All of them are versions of the authentic images, altered with a copy-and-paste attack in Adobe Photoshop CS3 v10.0.1 on the Windows XP operating system. The forged pictures can be products of copy-move (copying from the same image) or splicing (taking copied content from a different picture) operations.

The operations are carried out with one or more of these factors in mind:

1. There is no set boundary for the copy-pasted region. It can be polygonal or completely custom-designed by the forger.
2. Resizing, rotation, reshaping on a copied part of a picture can be used to generate a forged picture.
3. A variety of sizes can be used when copying and pasting the altered parts.

Dividing the Database

CASIA v1.0 database is divided into two main sets, authentic and tampered. Furthermore, we divided the tampered sets, 921images, according to the source of the copied region(s) into two subsets: Copy-Move (from the same image) and splicing (from another image).

Copy-Move Subset

Copy-move subset consists of 461 tampered digital images in which the copied region(s) are taken from same authentic image. Moreover, we divided this subset according to the type of operation employed on the tampered region shape and the copied region before pasting.

Type of operation

Mainly, there are three operations employed on the copied region(s) before pasting which are rotate, deform and resize. In different cases, either none of these operations is employed or a combination of two operations is employed. Consequently, there are 7 categories in this subset which are specified in Table 6.1.

Table 6.1: Categories obtained by dividing a copy-move dataset based on the type of operation.

Category name	**Operation**	**No. of images**
C_Rotate	Rotation	7
D_Deform	Deform	12
R_Resize	Resize	23
CD	Rotation and Deform	1
CR	Rotation and Resize	8
RD	Resize and Deform	5
N_Nothing	-	405
Total	**461**	

Tampered Region Shape

The four tampered region shapes of the copied part(s) are circular, rectangular, triangular and arbitrary. As a result, this subset has 4 categories which are clarified in Table 6.2.

Table 6.2: Categories obtained by dividing a copy-move dataset based on the region shape of the copied part(s).

Category name	**Region Shape**	**No. of images**
A_Arbitrary	Arbitrary	110
C_ Circular	Circular	102
R_ Rectangular	Rectangular	148
T_Triangular	Triangular	101
Total	**461**	

Splicing Subset

Splicing subset consists of 460 tampered images where the copied region(s) are taken from different images. We divided this subset according to the type of operation employed on the region where it is copied prior to pasting and tampered region shape.

Type of operation

As in copy-move subset, there are three operations employed upon the copied region(s) prior to pasting which are rotate, deform and resize. In different cases, either none of these operations is employed or a combination of 2 operations is employed. Consequently, there are 7 categories in this subset which are specified in Table 6.3.

Tampered region shape

There are four tampered region shapes of the copied part(s) which are circular, rectangular, triangular and arbitrary. As a result, this subset has 4 categories which are clarified in Table 6.4.

Table 6.3: Categories obtained by dividing a splicing dataset based on the type of Operation

Category Name	Operation	No. of images
C_Rotate	Rotation	18
D_Deform	Deform	41
R_Resize	Resize	182
CD	Rotation and Deform	2
CR	Rotation and Resize	37
RD	Resize and Deform	23
N_Nothing	-	157
Total		**460**

Table 6.4: Categories obtained by dividing a splicing dataset based on the region shape of the copied part(s).

Category name	Region Shape	No. of images
A_Arbitrary	Arbitrary	426
C_ Circular	Circular	12
R_ Rectangular	Rectangular	21
T_Triangular	Triangular	1
Total		**460**

"CASIA Tampered Image Detection Evaluation Database Version 2.0"

"CASIA Tampered Image Detection Evaluation Database Version 2.0 (CASIA TIDE v2.0)" was also developed at the "Chinese Academy of Science" by their "Institute of Automation's National Laboratory of Pattern Recognition".

Brief Description

When comparing "CASIA TIDE v2.0" to V1.0, it has larger size, more naturalistic and challenging tampered images. It uses post-processing around tampered regions. It consists of 12,323 color images. 7,491 of the images are authentic and 5,123 of them are tampered. The digital images have various sizes that vary from 240×160 to 900×600 pixels. Unlike V1.0, that contains only JPEG format, V2.0 contains samples of uncompressed images in addition to different Q factors JPEG images. Authentic images are categorized into different categories as in V1.0, but with one additional "indoor" category to consider the image illumination impact. Figure 6.2 shows examples of authentic images (row 1) and their forgeries (row 2).

Figure 5.2: Authentic images (row 1) and Forgery counter parts (row 2).

VI. EXPERIMENTAL RESULTS

This chapter discusses about the test results and performance of the proposed Image Forgery Detection System using the benchmark databases: "CASIA Tampered Image Detection Evaluation Database Version 1.0 (CASIA TIDE v1.0)." and "CASIA Tampered Image Detection Evaluation Database Version 2.0 (CASIA TIDE v2.0)."

In pre-processing method, RGB image (Figure 7.1) is converted to YCbCr components (Figure 7.2).The detection of forgery is easy from YCbCr color model compared to RGB color model therefore, conversion process is carried out. Human color vision comprehends the luminance component much better than the chrominance one. Consequently, most of the manipulating indications, which could not detected by human naked eyes, are hid in the chromatic channel. And thus, chromatic channels are utilized for further processing. In this work chrominance component Cb is used, which undergoes block processing (8x8).

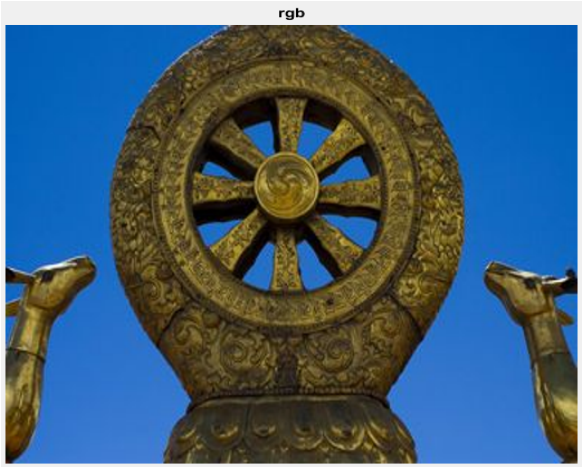

Figure 7.1: Input RGB image

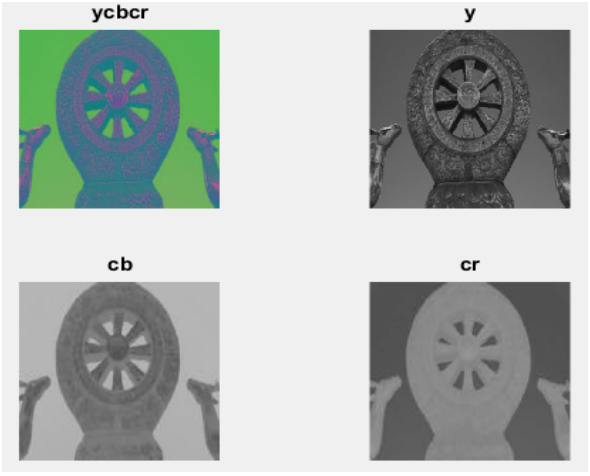

Figure7.2: RGB toYCbCr converted image

The proposed system performance on CASIA 1 and CASIA 2 datasets is shown in above Figure 7.3 and Figure 7.4 with accuracy of 89.57% and 84.93% is obtained respectively. After block processing by using Cb component, LBP and DCT technique is applied and Standard Deviation is computed which is used as feature vector. The obtained feature vectors of image dataset are provided to SVM classifier which classifies authentic and tampered images. Finally, accuracy performance is evaluated.

VII. CONCLUSION AND FUTURE SCOPE

This chapter explains Conclusion and Future Scope of the dissertation work.

7.1 CONCLUSION

In this project work, Image Forgery Detection technique established upon LBP and DCT is proposed. The image chromatic component is firstly separated as overlapping blocks and then, LBP code for each block is translated into DCT domain. And then, Standard deviations of DCT coefficients of all the blocks are calculated and are then used as features. A SVM classifier is utilized for classification. The proposed technique shows its consistency over "CASIA TIDE v1.0" and "CASIA TIDE v2.0" datasets with accuracies 89.57 and 84.93respectively. The results obtained are significantly greater than that of other recent methods. The proposed technique has addressed the current issue successfully. And also, it is considerably faster than the existing systems. It has detected image forgery with best success rate in the digital image dataset. Result of the system reveals its effectiveness and robustness, and can be applied in systems which are aimed for detection of forged images.

7.2 FUTURE SCOPE

The present work can be extended to investigate in comparing of different color spaces in Digital Image Forgery Detection.

In future more than one feature could be selected and detection performance of the proposed system can be increased.

REFERENCES

[1] H. Farid. "A Survey of image forgery detection." IEEE Signal Processing Magazine, vol. 26, pp. 16-25, 2009

[2] B. Mahdian and S. Saic. "A bibliography on blind methods for identifying image forgery," Signal

Processing: Image Communication, vol. 25, no. 6, pp. 389 - 399, July 2010.

[3] Popescu A, Farid H. “Exposing digital forgeries by detecting duplicated image regions.” Technical Report TR2004-515.Department of Computer Science, Dartmouth College; 2004.

[4] QianruZheng, Wei Sun and Wei Lu “Digital Spliced Image Forensics based on Edge Blur Measurement” IEEE International Conference on, 2010.

[5] S. Bayram, H. T. Sencar, and N. Memon, "An efficient and robust method for detecting copy-move forgery," in Acoustics, Speech and Signal Processing, 2009.ICASSP 2009. IEEE International Conference on, 2009, pp. 1053-1056.

[6] H. Ling, H. Cheng, Q. Ma, F. Zou, and W. Yan."Efficient Image Copy Detection Using Multiscale Fingerprints," IEEE MultiMedia, vol. 19, pp. 60-69, 2012.

[7] B. Xu, J. Wang, G. Liu, and Y. Dai, "Image Copy-Move Forgery Detection Based on SURF," in Multimedia Information Networking and Security (MINES), 2010 International Conference on, 2010, pp. 889-892.

[8] Micah K. Johnson and HanyFarid “Exposing Digital Forgeries in Complex Lighting Environments” IEEE transactions on information forensics and security, vol. 2, no. 3, September 2007.

[9] Y. Cao, T. Gao, L. Fan, and Q. Yang. "A robust detection algorithm for copy-move forgery in digital images," Forensic Science International, vol. 214, pp. 33-43, 2012.

[10] W. Wei, S. Wang, X. Zhang, and Z. Tang, "Estimation of image rotation angle using interpolation-related spectral signatures with application to blind detection of image forgery," Information Forensics and Security, IEEE Transactions on, vol. 5, pp. 507-517, 2010

[11] Lukas J, Fridrich J, Goljan M, "Detecting digital image forgeries using sensor pattern noise". Proc of Security, Steganography, and Watermarking of Multimedia Contents VIII, part of EI SPIE 2006. San Jose, CA, USA

[12] L. Weiqi, H. Jiwu, and Q. Guoping, "Robust Detection of Region-Duplication Forgery in Digital Image," in Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, 2006, pp. 746-749.