Journal of Intelligent Systems and Internet of Things
Vol. 17, No. 01, PP. 409-424, 2025
DOI: https://doi.org/10.54216/JISIoT.170129

Robust Forgery Detection in Digital Images Utilizing the Multiple Image Splicing Data Set (MISD)

Heba Adnan Raheem[1,*]
[1]Department of Computer Science, College of Computer Science and Information Technology, University of Kerbala, Karbala, Iraq
Email: hiba.adnan@uokerbala.edu.iq

Abstract

In the area of digital information, establishing the authenticity of an image has grown to have greater significance as more and more persons have access to sophisticated image editing technologies. There is however a challenge in detecting such a forgery since it is usually very realistic and it is hard to know the difference between the real images and the fake ones. This paper aims at creation of a mechanism of identifying forged images based on Multiple Image Splicing Dataset (MISD) as a reference point. The suggested system will help to improve the results of the forgery detection, paying particular attention to the images processing during some of the pre-processing steps Firstly, converting colors into the hue-based histograms and RGB histograms, and hue-based histograms in an HSV, in comparison between the original and forged image, its HSV histogram, and its grayscale histogram, etc. Lastly, compute MSE and SSIM original and forged image. The implementation results showed that average value of MSE and SSIM metrics on Multiple Image Splicing Dataset (MISD) equal to 184.82 and 0.65 respectively that means the suggested method proved the efficiency of the technique to identify forged images as quickly as possible but still retain accuracy.

Received: January 03, 2025 Revised: February 25, 2025 Accepted: May 05, 2025

Keywords: Image forgery; Image splicing; Feature extraction; MSE; SSIM

1. Introduction

The damage of an image is more effective on observers than millions of words as image is presented in courtroom, in scientific studies, political essays and also in celebrity publications, since image is a natural and productive method of people communicating [1]. To exemplify, there is no necessity to convert a image in one language into another, the quick access, convenience of using and the low prices of devices that facilitate the process of capturing, storing, and transmitting images, such as portable devices, scanners, and other electronic cameras has helped [2]. Meanwhile, due to the quick accessibility of software packages utilized to alter and manipulate images, it becomes extremely simple even to the least experienced of users to manipulate images and predominantly generate images [3]. This increases the possibility of forgery and manipulation of images, and this is not limited to experts and specialists. Therefore, the weight and integrity that digital images enjoy is weakened by the progress of digital technology. For example, images from fashion magazines have been modified by 100%. The proposed system is related to detecting one type of image manipulation: the middle between images and video clips [4].

Image forgery detection is a very important area of life that tries to detect image manipulation or alteration. The image forgeries have been quite difficult to detect with the emergence of advanced editing tools [5]. Digital watermarking, statistical analysis, and machine learning are different methods utilized to examine photos with features of manipulation [6]. Nevertheless, the matter is still complicated by the fact that there is a great variety of forgery techniques, and the technologies of editing change continuously. In this chapter, we explore the fundamentals and advancements in image forgery detection, addressing key challenges and emerging trends in the field as shown in Figure 1 [7].

Figure 1. Original and forged images [7].

The image forgery detection is classified into two procedures that are founded on the previous knowledge of the forgery detection. They are Active approaches based forgery checking and passive approaches based forgery checking as depicted in Figure 2 [8].

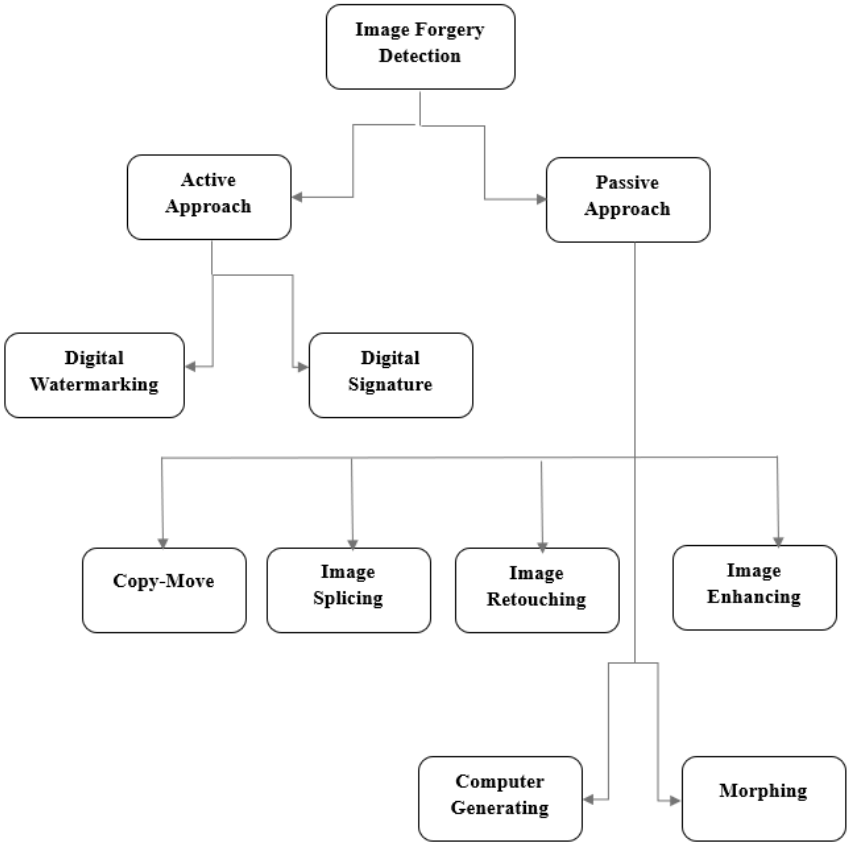


Figure 2. Forged image detection Types [8].

The forgery detection mechanism in the active images is that of providing some information on the image in an attempt to identify the digital absurd description like name, date, signature, etc., as it involves introducing special equipment to help identify the mark that enhances accuracy in the authenticity of the digital image. Active methods are of two kinds namely; digital signature and digital water making [9, 10]. The retrieved confidential data or signatures are checked with the data that is stored to carry out a verification process on the date in which the data is being retrieved to the receiving party. The requirement or non-requirement of the original image may not be meag in the receiving party in the course of the process of the examination since the procedure of checking the data retrieval in the presence of the original image is referred to the process of auditing non-secretive approaches and the procedure of verifying data retrieval without the presence of the original image in the process of concealing digital information [11].

A. Digital Watermarking

It is a technology that includes embedding the watermark data in the multi-media where it is later extracted from the watermarked medium where it is detected. These methods include tamper resistance, digital content verification, digital authentication, and image integrity [12].

B. Digital Signature

It is regarded as one of the active means of detecting the image forgery or tampering since it is referred to proving the authenticity of the digital document by the means of a type of mathematical schemes contributing to the creation of the digital signature when strong bits are taken out of the original images and divided into 16 x 16-pixels blocks. The division process has a secret key to come up with a random matrix with numbers randomly distributed between zero- and one-time intervals. Then a low-pass filter is taken on each random matrix and this is repeated to achieve a smooth random pattern [13].

The stage of adding a digital signature to the system is through applying a signature process to the digital image and includes several steps as follows [14]:

1. Image analysis based on the waveforms.
2. Extract the SDS variables.
3. Cryptographically hash these SDS variables.
4. Creating the cryptographic signature based on the private key of the sender of the digital image.
5. Sending the image and the cryptographic signature created in the previous step to the recipient, where this signature is a simple approach that is fundamentally based on authenticating the digital image [15].

Passive forgery detection criteria is exactly the opposite of active mode of detection. Passive techniques are also unquestionably used to confirm the falsehood of the image without prior knowledge of the real image or its property [16]. The passive techniques of verifying the genuineness of the image entail the application of the statistics and contents of the image that are availed. The verification is done through the use of the information of the image it is without any other information. The passive methods are based on the later recognition of the forged image based on the knowledge at hand and thus also known as blind approach [17].

C. Copy Mover Forgery

Copy and move forgery is a process that entails replicating some of the contents of an image that had been pasted on another segment of the same image frame. It is aimed to conceal a portion of the information in the original image. This is the most commonly used method for forging digital images because it is based on the copied part remaining from the same image. There are no significant visible changes seen by the analyst. Therefore, detecting these changes is difficult, as shown in Figure 3 [18].

Figure 3. Copy move forgery.

D. Digital Images Retouching

It is considered one of the least harmful types of digital image forgery, as it does not significantly change the visual message of the image. The image editor changes the background, adds some colors, and increases the saturation of some areas of the image to achieve balance. It is used to improve the image or reduce a certain feature of it and add quality to the image to attract the recipient's attention and draw his attention, as it shown in Figure 4 [19].

Figure 4. Copy move forgery.

E. Enhancing

This form of manipulation does not alter the content of the image entirely, but it incorporates the adjustment of the contrast of the image, altering the color, regulating the noise, as well as, boosting the resolution. Such kind of manipulation indirectly influences the image interpretation. Figure 5 demonstrated how the time of the day when the image was captured changed [19].

Figure 5. Enhanced image.

F. Computer Generating

Computer-generated image forgery involves the creation or manipulation of images using digital editing tools or algorithms. It encompasses various techniques aimed at fabricating synthetic images or altering existing ones to produce realistic but deceptive results as shown in Figure 6 [19].

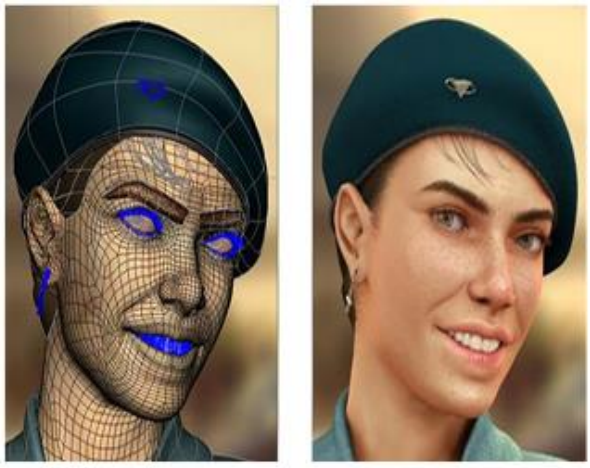


Figure 6. Computer Generating [19].

G. Splicing Forgery Method

Photographic manipulation is done by using a composite of two or more images to add a new image, where the images are carefully connected so that the borders are often visually imperceptible, as shown in the Figure 7 [20].

Figure 7. Splicing method [20].

H. Morphing

It is founded on a digital technology that helps in changing the original image to another different image by bits as revealed in the figure where the image of a person is changed to a space doll image whereby the shape and appearance of the original image are gradually altered into a new image with a different shape and look. The features of the original image, and the features of the forged image are in the intermediate image, and the intermediate image will have a side that will have the characteristics of human part and the characteristics of alien part as it represented in Figure 8 [21].

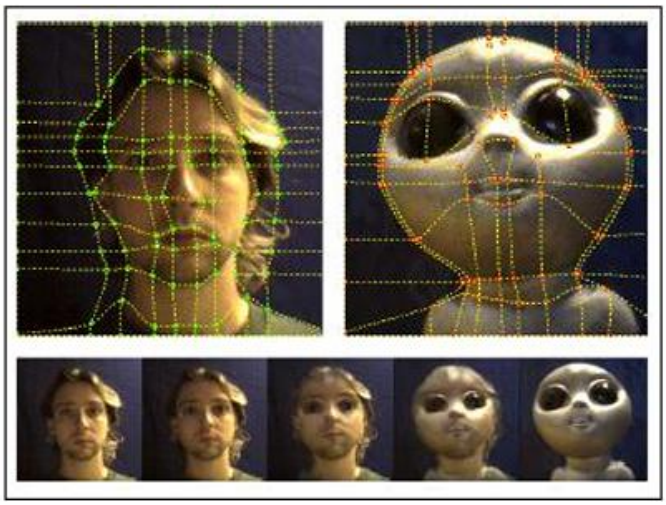


Figure 8. Morphing [21].

The practice of image splicing detection has been described in literature survey as having different approaches, using geometry invariants and consistency of camera characteristics, and using deep learning models based on convolutional neural networks (CNNs), and auto encoders. However, these methods often relied on datasets that did not adequately represent the complexities associated with multiple splicing. The MISD not only includes a diverse array of spliced images but also offers ground truth masks, enhancing the accuracy of detection algorithms by providing clear references for identifying spliced regions, research directions sorted as follows:

In [22] the authors relied on the FCN algorithm, which contributes to identifying the location of the manipulated region within the image, because they had the original image in a database where fake image was to be positive and negative samples were to be black images which represent the basic truth of the original image in order to differentiate the differences between the fake image and the original image. The output of the developed algorithm

revealed that it led to the determination of the position of the fake area and it had been a better performance than the external ones presently existing in this area, as it provided a viable approach to detect digital image forgery.

In [23] the authors focused on improving the accuracy of detecting forgery between images using low-dimensional feature vectors by proposing the approximate fractional Matt Shadow entropy to convert the discrete waves that contribute to capturing the effects of connection within the image in a way that is by analysing the original image into a number of sub-images with different frequency ranges. The standard CASIA v2 dataset was adopted and the results showed the accuracy of the process of detecting fake images compared to other modern methods with low dimensions for different feature vectors and from the image.

In [24] researchers have proposed another method ResNet-conv which plays a role in detecting forging of blind images with the use of a new basic structure ResNet-conv, the deep learning process with the creation of a map of the original features which was replaced by the set of convolutional layers. and then training the Mask RCN algorithm to create masks for the regions and forged images based on allocating the distinct pieces from the tampered regions and comparing them based on the degree of convergence with the original images, where many processing techniques were applied to the input images, and the results showed the efficiency of the proposed algorithm compared to other techniques that are based on using a set of image linking data generated by the computer.

In [25] an innovative method was proposed that contributes to the process of detecting image forgery based on the transformation of the discrete cosine value and the local binary pattern to extract specific features in the image based on the averaging factor, where the images were divided into blocks of the same size that do not overlap with each other, and the discrete cosine was applied to the two-dimensional blocks to capture the changes affecting the image forgery, and the local binary pattern was applied to enhance the effects of forgery and detect them, and the average value of all blocks of the local binary pattern was calculated to produce a number of features that contribute computationally efficiently to detecting image forgery, where the SVM algorithm was implemented to evaluate the proposed approach to detect image forgery in grayscale and colors and use a data set which is grounded on the Internet of Things, the outcomes of the experiment demonstrated the effectiveness of the proposed approach with regard to the performance measures in the face of the limited availability of forged image training samples.

In [26] the researchers proposed a new technique that contributes to detecting image forgery based on linking images using discrete waveform transformation as well as graphs of local binary discriminative patterns. Was the color image converted and discrete waves applied with YCbCr for the digital image analysing. Each sub-band was contrasted with the help of the prevailing rotating local binary patterns that led to the creation of the binary feature vector. The support vector machine is used as the basis of the proposed system to come up with image forgery detection. The results showed that the proposed system outperformed modern detection techniques with an accuracy of 98.95%.

In [27] the authors proposed using a MWC-Net multi-task wavelet correction network that contributed to learning more comprehensive and representative features to detect link forgery and distinguish its location based on wavelet collection, decompression and reconstruction based on the features of link forgery images, which reduced the loss of information during feature learning. MWC-Net was based on a multi-task strategy that contributed to more comprehensive learning to improve image forgery detection. The results showed that the proposed system outperformed other methods based on the same image forgery features based on public data.

In [28] the authors proposed a method to detect image forgery based on the color distribution of pixels near the edge of the images by extracting these pixels using the contour let transformation technique, which accurately distinguished the original edges and manipulated edges based on the IQR quartile range criteria, which distributed the chromatic histograms and borders in the YCbCr color space. This method was used to segment to improve the localization performance and reduce the computation time in particular, as the effectiveness of the proposed system was proven based on a data set to detect the communicative forgery in Colombia. The results noted the superiority of the proposed system in the accuracy of detecting image forgery by about 97% with 100% privacy.

In [29] The researchers were able to use a collection of databases to detect forged image splicing, namely Colombia Carvalho and CASIA V1.0, and detect forgery like modified CASIA database like the proposed system since image splicing detection does not have multiple spliced images. Multiple-spliced images were sorted to give a total of 300, high quality, clear, and realistic images. The outcomes of the suggested system demonstrated that it offered a collection of quality images that can be popular and gave some prospects to researchers operating in the given sphere.

The researchers in [30] came up with a CNN model to identify fake images with high precision in real-time using a few variables. The lightweight model was introduced on the basis of a group of convolutional layers that can be applied in a low-source setting. The proposed system was compared to other works in detail. The findings covered the sensitivity of the algorithm on CASIA 1.0 and 2.0 databases, with an accuracy of 99.1, forgery detection on

CASIA database with the percentage of 99.3, and forgery detection on CUISDE database with the percentage of 100. The system was accurate as a system of detecting the image that is forged in real time.

In [31] Authors have suggested a different way to find image forgery and manipulation using DCU-Net-channel UNIT network. The proposed system is grounded on the division of the network-based detection frame into three elements, encoder, and feature fusion and decoding. The remnants of the forged and manipulated images are extracted with the help of the high frequency filters. The other images of the filter are produced. It includes on the frame details of the manipulated area respectively which is generated according to the network model is that of dual-channel encoding. Thereafter, the original image and the modified image are inputted. The deep features obtained during the encoding are combined in addition to the tampered during convolution and dilation in the secondary fusion technique features. In decoding, the feature map is used. It was demonstrated in the results of the proposed system on the Colombia dataset that the algorithm was optimally effective in identifying and resisting noise and recompression attacks on JPEG images.

The purpose of the study of this work are developing algorithms capable of detecting sophisticated image manipulations. Raising public awareness about the importance of verifying the credibility of images and not falling for fake images and evaluating the effectiveness of existing image forgery detection methods and identify areas for improvement.

2. Methodology

In this study, the technique that has been used in the scope of methodology considers the creation and application of splicing forgery detection method in digital images. It involves a few major steps that will maximize the precision and performance of the splicing forgery detection algorithm. The Figure. 9 was used to demonstrate the proposed system:

The following steps are used to explain how an image forgery detection algorithm can be implemented and the most important processes included are pre-processing, visualization, and comparison and quality assessment. The goal would be to provide an in-depth study of the image forgery detection, employing a wide variety of image characteristics and measures:

A. Define file paths, Read images in data set:

Start by defining the path of the original and forged image folder. Then, go through images of both directories to be made ready to analyse it further.

B. Check for Image Identity

Make sure that each folder contains the same number of images and make sure they are not of different identity. In case the images are the same then produce a forged image by overlaying another image to the original image.

C. Preprocess Images

Transpose images into HSV colour space using rgb2hsv function, calculate hue variations, by subtracting the forgery image on original image, and calculate grayscale, RGB and HSV histograms of original image and forged image.

The raw input images undergo pre-processing stage where they undergo various operations to enhance the quality of the input images as well as transform them into a stage where they can go through more analysis and processing. These operations include:

```
Algorithm Image_Forgery_Detection

Start
Define dataset paths
Load original image
Load forged image

If original image == forged image then
    Merge original image with another image
    Create forged image
End If

Preprocess original and forged images
Display images for visualization
Detect forgery regions in the image

Compute MSE between original and forged images
Compute SSIM between original and forged image

Repeat process for all images in dataset
End
```

Figure 9. The image splicing forgery detection algorithm implementation pseudo code.

1. Image Resizing: This operation involves manipulation of dimensions of an image. In the detection of forgery, the resizing should do the same, on the other hand, so that the original and the forged images are of identical dimensions, as only under that condition can their comparison and analysis be conducted.
2. HSB Colour Space Convertor RGB: Images are stored in the RGB (Red, Green, Blue) Colour space but converted to the HSV (Hue, Saturation, Value).

H: The colour quality (Red, Green, Blue).
S: Intensity of colour.
V: Brightness of the colour.

As demonstrated in Figure 10, the forgery can be detected with simplification and improvement using colour space.

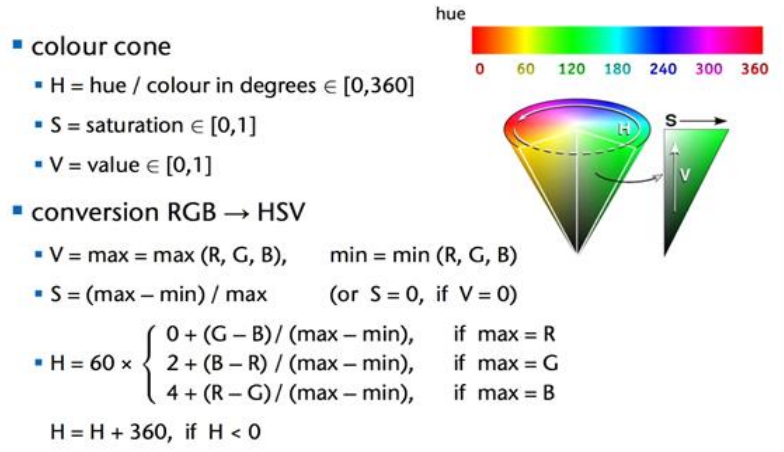


Figure 10. Correlation between the HSV colour system and the RGB colour system.

3. Hue Component Extraction: Colour tone of an image would be represented in the colour component. Through this extraction, algorithms of forgery detection can concentrate on colour differences in both original and forged images which most of the time are a pointer of forgery. Mathematically, hue extraction is isolation of hue channel in the HSV representation of image.
4. Histogram Calculation: The histogram is a chart used to display the distribution of pixels in a image. Computing of a histogram of the grayscale and RGB colour space assists in examining the general distribution of brightness, contrast and colour intensity in the images. Hue, saturation, value components Insight into the discussions of colour in HSV Colour space are provided in histograms, which can be helpful in identifying colour-based forgeries [32, 33]. Examples of Histogram were shown in Figure 11 below.

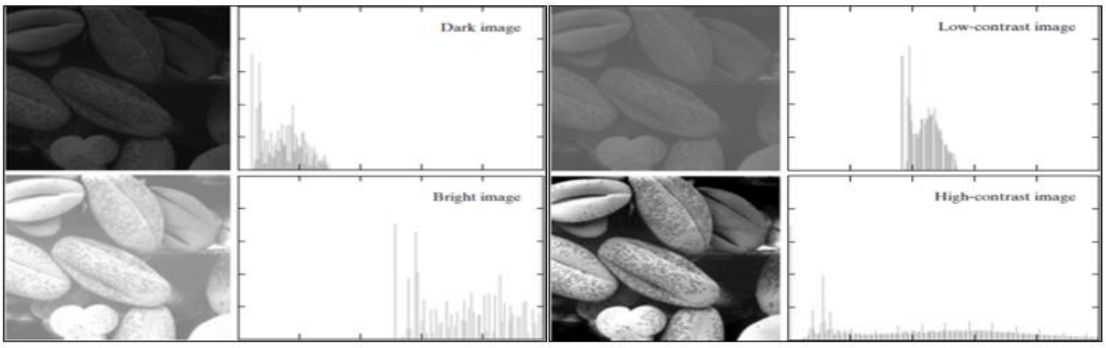
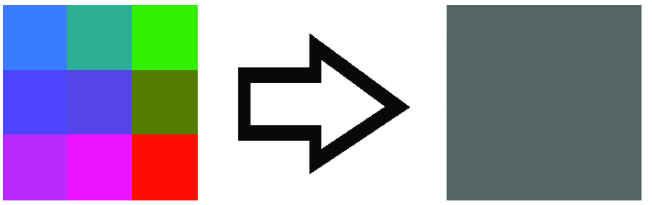


Figure 11. Correlation between the HSV colour system and the RGB colour system.

5. Grayscale Conversion: Creating grayscale images makes processing images easier because Colour data is eliminated and each pixel in an image observes only one intensity level. The images of forgery can be detected using grayscale images to narrow down on the dissimilarities between the original and forged images in terms of structure and luminance. With this formula :(0.299) red + (0.587) green + (0.114) blue as in Figure 12.



(a) RGB pixels. (b) Grayscale pixels.

Figure 12. RGB pixel to grayscale pixel converter

D. Visualization of Results

Original image plot and forged image plot and difference in hue image of original and forged image, grayscale histogram of original image, RGB histogram of original image, and HSV histogram of original image.

E. Calculate MSE and SSIM of original and forged images:

Mean Squared Error (MSE) and Structural similarity Index (SSIM) would be computed in order to quantitatively measure the difference between the original and forged image. When assessing the quality and usefulness of different forgery detection methods, it would be necessary to adopt powerful assessment metrics that offer information on the quality and sameness of photographs.

Mean Squared Error (MSE) is an often-applied measure of the difference that exists between two images. It is a computation of an average of squared differences between similar pixel intensities in the original and the forged image. MSE is mathematically defined as:

$$MSE = \frac{1}{N}\sum_{i=1}^{N} \left(I_{Original}(i) - I_{Forged}(i)\right)^2 \quad (1)$$

where $I_{Original}(i)$ $I_{Forged}(i)$ represent the pixel intensities of the original and forged images, respectively, and NN is the total number of pixels. MSE value between 0 and ∞, so a lower MSE value indicates a smaller difference between the original and forged images, implying higher similarity.

Structural Similarity Index Measure (SSIM) is a perception-based metric that measures the similarity between two images, taking into account luminance, contrast, and structure. Unlike MSE, SSIM considers the human visual system's characteristics.

SSIM is calculated by comparing three components: luminance (ll), contrast (cc), and structure (ss). The overall SSIM index is computed as the product of these components:

$$SSIM(X,Y) = \frac{2\,\mu_X * \mu_Y + C_1}{\mu_X^2 + \mu_Y^2 + C_1} * \frac{2\,\sigma_{XY} + C_2}{\sigma_X^2 + \sigma_Y^2 + C_2} * \frac{2\,\sigma_{XY} + C_3}{\sigma_X + \sigma_Y + C_3} \quad (2)$$

where μ_x, μ_y, σ_x, σ_y, and σ_{xy} are the means and covariances of x and y, and C_1, C_2, and C_3 are constants to stabilize the division with weak denominator. SSIM values range from -1 to 1, with 1 indicating identical images [33].

3. Iteration

Repeat the above steps for each pair of original and forged images in the dataset, ensuring thorough analysis and detection of image forgeries.

4. Dataset

One of the most important components of verifying the validity of digital forgery detection techniques is the need for a set of standard data. Previous research trends on detecting image forgery were based on a standard data set to link images. Similarly, the proposed system is based on a set of data dedicated to this purpose, which is the Multi-Image splicingData Set (MISD) to detect image forgery. The database contains a different set of images from CASIA V1.0, which were merged into a single data set containing a set of realistic images in natural colours. It consists of 618 original images in JPG format and 300 multi-link images in JPG format with dimensions of 384 × 256 pixels[29] . They are divided into eight main categories: animals, architecture, portraits, plants, art, nature, indoor spaces, scenery, and texture. The sent images were created using the Figma program, which contributes to the process of processing different images. Table 1 showed the specifications of the proposed data set to detect image forgery.

Table 1: Specifications of multiple image splicing dataset [29].

Area	Computer Vision
More precise area	Image forgery detection Image forensics
File Format	JPG
Image Dimensions	(384 × 256)
Number of Image Categories	8 (scene,, texture,, architecture,, character,, plant,, art,, nature,, indoor and animal)
Count of Authentic Images	618
Count of Spliced Images	300
Total Ground Truth Masks	300

The MISD was organized into two folders, one for original images and the other for forged images. Subsequently, the pre-processing, visualization, and quality assessment steps were applied to these images using the code.

5. Results

We implemented the forgery detection techniques using MATLAB with the provided code on the Multiple Image Splicing Dataset (MISD) as following steps:

A. Forged Image by Addition

Images were identical, create a forged image by merging the original and another image as shown in Figure 13.

Figure 13. Adding image (Panda image) to original image to make forged image

B. Hue Difference Image

The huge difference image is a visualization that highlights areas where the hue (colour) of the forged image differs significantly from that of the original image.

It is computed by extracting the hue component from both the original and forged images and then calculating the absolute difference between them.

Areas of significant hue difference indicate potential regions of manipulation or forgery, such as colour alterations or additions as shown in Figure 14.

Figure 14. Hue difference between original image and forged image

C. Grayscale Histogram

Grayscale histograms provide insights into the distribution of pixel intensities in the images, representing their overall brightness and contrast.

Histograms for both the original and forged images are plotted, showing the frequency of pixel intensity values.

Differences in the histogram shapes or peaks may indicate areas where modifications have been made, affecting the brightness or contrast of the images as shown in Figure 15 as the x-axis of a grayscale histogram represents the intensity values of the pixels, typically ranging from 0 (black) to 255 (white) for 8-bit images. The y-axis shows the frequency or number of pixels with each intensity value

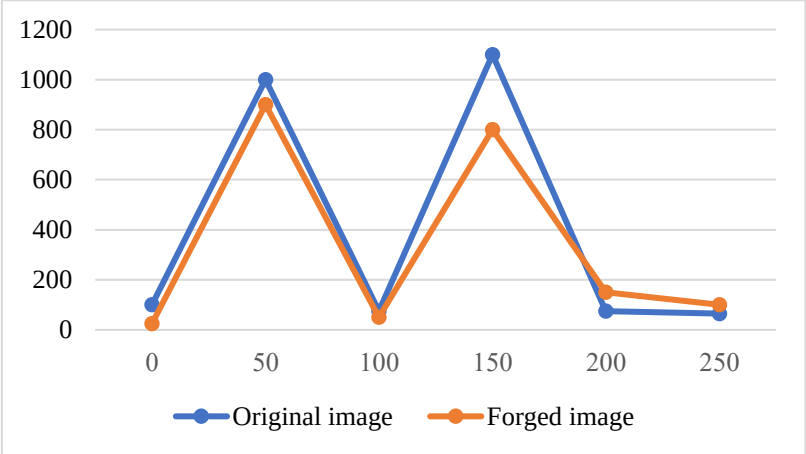


Figure 15. Grayscale histogram for original image (in Blue colour) and Forged image (in Red colour).

D. RGB Histogram

RGB histograms are generated separately for each colour channel (red, green, blue) in both the original and forged images.

These histograms illustrate the distribution of colour intensities across different colour channels, revealing potential alterations in specific colour components.

Variations in the histogram patterns or shifts in colour distribution may indicate manipulations or modifications in certain colour channels as shown in Figure 16.

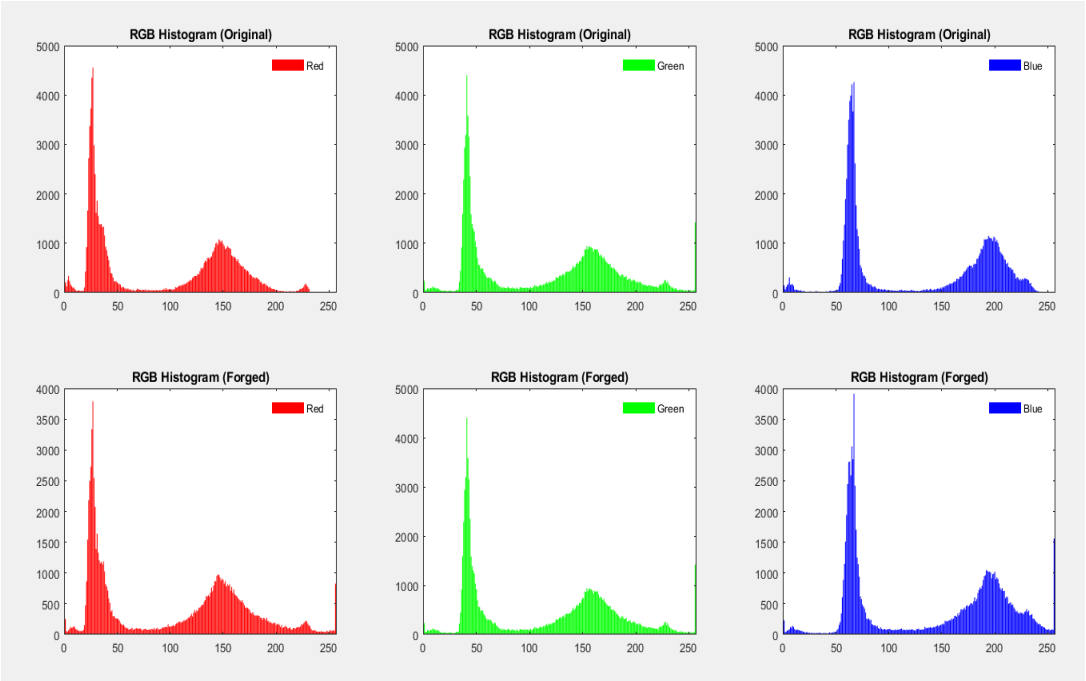


Figure 16. RGB histogram for each channel of RGB color in both original image and forged image.

E. HSV Histogram

HSV histograms depict the distribution of hue, saturation, and value components in the images. Similar to RGB histograms, HSV histograms provide insights into the colour characteristics of the images but in a different colour space.

Changes in the distribution of hue or saturation values may signal alterations in colour tones or saturation levels, suggesting possible forgery as shown in Figure 17. The X-axis: represents the values of the channels in the HSV colour space. Hue (H): Ranges from 0 to 179 in OpenCV (due to the 8-bit representation). Saturation (S): Ranges from 0 to 255.

Value (V): Ranges from 0 to 255. Besides, the Y-axis: represents the count of pixels in the image that correspond to each value on the X-axis. This indicates how many pixels exhibit that specific intensity for each channel.

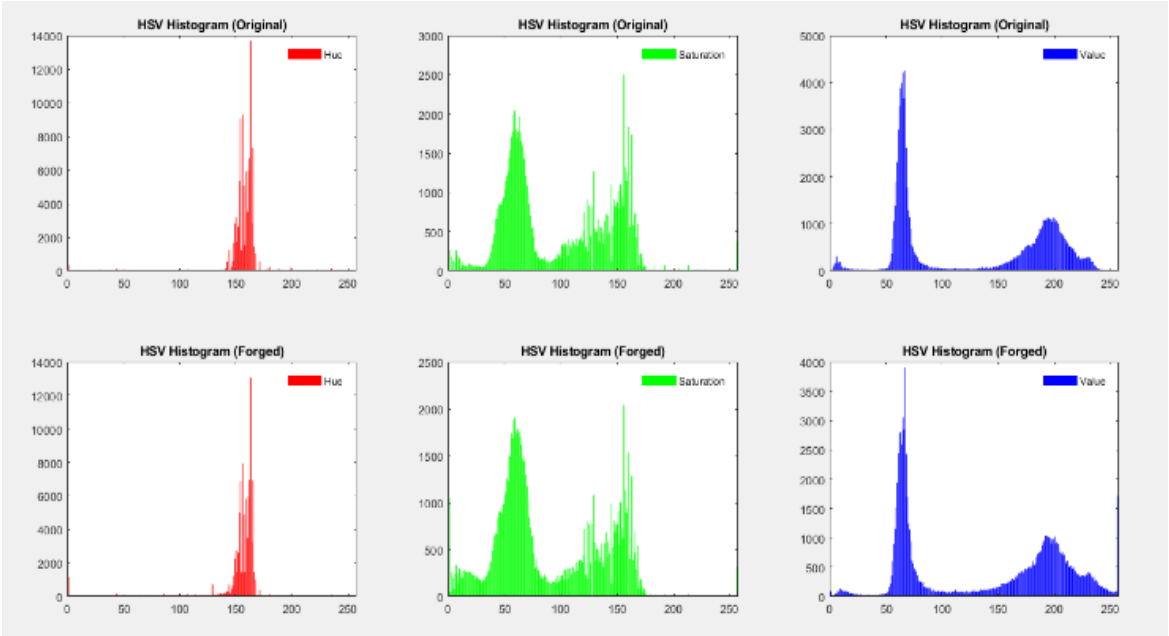


Figure 17. HSV histogram for each channel of HSV in both original image and forged image.

F. Difference Image and Suspicious Regions

The difference image is computed by calculating the absolute difference between the original and forged images.

Thresholding the grayscale difference image highlights areas where significant differences exist between the two images.

These suspicious regions indicate potential regions of interest where image manipulation or forgery may have occurred, guiding further investigation as shown in Figure 18.

Figure 18. Suspicious areas in forged image circled with the help of white colour.

G. Mean Squared Error (MSE): Structural Similarity Index (SSIM)

The detection algorithms used to detect forgeries in images are tested on a number of criteria as there is a need to evaluate their capabilities in detecting image forgeries. Here, we define the metrics that are employed to measure the performance of our forgery detection algorithm that are implemented with the help of the code as follows:

MSE is a metric that measures the mean squared distance between pixel values in the original and forged image and it is used to establish the overall difference in image. The lower value of MSE demonstrates that they are more similar. SSIM estimates the structural similarity of original and forged images basing on luminance, contrast and structure. The greater SSIM value is the greater the level of resemblance between the original and forged images. These measures will provide quantitative measures of the quality and similarity of the images together with qualitative analysis of the visualizations and histograms. Table 2 and Table 3 bellow demonstrate the implementation results:

Table 2: Quantitative results for splicing forgery

SSIM	MSE	Image pair
0.68	165.47	Splice_01
0.66	182.72	Splice_02
0.62	201.94	Splice_03
0.70	149.61	Splice_04
0.60	224.37	Splice_05

Table 3: Average results (splicing only)

Average value	Metric
184.82	Mean MSE
0.65	Mean SSIM

The implementation results of Table 2 and Table 3 above shows confirm that the image splicing introduces noticeable structural and intensity distortions in images. MSE effectively captures pixel-wise inconsistencies. SSIM highlights perceptual and structural degradation due to boundary artifacts. The combined use of MSE and SSIM provides a robust baseline evaluation for detecting splicing –based image forgeries in the MISD dataset. For splicing –only forgery detection, the MISD dataset experiments demonstrate:

- High MSE value (>180) indicate strong manipulation effects.
- Low SSIM value (~0.66) confirm reduce structural similarity.

Thus, MSE and SSIM are effective metrics for evaluating splicing forgeries, especially when used together.

6. Discussions

The metrics that we have evaluated (MSE and SSIM) are the most appropriate metrics to the task of evaluating the quality and similarity of images. In MSE, the degree of image similarity is given in quantitative terms, whereas in SSIM both structure and perceptual terms are taken into account with regard to image similarity.

The chosen metric results reflected that the Lower MSE values yield bigger conformity between the original and forged images, meaning that the featured forgery has been detected with low-level image deformity. Those values of SSIM which are higher indicate more similarity between the original and forged image which means proper detection of forgery and still maintains the quality of the image.

Limitations and factors to be considered during the proposed method are as follow, the MSE can fail to reflect the differences between the images visually and can be biased by the outliers. SSIM is based on the perceived human image and may not be objectively reflective of what the image contains.

7. Conclusion

The intended system will come up with a robust technology that will help in the detection of the forged images with advanced image processing method on a series of multiple image linkage datasets, which will show the improvement of accuracy in detecting image forgery. It clarified that the forgery detection in digital images is an immensely crucial area of study due to the significant advancement with the achievement of technology. Both the Hue difference image as well as the grayscale histograms showed that, there were significant differences in both the original and the forged images particularly in places where the manipulation or forgery could have taken place. RGB and HSV histograms also gave understanding of the colour distribution and properties of the images, which helped in the detection of suspicious areas. It was further confirmed that the techniques of forgery detection work by the difference between image and computed metrics (MSE and SSIM) by the fact that the lower the MSE and the higher the SSIM the closer the similarities in the images of both the original and the forged ones. The results of the forgery detection methods reveal the effectiveness of the methods of the forgery detection on detecting multiple image splicing forgery on the dataset of MISD. The findings and analysis bring in the development of the image forensics field and present invaluable information in the way of detection and identification of images forgery. Possible ways future works can go involve improved feature extraction through investigation with deep learning methods like CNNs and RNNs to carry out auto feature extraction to improve detection. Real-Time Detection Techniques: Explore real-time detection of image forgeries, which can be used to provide prompt response in various applications such a live streaming, video surveillance, etc. Future directions will involve the incorporation of deep learning models like convolutional neural networks to enhance further the accuracy of the detection accuracy, and implementation of real-time detection instruments in live streaming and video monitoring systems.

Funding: This research received no external funding

Conflicts of Interest: The author declare no conflict of interest.

References

[1] A. Khayeat, "Copy-move forgery detection in digital images," Ph.D. dissertation, Cardiff Univ., Cardiff, U.K., 2017.

[2] A. Cepak and T. J. Mesyn, "Fakes, forgery, and Facebook," in Handbook of Visual Communication, 1st ed., S. Josephson, J. D. Kelly, and K. Smith, Eds. New York, NY, USA: Routledge, 2020, pp. 465–480.

[3] S. M. Pizer et al., "Adaptive histogram equalization and its variations," *Computer Vision, Graphics, and Image Processing*, vol. 39, no. 3, pp. 355–368, 1987.

[4] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 3rd ed. Upper Saddle River, NJ, USA: Prentice-Hall Inc., 2007.

[5] D. G. Lowe, "Distinctive image features from scale-invariant keypoints," *International Journal of Computer Vision*, vol. 60, no. 2, pp. 91–110, 2004.
[6] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 4th ed. New York, NY, USA: Pearson Education, 2018.
[7] B. S. Kumar, S. Karthi, K. Karthika, and R. Cristin, "A systematic study of image forgery detection," *Journal of Computational and Theoretical Nanoscience*, vol. 15, no. 8, pp. 2560–2564, 2018.
[8] Kaur and J. Rani, "Digital image forgery and techniques of forgery detection: A brief review," *International Journal of Technical Research and Science*, vol. 1, no. 4, pp. 18–24, 2016.
[9] Q. C. Yang and C. L. Huang, "Copy-move forgery detection in digital image," in *Advances in Multimedia Information Processing – PCM 2009* (Lecture Notes in Computer Science, vol. 5879), P. Muneesawang et al., Eds. Berlin, Germany: Springer, 2009.
[10] V. Christlein, C. Riess, J. Jordan, and E. Angelopoulou, "An evaluation of popular copy-move forgery detection approaches," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 6, pp. 1841–1854, Dec. 2012.
[11] Tao, C. Li, J. M. Zain, and A. N. Abdalla, "Robust image watermarking theories and techniques: A review," *Journal of Applied Research and Technology*, vol. 12, no. 1, pp. 122–138, 2014.
[12] Fridrich, "Robust bit extraction from images," in *Proceedings of the IEEE International Conference on Multimedia Computing and Systems*, Florence, Italy, Jun. 1999, vol. 2, pp. 536–540.
[13] K. Doke and S. M. Patil, "Digital signature scheme for image," *International Journal of Computer Applications*, vol. 49, no. 16, pp. 1–6, 2012.
[14] B. Shwetha and S. V. Sathyanarayana, "Digital image forgery detection techniques: A survey," *ACCENTS Transactions on Information Security*, vol. 2, no. 5, pp. 22–31, 2017.
[15] C.-M. Pun, X.-C. Yuan, and X.-L. Bi, "Image forgery detection using adaptive oversegmentation and feature point matching," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1705–1716, Aug. 2015.
[16] Fridrich, D. Soukal, and J. Lukas, "Detection of copy-move forgery in digital images," in *Proceedings of the Digital Forensic Research Workshop (DFRWS)*, vol. 3, no. 2, pp. 652–663, 2003.
[17] Z. Zhang, C. Wang, and X. Zhou, "A survey on passive image copy-move forgery detection," *Journal of Information Processing Systems*, vol. 14, no. 1, pp. 6–31, 2018.
[18] R. Sekhar and R. S. Shaji, "A study on segmentation-based copy-move forgery detection using DAISY descriptor," in *Proceedings of the International Conference on Soft Computing Systems* (Advances in Intelligent Systems and Computing, vol. 398), L. Suresh and B. Panigrahi, Eds. New Delhi, India: Springer, 2016.
[19] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, San Diego, CA, USA, 2005, vol. 1, pp. 886–893.
[20] D. W. Scott, "Scott's rule," *WIREs Computational Statistics*, vol. 2, no. 4, pp. 497–502, Jul./Aug. 2010.
[21] Z. Xu, Y. Liu, S. Du, P. Wu, and J. Li, "DFOB: Detecting and describing features by octagon filter bank for fast image matching," *Signal Processing: Image Communication*, vol. 41, pp. 61–71, 2016.
[22] Zhang, Y. Li, S. Niu, Z. Cao, and X. Wang, "Improved fully convolutional network for digital image region forgery detection," *Computers, Materials & Continua*, vol. 60, no. 1, pp. 287–303, 2019.
[23] H. A. Jalab, T. Subramaniam, R. W. Ibrahim, H. Kahtan, and N. F. M. Noor, "New texture descriptor based on modified fractional entropy for digital image splicing forgery detection," *Entropy*, vol. 21, no. 4, p. 371, 2019.
[24] B. Ahmed, T. A. Gulliver, and S. alZahir, "Image splicing detection using Mask R-CNN," *Signal, Image and Video Processing*, vol. 14, no. 5, pp. 1035–1042, 2020.
[25] M. Islam, G. Karmakar, J. Kamruzzaman, and M. Murshed, "A robust forgery detection method for copy–move and splicing attacks in images," *Electronics*, vol. 9, no. 9, p. 1500, 2020.
[26] H. Siddiqi et al., "Image splicing-based forgery detection using discrete wavelet transform and edge weighted local binary patterns," *Security and Communication Networks*, vol. 2021, Art. no. 4270776, 2021.
[27] X. Bi, Z. Zhang, Y. Liu, B. Xiao, and W. Li, "Multi-task wavelet corrected network for image splicing forgery detection and localization," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME)*, Jul. 2021, pp. 1–6.

[28] Habibi and H. Hassanpour, "Splicing image forgery detection and localization based on color edge inconsistency using statistical dispersion measures," *International Journal of Engineering*, vol. 34, no. 2, pp. 443–451, 2021.
[29] D. Kadam, S. Ahirrao, and K. Kotecha, "Multiple image splicing dataset (MISD): A dataset for multiple splicing," *Data*, vol. 6, no. 10, p. 102, 2021.
[30] M. Hosny, A. M. Mortda, N. A. Lashin, and M. M. Fouda, "A new method to detect splicing image forgery using convolutional neural network," *Applied Sciences*, vol. 13, no. 3, p. 1272, 2023.
[31] H. Ding, L. Chen, Q. Tao, Z. Fu, L. Dong, and X. Cui, "DCU-Net: A dual-channel U-shaped network for image splicing forgery detection," *Neural Computing and Applications*, vol. 35, no. 7, pp. 5015–5031, 2023.
[32] Dammak, M. Mejdoub, and C. Ben Amar, "Histogram of dense subgraphs for image representation," *IET Image Processing*, vol. 9, no. 3, pp. 184–191, 2015.
[33] H. Mohammed, D. H. Badr, and F. Ali, "Detection of image forgery using information standard method with SVM," *Journal of Physics: Conference Series*, vol. 1818, no. 1, p. 012212, 2021.