RESEARCH ARTICLE

Identifying Image Falsification by Enhanced Auto Colour Correlation Approach – A Forgery Forensic

*Venkata Reddy Medikonda[1], Vignesh Janarthanan[2]

[1]Associate Professor, Department of Computer Science and Engineering, Sreyas Institute of Engineering and Technology, Bandlaguda, Hyderabad, India.

[2]Professor, Department of Computer Science and Engineering, Sreyas Institute of Engineering and Technology, Bandlaguda, Hyderabad, India.

Received- 28 February 2017, Revised- 6 April 2017, Accepted- 20 May 2017, Published- 22 June 2017

ABSTRACT

As images are increasingly being used today as evidences for criminal justification, the forgery on the images that are used for criminal investigations can cause a great threat in the implementation of truth and justice. The innovations in digitizing technology along with image editing software have made it very easy to tamper digital images. So, there is a need for examining the authenticity of the images. Digital image forensics has emerged to solve the problems behind this conflicting issue. In this work, the test images are pre-processed by means of blur-index calculation and false colour removal with the help of nearest neighbour algorithm. Next the colour feature extraction process is carried out. This is done by generating the histogram of the image, and feeding it as input to the Colour Index Local Auto-Correlations (CILAC) model, to extract the colour index. This facilitates the enhanced Auto Colour Correlation (ACC) approach. Next the image undergoes 8Z affine transformation and the images are matched to obtain the result. Finally, a comparison of the results obtained with the other existing methods is done which reveals that the ACC enhanced approach has a better performance in terms of precision, recall and F1 score.

Keywords: Blur-index calculation, False colour removal, CILAC, Enhanced ACC, 8Z Affine Transformation.

1. INTRODUCTION

It was from the very olden years the technology of photography was used for the process of creating portraits. The photographers who framed the portraits rapidly turned into the picked strategy of altering their photos by performing retouching processes on their portraits to satisfy the sitter which could in turn enhance the sales of their portraits. The action of image forgery was evidenced in the 1840s itself. “Self Portrait of a Drowned Man”, framed by a person named, Hippolyte Bayradis was the primordial fake image in which he was seen as committing suicide. The other person whose image was forged was Abraham Lincoln [1]. In this image his head was superimposed on John Calhoun’s head. These are only two, but there were and are many such forgeries that can be still stated to have been performed on the images. Ever since the usage of digital images, tampering of the images has also started to increase. Intentionally causing alterations in the image without possessing the right to do it is coined as “digital image tampering”. As the digital images are easily prone to illegal distribution, the proprietors of those data are very keen in making their data identified under their ownership copyrighted. But copyrighting all the digital images at every instance by all means is a practically impossible task to perform.

There are numerous tools that can perform manipulations on the digital images and thereby lead to data misjudgement. Digital images were used basically as evidences for proving criminal actions, to perform forensic

*Corresponding author. Tel.: +919703223757

Email address: venkat.medikonda@gmail.com (V.R.Medikonda)

Double blind peer review under responsibility of DJ Publications

https://dx.doi.org/10.18831/djece.org/2017021001

2455-3980 © 2017 DJ Publications by Dedicated Juncture Researcher’s Association. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

studies, in activities related to law enforcements and the list includes areas that relate to security factors too. The advancement in the camera features with mega pixel range not only has caused the images to achieve a greater quality, but also has caused the forgery hard to be detected when the data are seen physically through the human eye. As the digital images can be easily altered by the aid of software tools that have the capability to edit the images like Photoshop, GIMP and Corel paint shop, etc., the changes that are made in the images are too impossible to be found out [1]. This is because of the advancement that has materialized in digital cameras, specifically emphasising the high resolution pixel range feature that fall under one of the best sophisticated features of the best digital cameras, and if the alterations befall in such minute pixel values, even humans can hardly find out the meddling that has occurred in the images. This has given an emergency alert to the investigators to rely on the techniques that can find out the forged section that was incident on the original image.

The initiation and quick spread of digital tampering in the case of still and moving pictures has triggered moral issues concerning truth, duplicity, and integrity in digital images and digital videos. With experts testing the moral limits of truth, a considerable failure in terms of public trust has now started in the minds of people when they encounter digital images. This persuaded the requirement for tools that can easily find out whether the image is tampered or not, by just examining the image that is suspicious. The counterfeiter ought to utilize a solitary or a mixed arrangement of a series of actions for such operations related to image forgery. Consequently, the Digital Image Forensics (DIF) too must possess a series of operations to reveal the fraudsters. This paper proposes an innovative approach to detect forgery in digital images.

1.1. Need for DIF

On one hand, the internet has given us a highly complex but helpful approach in sharing and exchanging the data the whole way all over the world; but on the other hand, it is to be noted that this cyberspace has likewise created a platform for criminals to exercise their criminal activities. Identity theft, risks to nation’s security and copy-right breach are a few to be named under internet crimes by fraudsters [2, 3].

As already mentioned, images which encompass well-provided collection of data are rampant over the cyber space. Adjustments in the images are done by attackers to change or hide its importance by utilizing advanced software tools as mentioned earlier. These software tools are effortlessly accessible today on PCs and portable PCs as well as on handheld cell phones [3]. Confirming the authenticity of the digital image based on criteria like integrity and source is the actual field of concern of DIF. Distinguishing proof of source includes deciding the methods by which the images are taken such as camera, scanner, and regenerative means [4, 5]. Likewise the, integrity of the image can be affirmed by examining the image for its alterations basically called as tamper detection. The tamper detection techniques for DIF are categorized into active and passive tamper detection techniques.

2. LITERATURE SURVEY

2.1. DIF classification and techniques

DIF can be classified broadly under two major heads, as active forensics and passive forensics. This is exhibited in the hierarchical representation expressed in figure 1. Active forensics [6] involves techniques that can extract digital signatures or watermarks that are inserted in the image. But in passive forensics extracting the details of forgery attacks like copy-move, image splicing and image retouching are performed. Here the features of the image are taken into account to find the forgery action on the image.

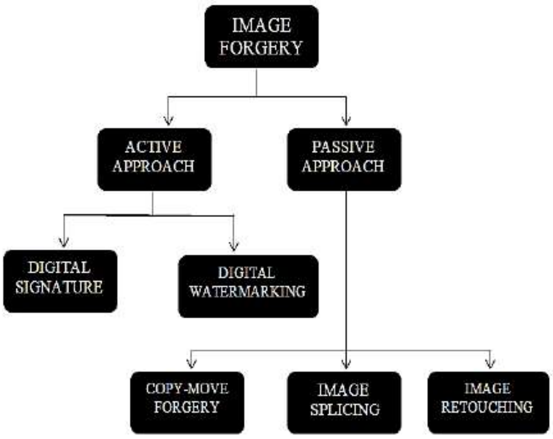


Figure 1.DIF classification

The digital image forgery detection techniques can be classified as shown in figure 2.

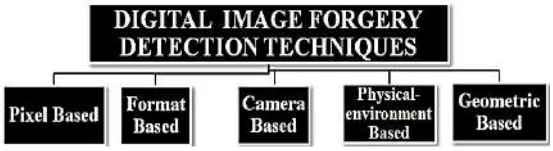

DIGITAL IMAGE FORGERY DETECTION TECHNIQUES
Pixel Based
Format Based
Camera Based
Physical-environment Based
Geometric Based

Figure 2.Digital image forgery detection techniques

2.2. Copy-move forensics

Our focus is on the copy-move forgery detection technique [6]. DWT (Discrete Wavelet Transform) was proposed to detect forgery by a process of lessening the image size and partitioning the image into overlapping blocks of similar sizes and at last the feature vectors related to the image were performed using Fast Walsh-Hadamard Transform (FWHT). To enhance the efficiency, multi-hop jump algorithm was performed to detect the computational cost. Though the computational cost was not that much high, it lefts behind the most important features such as image filtering, recognizing the pattern of the image under suspicion and examining the texture of the image.

This led to Dyadic Wavelet Transform (DyWT) algorithm, where it follows shift invariant technique. Here the actual image was partitioned into many representations also called as sub-bands and matches and non-matches were found out with false positive rates [7]. Furthermore, in the DyWT algorithm, the image was pre-processed by colour conversion techniques and the features of the images were extracted using the Discrete Cosine Transform (DCT) and Stationary Wavelet Transform (SWT). The drawback of DyWT was that, the image to be detected for copy-move must be converted into a grayscale image as a pre-processing step. In the DCT approach, the features of the images were displayed as blocks that were found to be overlapping. This approach was found to be effectual in the way it used the technique of mutual pairs. This technique possessed a feature where false matches were very less but it failed to detect the images which were of large size having similar textures.

FMT (Fourier-Mellin Transform) was found out to detect forgery in images exhibited with scaling and rotational transformations. In this technique, log-polar mapping was performed to represent the image blocks and from the correlation coefficients, the feature vectors of the blocks were found out [9]. This technique was found to be robust to pre-processing functionalities like blurring, noise, JPEG compression, scaling and translation. However it was unable to find the regions which were rotated above 10° and the regions were the scaling was above 10 per cent. Singular Value Decomposition (SVD) was used to detect tampering in the image. The SVD approach generated algebraic and geometric feature vectors. Here the images were partitioned into blocks that were of the overlapping model. This approach was able to fix the copy-move tampering. But this technique was found to be detecting the forgery in the images of invariable regions like sky and ocean. Though it enjoyed the benefits of less computational complexity and robustness during post processing functions, this technique could not deal with JPEG compression.

With the PCA technique, changes in the image due to noise and lossy compressions could very well be detected precisely. But the efficiency of the algorithm was decreased as the image had a lower quality due to decreased block size. SVM classifier was engaged to detect image forgery, where the process involved two phases such as training phase and testing phase with the help of a database to detect image forgery [8]. Though SVM classifiers created precise classifiers and were robust to noise, it was computationally expensive.

Also algorithms like Same Affine Transformation selection (SATs) was used to find forgery in images [9]. Its algorithm was invariant to rotation exhibiting false positive rate. The precision regarding the detection rate of forgery reduced with the increased size of the image.

A forgery detection method based on image matching was performed by using SIFT (Scale-Invariant Feature Transform) technique [10]. Here the false matches were identified but even a little variation in the luminance produced key-points same as those created for big variations and the increase in the key-points surged the computational complexity of the algorithm. SURF (Speeded-Up Robust Feature Extraction) technique was also involved where the feature matching, pruning and duplicated regions were identified. SURF as the name says was intended to enhance the speed of SIFT, detecting the points of interest faster. Though SURF was as good as SIFT, this notion was not for features such as scaling, large blur and viewpoint invariance when SURF was compared with SIFT. SIFT along with Zernike was also performed to detect location based duplication in the images suspected for forgery even after the image was subjected to rotations. Though Zernike moments could detect the copy-paste regions which were flat, it was a complex task to calculate the Zernike moments.

2.3. Current approach

The previous techniques of forgery detection were complex and costly indeed. Here the Auto Colour Correlation (ACC) which was a method adopted earlier only to find the features of the image was also imposed to find the forgery in the images [11]. The Colour Index Local Auto-Correlations (CILAC) method which is a vast sub-division of ACC was adopted to extract more specific colour spacing of the images in detail which proved to be a robust framework encompassing the minute filtering process on the images as an initiative part of pre-processing the image, when compared to other such colour feature extraction techniques [12]. It was by the use of Nearest Neighbour algorithm after calculating the quality of the image, the filtering of the image was successfully performed [13].

3. ACC ENHANCED APPROACH - PROPOSED SYSTEM

The proposed method contains three main phases such as,

- Image pre-processing
- Colour feature extraction
- Forgery detection

The representation of the three phases and the actions that occur under each of these phases are mentioned clearly as depicted under figure 3.

3.1. Image pre-processing phase

In the proposed system, pre-processing the image is the first step. There are chances that the criminals might have subjected the data of importance to some disturbances so that the copy-moved regions can never be easily identified by human perception. In the pre-processing step, noise and disturbances that are present in the image are removed. Only when the noisy data are removed from the image, it can be found whether any activities related to forgery are incidental on it.

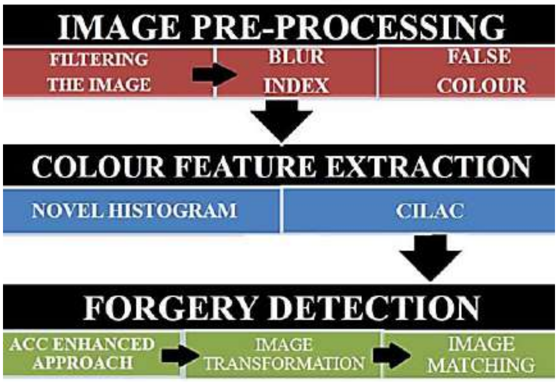


Figure 3.Phases of ACC enhanced approach

3.1.1. Filtering the image

This is the initial process under the image pre-processing phase. Here the image is subjected to noise removal processes that include removing blurredness in image and identifying the false colouring in the image. As the images that may be forged could have been taken from a distant camera positioning or while the object is at motion, or from a camera of poor quality, there is a high possibility of noise presence in that image. So techniques must be included to remove the noise and other sorts of disturbances from the image. The techniques like blur metric, false colour measurements are adopted to find the degree of flaws in the image.

3.1.1.1. Blur Index (BI) calculation

The technique used to calculate the blurriness in the image is represented in figure 4.

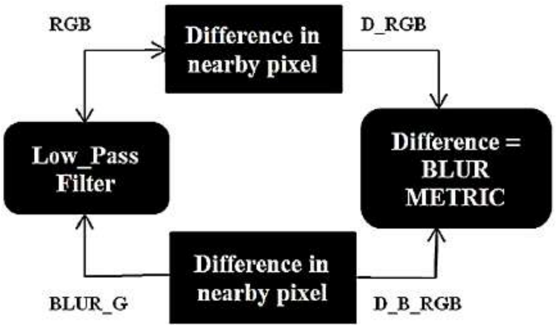


Figure 4.Blur index calculation

The RGB image has channels like red, blue and green. From all these three channels, the green channel alone is taken to perform the BI calculation. This green channel which is taken from the RGB image is made to pass through a low-pass filter. This leads to a blurred green image. The vertical component refers to the row of the RGB image matrix denoted as a, and the horizontal component refers to the column of the RGB image matrix denoted as b. The filter applied is expressed in equations (3.1) and (3.2).

$$\mathrm{F_v} = \frac{[1111111111]}{9} \tag{3.1}$$

$$\mathrm{F'_v} = (\mathrm{F_v^t})_{\mathrm{a,b}} = \mathrm{F_h} \tag{3.2}$$

Here, F_v is the vertical section of the matrix F and F_v' is the transpose that gives the horizontal section of the matrix F which is denoted as F_h. After applying the filter, the difference between the pixels that are present near the original image's green channel and blur green is estimated. This is done by means of equations (3.3 to 3.6) given below. These equations calculate the actual difference between the rows and columns of the original and blur green images.

$$\mathrm{D_{Fv\,(a,b)}} = |\mathrm{F(a,b) - F\,(a-1,b)}|;\ \text{for a} = 1 \text{ to i} - 1, \text{b} = 0 \text{ to j} - 1 \tag{3.3}$$

$$\mathrm{D_{Bv\,(a,b)}} = |\mathrm{B(a,b) - B(a-1,b)}|;\ \text{for a} = 1 \text{ to i} - 1, \text{b} = 0 \text{ to j} - 1 \tag{3.4}$$

$$\mathrm{D_{Fh}(a,b)} = |\mathrm{F(a,b) - F(a,b-1)}|;\ \text{for b} = 1 \text{ to j} - 1, \text{a} = 0 \text{ to i} - 1 \tag{3.5}$$

$$\mathrm{D_{Bh(a,b)}} = |\mathrm{B(a,b) - B(a,b-1)}|;\ \text{for b} = 1 \text{ to j} - 1, \text{a} = 0 \text{ to i} - 1 \tag{3.6}$$

Here, i is the width of the image and j is the height of the image. This measurement involves both the vertical as well as the horizontal directions to obtain the D_RGB and D_B_RGB matrices. Here, D_RGB represents the difference in the RGB matrix and D_B_RGB represents the difference in the blur RGB matrix. The extent of the difference that is present in both these matrices gives the blur metric.

3.1.1.2. False colour

The feature of false colour reckons the range of pixel values with varied colours, from the nearby pixel vales. This procedure is done on various forms of the same input image that is to be checked for forgery. To conduct the estimation of quality of the image, in this technique it is a must to find the edges that are present mutually in all the forms of that particular image which is subjected to test. It is after which, the corresponding form of the image to be calculated for image quality inspection is divided into sub-matrices in the 5×5 range. The median of this particular sub-matrix is estimated by analysing each and every pixel. At last the matrix along with the estimated median value is examined from the data obtained from the edges that are recognized. This process is encapsulated by the aid of the formula given in equation (3.7).

$$\mathrm{F_C} = \frac{\sum_{\mathrm{a,b}\,\in \mathrm{ME}}[(\mathrm{CG_{a,b}} - \mathrm{AC_{a,b}}) - \mathrm{CM_{a,b}}\,]^2}{\mathrm{num_{ME}}} \tag{3.7}$$

Here F_c represents false colour, ME represents edges that are mutually present, CG represents the channel in green and AC represents the channel analysed be it red, blue or green. CM represents the channel median to be analysed and finally num_ME represents the number of edges that are mutually present. This formula gives the range of false colour present in the forged image.

3.1.1.3. Nearest neighbour algorithm

The false colour in the image usually occurs when the edge of the image does not fall under a part of the image. The false colour detection formula is applied to the nearest algorithm. After its application, the common edges of various forms of the image are obtained. The value of median from the RGB image to be analysed is compared with the edges that are mutually present and then the false colouring is found out. Although there might exist situations of images to be unclear if they were taken from sources whose focal points were not stable while capturing, there is also great possibility of the images to be purposely made to become blurred. Also there is a fact that the image with noise for example blurriness or false colour could very well hide some useful data. So it is necessary to check the quality of the data (image). After checking the quality of the image, the image that is under suspicion is subjected to the histogram generation process.

3.2. Colour feature extraction

After the pre-processing step, the colour feature extraction process is performed. In this phase the colour features are extracted by two means. The first one is the histogram generation technique and the next one involves a more colour indexing classification named as CILAC.

3.2.1. Histogram generation process

In the histogram technique, the image is partitioned into blocks and by using the histogram approach the RGB values of the input image are calculated. In this process the sum of RGB intensity which is expressed as $\mathrm{sum_{RGB}}$ is calculated at each pixel level. To perform this calculation, the following equation (3.8) is adopted.

$$\mathrm{sum_{RGB}}(a,b) = I_R(a,b) + I_G(a,b) + I_B(a,b) \qquad (3.8)$$

Here, $\mathrm{sum_{RGB}}$(a,b) denotes the sum of ranges of the red, green and blue values at pixel locations a and b, I_R(a,b) denotes the red intensity value of the pixel at locations a and b, likewise I_G(a,b) and I_B(a,b) denotes the green and the blue intensity values of the pixel at locations a and b respectively. For this process, the image under suspicion is fed as an input. The $\mathrm{sum_{RGB}}$ values are calculated using equation (3.8). The images are further subjected to more filtering process for extracting the colours.

3.2.2. Colour Index Local Auto-Correlations (CILAC)

After the RGB values are obtained, to perform the forgery detection in the image, first the image must be converted into HSV space. The colour aspects and the colour related features of the images are extracted by a technique called CILAC. Here the images which are to be sensed for forgery are subjected to pixel wise calculation regarding the colour aspects present in the image. The pixel values of the coloured image that are thus calculated are then subjected to colour-indexing autocorrelations by spacial means. This technique to index the colour finds its way enhanced just because it follows a different criterion in indexing numerous colour patterns present in the image.

The second stage of the second phase of the proposed system is the CILAC that extracts the colour index. The overall process of CILAC is depicted under figure 5. The pixel values obtained from the histogram technique mentioned above, is fed into the CILAC method. This method finds the enhanced colour space; colour indexing and finally the identification of auto correlations.

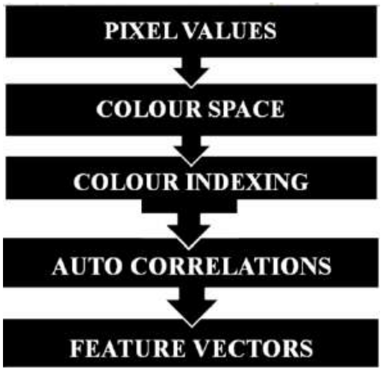


Figure 5.Process flow of feature vector generation by CILAC

Here, the RGB values from the above used histogram technique are given to the system to find the colour spaces like L*a*b and Hue, Saturation Value (HSV) and as the next step, the pixel values from the corresponding colour space is indexed on the basis of numerous basic colours that are adopted by this proposed model to express the sparse vector which is expressed by the alphabet c. At last the auto correlations are estimated and the false matches and the forgery in the images are detected to have a high precision value when compared to the previously available methods used so far to detect image forgery.

To perform the image forgery detection and false matching, the ACC technique is adopted. The indexing is first performed with the help of the predefined colours of the RGB regarding the basic colours like P7/P8/P15. In the P7 colour space indexing process, the dark pixels are eliminated as being of raw type. The P8 indexing adds black colour. The L*a*b colour space, makes use of the eight to fifteen basic colours of RGB for its colour space to be mapped. The basic colours of HSV are obtained from the upper points of the cone. Cluster Centre Colours (CCC) which represents the colour indices from C8 to C15 is set up, as already determined data in a data set to map the image into more specific colour values. As the colour spaces to index the colours are predefined, the colouring quality of the image is enhanced to a rich quality prohibiting noise as well. The k-nearest algorithm is performed to find the nearby voting weights of the colours that are indexed.

The sparse matrix is obtained by following the equation that obtains the weights of each and every pixel value.

The weights are calculated using equation (3.9) which gives the sparse vector c.

$$\widehat{w_j} = \frac{w_j}{1+\sum_{m=2}^{k} w_m} \qquad (3.9)$$

By using the sparce vector, auto correlations of the colours for both the zeroth and the first order are estimated by the equations (3.10) and (3.11) which state the point_of_references, expressed as P_{R_0} and P_{R_1}.

$$P_{R_0}(i) = \sum_{rp} c_i\,(rp) \qquad (3.10)$$

$$P_{R_1}(i,j,d) = \sum_{r} c_i(rp)c_j(rp+d) \qquad (3.11)$$

where, rp is the reference point, c_i is the colour index and d is the displacement. The results when compared with the previously available methods regarding indexing of the colours in a collection of images given as input are provided in the graphical representation in figure 11. This approach also yields the more enhanced blocks of the image that underwent ACC.

3.3. Image forgery detection

3.3.1. ACC enhanced approach

This phase in the proposed system represents ACC as a technique that has used CILAC's enhanced colour featuring output for the ACC approach for the first time to detect image forgery. The ACC which usually extracts only the colouring features is used here to detect forgery and so is named as ACC enhanced approach. The input data which is to be checked for forgery is subjected to 8Z affine transformation. This is done, as the image may be subjected to forms of transformations like rotation, scaling etc., so as to hide the forgery which was committed by means of subsequent copy-move forgery actions.

3.3.2. Finding the match

Here the two adjacent blocks of the ACC enhanced approach is matched to find the forgery. The features extracted from the above equation (3.11) in correspondence to the block under forgery are subjected to comparison by means of every adjacent block to find the match. The approach of distant metric (d) is used to perform this function. This can be expressed from the equation (3.12) as,

$$|B - B'|_{\gamma,d} = \sum_{i,j\in[m],k\in[d]} \frac{|\gamma^{(k)}_{c_ic_j}(B) - \gamma^{(k)}_{c_ic_j}(B')}{1+\gamma^{(k)}_{c_ic_j}(B)+\gamma^{(k)}_{c_ic_j}(B')} \qquad (3.12)$$

Here B and B' represent the neighbour blocks that are compared at every instant till all the blocks are compared. The end results reveal the matching data that detects the forgery incidental on the image.

4. RESULTS AND DISCUSSIONS

4.1. Image pre-processing

Here the image is pre-processed by means of filtering techniques to find out disturbances in the image. The two techniques used to filter are BI calculation and the false colour technique. These techniques are adopted to find the quality of the tampered image. The input of the tampered image which is blurred is shown in figure 6.

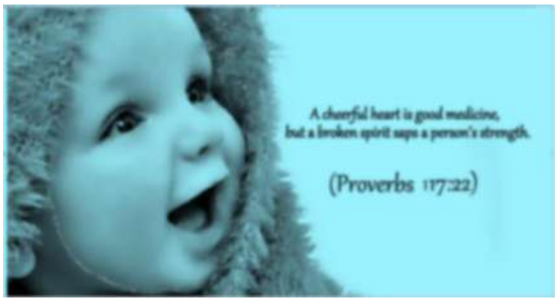

A cheerful heart is good medicine,
but a broken spirit saps a person's strength.
(Proverbs 17:22)

Figure 6.Forged blurry image

The BI value is calculated and then the image is corrected using the nearest-neighbour algorithm. The output of the image after removal of blur is presented in figure 7.

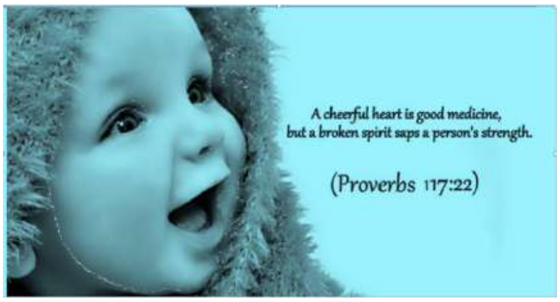

A cheerful heart is good medicine,
but a broken spirit saps a person's strength.
(Proverbs 17:22)

Figure 7.Blur removed image

Next in the image, the false colour trait is checked. The false colour detection algorithm, finds the false colour range and again the nearest neighbour technique removes the false colour from the image. The removed false colour is presented in figure 8.

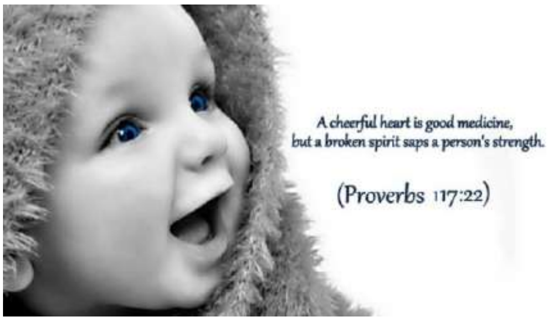

A cheerful heart is good medicine,
but a broken spirit saps a person's strength.
(Proverbs 17:22)

Figure 8.False colour removed image

This shows that the image which was tampered was actually a colour image and not a black and white one. The tampered image showed that the baby had black eyes, but actually the eyes were blue. Forgery is found and so this image needs to be further filtered.

4.1.1. Nearest Neighbour method

The nearest neighbour method is found to be the best chromatic interpolation method among the various such methods that can correct the image to give clarity to the image by evaluating its quality. This is given by the graph as in figure 9, when the above two traits like blur index and false colour were taken into account for a large database. It is obvious that only the nearest neighbour algorithm in which the blur metric and the false colour formula were applied, yielded best results when compared to other such algorithms that used the quality evaluation techniques like blur metric and false colour identification.

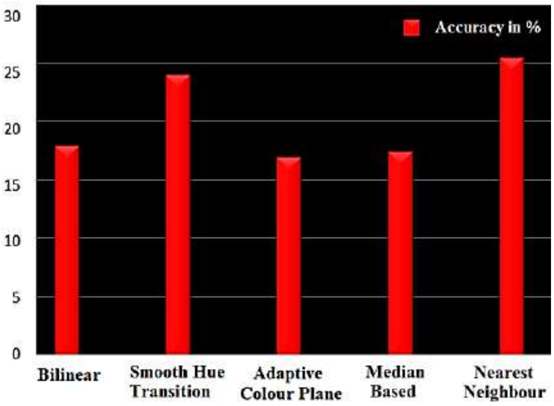
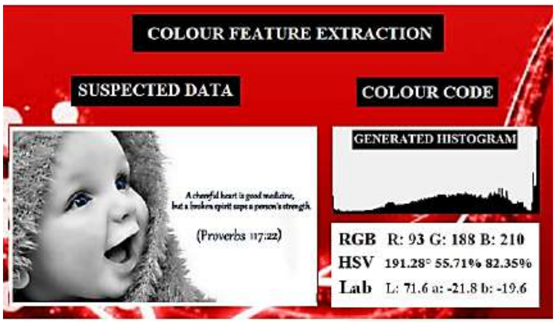


Figure 9.Comparing accuracy among various chromatic interpolation methods

4.2. Colour feature extraction

Next, the histogram of the image which is suspected to be tampered is fed for histogram calculation. The calculated histogram is given in figure 10.

The histogram generated reveals the RGB pixel values. The RGB pixel values are fed to the CILAC auto correlation technique to find the colour codes. This undergoes L*a*b and HSV calculations.


COLOUR FEATURE EXTRACTION

SUSPECTED DATA

COLOUR CODE

GENERATED HISTOGRAM

RGB R: 93 G: 188 B: 210

HSV 191.28° 55.71% 82.35%

Lab L: 71.6 a: -21.8 b: -19.6

A cheerful heart is good medicine,
but a broken spirit saps a person's strength.
(Proverbs 17:22)

Figure 10.Colour feature extraction

The CILAC method is proved to be the best method among other such methods as evident from figure 11.

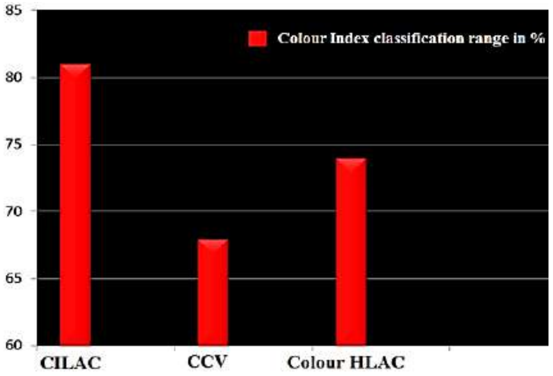


Figure 11.Classification of colour index among various methods

4.3. Image forgery detection

The image which is suspected to be forged is converted into blocks using the matrix obtained from the colour extraction matrix. As the next stage which heads towards the forgery detection process, the ACC technique encounters the image to undergo 8Z affine transformation. Here the algorithm finds the block (given under dotted square lines) that is suspicious to forgery and that block is subjected to 8Z affine transformation. This is shown in figure 12.

4.3.1. Finding the match

In the forged image shown in figure 12, a part of the text was actually placed at a varying distance in order to add a single digit altering the already present original data. This forgery action was found out to be injected in the block, when it was compared with the original image, block by block. Thus the match was found out depicting the copy-move forgery action that was incidental on the real data. The final result is shown in figure 13.

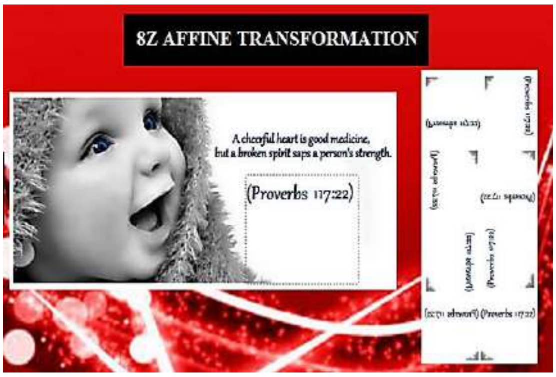

8Z AFFINE TRANSFORMATION
A cheerful heart is good medicine, but a broken spirit saps a person's strength.
(Proverbs 17:22)

Figure 12.8Z affine transformation

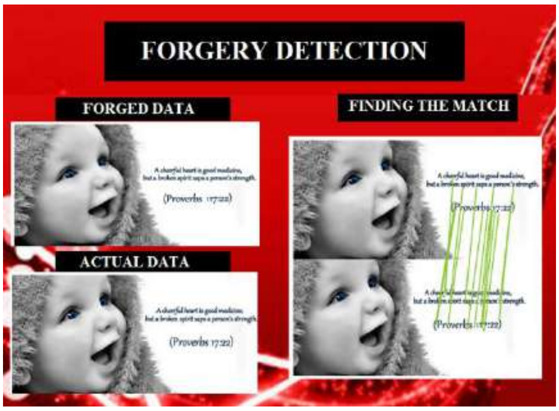


Figure 13.Detection of forged area

4.4. Evaluation of the proposed system

A collection of 500 images were taken randomly and were tested for forgery. The forgery detection in terms of true positives, false positives which were performed using the parameters like precision, recall and F1 score are shown in table 1.

Table 1.Evaluation parameters in ACC enhanced approach with 500 images

Precision (p_r)	Recall (r_c)	F1
0.9789	0.9234	0.9362

The proposed copy-move forgery detection proved to be effective when compared to existing methods to detect copy-move forgery which is clear from figure 14.

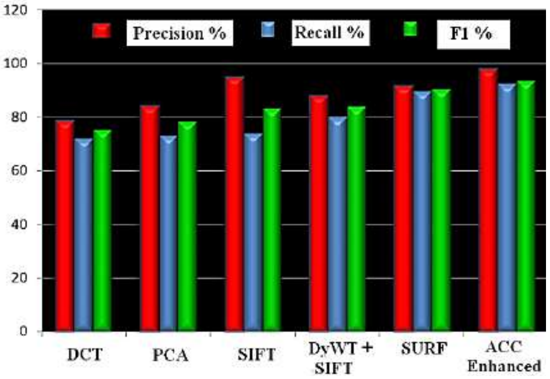


Figure 14.Graph showing performance of ACC enhanced approach

5. CONCLUSION AND FUTURE ENHANCEMENT

With computerized advancements, it is not only the photos which have become digital but also the videos. It cannot be denied that digital data in the form of images and videos can be stored and referred even after thousands of years. But the digital data can be very well subjected to manipulations, and tampering. Our research work did not address the detection of tampering in video surveillance evidences [14]. The main focus of the research was only the digital image. Involving ACC in video tampering detection with a focus on the sensor features of the camera can be a work of enhancement for future innovations in DIF [15].

REFERENCES

[1] Rani Susan Oommen, M.Jayamohan and S.Sruthy, A Survey of Copy-Move Forgery Detection Techniques for Digital Images, International Journal of Innovations in Engineering and Technology, Vol. 5, No. 2, 2015, pp. 419-426.

[2] C.Berin Jones, Cyber-Security and Combatting Cyber-Attacks: A Study, Journal of Excellence in Computer Science and Engineering, Vol. 3, No. 2, 2017, pp. 1-16, http://dx.doi.org/10.18831/djcse.in/2017021001.

[3] Anil Dada Warbhe, R.V.Dharaskar and V.M.Thakare, A Scaling Robust Copy-Paste Tampering Detection for Digital Image Forensics, Procedia Computer Science, Vol. 79, 2016, pp. 458-465, https://dx.doi.org/10.1016/j.procs.2016.03.059

[4] T Van Lanh, K.S.Chong and S.Emmanuel, A Survey on Digital Camera Image Forensic Methods, Multimedia and Expo, IEEE International Conference, 2007, https://dx.doi.org/10.1109/ICME.2007.4284575.

[5] T.S.Kiran, A Framework in Shadow Detection and Compensation of Images, DJ Journal of Advances in Electronics and Communication Engineering, Vol. 2, No. 3, 2016, pp. 1-9, http://dx.doi.org/10.18831/djece.org/2016031001.

[6] Nandini Singhal and Savita Gandhani, Analysis of Copy-Move Forgery Image Forensics: A Review, International Journal of Signal Processing, Image Processing and Pattern Recognition, Vol. 8, No. 7, 2015, pp. 265-272.

[7] Gajanan K.Birajdar and Vijay H.Mankar, Digital Image Forgery Detection using Passive Techniques: A Survey, Digital Investigation, Vol. 10, No. 3, 2013, pp. 226-245, https://dx.doi.org/10.1016/j.diin.2013.04.007.

[8] Hany Farid, Image Forgery Types and their Detection: A Review, Image Forgery Detection, IEEE Signal Processing Magazine, Vol. 26, No. 2, 2009, pp. 16-25, https://dx.doi.org/10.1109/MSP.2008.931079.

[9] Anil Dada Warbhe, R.V.Dharaskar and V.M.Thakare, A Survey on Keypoint Based Copy-Paste Forgery Detection Techniques, Procedia Computer Science, Vol. 78, 2016, pp. 61-67, https://dx.doi.org/10.1016/j.procs.2016.02.011.

[10] P.R.Ruikar and P.S.Patil, Copy Move Image Forgery Detection Using SIFT, Oriental Journal of Computer Science and Technology, Vol. 9, No. 3, 2016, pp. 235-245, http://dx.doi.org/10.13005/ojcst/09.03.09.

[11] A.V.Malviya and Siddharth A.Ladhake, Pixel Based Image Forensic Technique for Copy-Move Forgery Detection using Auto Color Correlogram, Procedia Computer Science, Vol. 79, 2016, pp. 383-390, https://dx.doi.org/10.1016/j.procs.2016.03.050.

[12] Anil Dada Warbhe, R.V.Dharaskar and V.M.Thakare, Computationally Efficient Digital Image Forensic Method for Image Authentication, Procedia Computer Science, Vol. 78, 2016, pp. 464-470, https://dx.doi.org/10.1016/j.procs.2016.02.089.

[13] M.Thangamani and P.Seetha Subha Priya, Image Retrieval System by Skin Colour and Edge Information, Journal of Excellence in Computer Science and Engineering, Vol. 1, No. 1, 2015, pp. 15-24, http://dx.doi.org/10.18831/djcse.in/2015011003.

[14] M.Jerian, S.Paolino, F.Cervelli, S.Carrato, A.Mattei and L.Garofano, A Forensic Image Processing Environment for Investigation of Surveillance Video, Forensic Science International, Vol. 167, No. 2, 2007, pp. 207-212, https://dx.doi.org/10.1016/j.forsciint.2006.06.048.

[15] Nitin Khanna, Aravind K.Mikkilineni, George T.C.Chiu, Jan P.Allebach and Edward J.Delp, Forensic Classification of Imaging Sensor Types, International Society for Optics and Photonics, 2007, http://dx.doi.org/10.1117/12.705849.