Computers, Materials & Continua
DOI:10.32604/cmc.2022.021047
Article

Tech Science Press

Efficient Forgery Detection Approaches for Digital Color Images

Amira Baumy[1], **Abeer D. Algarni**[2,*], **Mahmoud Abdalla**[3], **Walid El-Shafai**[4,5], **Fathi E. Abd El-Samie**[3,4] **and Naglaa F. Soliman**[2,3]

[1]Department of Communications, High Institute for Engineering and Technology, Al-Obour Obour City, Egypt
[2]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia
[3]Department of Electronics and Communications Engineering, Faculty of Engineering, Zagazig University, Zagazig, Sharqia, 44519, Egypt
[4]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menoufia, 32952, Egypt
[5]Security Engineering Lab, Computer Science Department, Prince Sultan University, Riyadh, 11586, Saudi Arabia
*Corresponding Author: Abeer D. Algarni. Email: adalqarni@pnu.edu.sa

Received: 21 June 2021; Accepted: 08 September 2021

Abstract: This paper is concerned with a vital topic in image processing: color image forgery detection. The development of computing capabilities has led to a breakthrough in hacking and forgery attacks on signal, image, and data communicated over networks. Hence, there is an urgent need for developing efficient image forgery detection algorithms. Two main types of forgery are considered in this paper: splicing and copy-move. Splicing is performed by inserting a part of an image into another image. On the other hand, copy-move forgery is performed by copying a part of the image into another position in the same image. The proposed approach for splicing detection is based on the assumption that illumination between the original and tampered images is different. To detect the difference between the original and tampered images, the homomorphic transform separates the illumination component from the reflectance component. The illumination histogram derivative is used for detecting the difference in illumination, and hence forgery detection is accomplished. Prior to performing the forgery detection process, some pre-processing techniques, including histogram equalization, histogram matching, high-pass filtering, homomorphic enhancement, and single image super-resolution, are introduced to reinforce the details and changes between the original and embedded sections. The proposed approach for copy-move forgery detection is performed with the Speeded Up Robust Features (SURF) algorithm, which extracts feature points and feature vectors. Searching for the copied partition is accomplished through matching with Euclidian distance and hierarchical clustering. In addition, some pre-processing methods are used with the SURF algorithm, such as histogram equalization and single-mage super-resolution. Simulation results proved the feasibility and the robustness of the pre-processing step in homomorphic detection and SURF detection algorithms for splicing and copy-move forgery detection, respectively.

Keywords: Image forgery; splicing algorithm; copy-move algorithm; histogram matching; homomorphic enhancement; SISR; SURF

1 Introduction

Security of the image content in the modern multimedia system is an issue of the primary concern of researchers in the last decade. Security of image content can be accomplished through several strategies such as watermarking, encryption, steganography, and image forgery detection. The basic idea of watermarking [1,2] and steganography [3,4] is to hide a secret message, signal, or image; in a cover image for conveying valuable information or owner copyright protection. The recent forgery detection algorithms [5–8] can be classified according to the types of image forgery. The most common algorithms are splicing algorithms and copy-move algorithms. These algorithms depend on different approaches such as Discrete Wavelet Transform (DWT), Local Binary Pattern (LBP), and Scale Invariant Feature Transform (SIFT).

The main contribution of the paper is to apply the pre-processing techniques on the images before extracting the features and develop robust forgery detection methods for splicing and copy-move forgery attacks based on simple signal processing tools. The remainder of this paper is organized as follows. Section 2 introduces a related work to review the types of forgery and technologies used in image forgery detection. Section 3 illustrates the proposed pre-processing algorithms that are used to enhance the image and detection accuracy. Section 4 presents an efficient blind technique based on homomorphic transform for splicing forgery detection and a robust method to identify the forged regions in copy-move images using SURF key-point extraction. Section 5 presents the experimental results and performance evaluation. Finally, Section 6 introduces the concluding remarks and future works.

2 Related Work

Forensics is the science of discovering any attempts to change some sort of original data or images. Image forensics, which is the topic of our interest, includes changing the contents of digital images in an unauthorized manner. Image forensics analysis aims at discovering some forgeries in images, such as splicing forgery, copy-move forgery, and retouching forgery. So, forgery detection techniques aim to discover the existence of forgery manipulations. Different approaches have been adopted for forgery detection, such as passive and active approaches [8–10]. Active forgery detection techniques work on the principles of embedding external information in the image, such as a watermark [11–13] or a digital signature [14–16]. Verification is performed through the detection of the watermark or signature.

The technique presented in [11] inserts the Computer-Generated Hologram (CGH) from the marked image into the host image. The CGH is defined as a numerical simulation of the natural phenomena of light interference and diffraction. Resizing operation is performed on the mark image according to two steps. First, the mark image is resized by a factor (1/64), then it is magnified to the size of the host image by adding zeros. Then, the Fourier transform is applied to the resized mark image to get the CGH.

The algorithm in [12] decomposes the image into RGB components and applies 2-DWT for each component in the original image and mark image. The watermarked component is produced from the low-frequency components for the original image and mark image. Then inverse wavelet transform is used to produce the watermarked image. The watermark in [13] is obtained from the halftone model of the original image, and then it is inserted in the transform domain of the original image. Both DWT and Discrete Cosine Transform (DCT) are used to generate the watermarked image.

As mentioned before, the second type of active technique depends on a digital signature. The technique in [14] produces a hash image with a Secure Hashing Algorithm (SHA-1) applied to the original image. Then, the hash image is encrypted by the Reed-Solomon Algorithm (RSA), a public-key algorithm, to get the signature. The length of the signature word equals 64 bytes. In parallel with the previous steps, the original image is encoded by Reed-Solomon (RS) code, and the signature is added to the encoded image to produce the encrypted image. Moreover, the technique enhances the randomness of the encrypted image using a chaotic logistic map.

The algorithm in [15] divides the image into a fixed number of blocks equal to 32 blocks for a row and 32 blocks for a column. For any image, the length of blocks is changed, but the number is fixed. Next, a matrix of means for all blocks is calculated in a row direction and column direction. Then, the final signature is created from the XOR function applied to the two matrixes. The method in [16] extracts the low-frequency wavelet component from the image, and then an adaptive Harris corner detector is applied to get the feature points. For each feature point, the mean and variance are calculated from its neighborhood, and the signature matrix is composed of the point feature coordinates and their mean and variance.

Passive forgery detection techniques depend on the signal or image itself for the detection of forgery. Similarity tools in statistics can be utilized with these techniques. Several studies have introduced a general survey [17–25] for different types of forgery techniques. In the copy-move technique [26–34], the copied parts share characteristics such as lighting conditions, background, and dynamic range with the rest of the images. So, forgery detection becomes more difficult. Several techniques have been investigated to detect the copy-move forgery. These techniques are classified into block-based techniques or key-point-based techniques [19]. Several algorithms start with preprocessing steps such as conversion between color systems, image enhancement, or noise removal. The feature extraction technique is the only difference between all approaches. The feature vectors should ensure a good representation of the images without losing any data. Then, matching is performed to get the duplication region by finding a high similarity between feature vectors.

The key-points-based techniques such as SIFT [26–28] and SURF [29,30] are used to reduce the computational complexity. These techniques are not affected by scaling, rotation transformations and are robust to noise. SIFT key-point descriptors are used in [26] as feature vectors. Copy-move detection is improved in [27] by using local phase quantization to extract the texture information from the image before applying the SIFT. The DyWT decomposes the image, and then SIFT transform is applied on the LL sub-band to extract the feature descriptors [28].

The dimension of the SIFT key-point feature vector is (1 × 128). So, the computational cost is slow. The use of integral images with a SURF key-point descriptor makes the computation of the descriptor faster than SIFT descriptor only, and the dimensions of the feature vector become (1 × 64). So, modern researches are directed to the use of SURF key points. SURF key points features are extracted, and their descriptors are matched with each other.

Many matching techniques have been investigated in the literature, such as Euclidean distance [31], KD tree, and nearest neighbor. An agglomerative hierarchical clustering [32] is applied to the spatial locations of the matched points. The splicing forgery detection techniques aim at discovering the sudden changes between image parts. The algorithm in [33] has been presented to identify the change in the illuminant colors. A grey-world algorithm is used to estimate illuminant sub-bands, and a comparison is performed between them to locate the forged regions. The image [34] is converted from RGB to YCbCr components, and the chrominance component is divided into overlapping blocks. An LBP is calculated for each block, and then the DCT transform is applied on the resulting LBP blocks. Finally, the standard deviations are calculated for each block to build the feature vector.

3 The Proposed Pre-Processing Techniques for Image Enhancement

Image enhancement techniques are used in a pre-processing step in many applications such as medical and satellite image processing [35–37]. Also, image enhancement can be used for forgery detection. It is used to increase the contrast between original and copied parts in any section of the image. The assumption upon which the enhancement is used in forgery detection is that any copied section in the image has a different illumination for that of the background.

Image enhancement methods can be classified into spatial-domain and transform-domain methods [35–38]. Spatial-domain methods depend on the direct manipulation of the pixels in the image. Transform-domain methods are used to enhance an image by processing in the selected transform domain. Spatial domain techniques are superior from the ease of implementation and speed perspectives. Therefore, only spatial-domain processing techniques will be discussed in this paper. Spatial-domain processing [35] is classified into point processing and mask processing. Point processing deals with the individual pixels only. It does not utilize the relation between pixels in the image. Unlike point processing, mask processing estimates the new pixel value from its original and neighborhood pixels.

This section is devoted to the pre-processing techniques applied to the images before extracting the features to improve the forgery detection algorithms. As mentioned in the literature review, pre-processing is necessary for image forgery detection because it enhances the contrast between original and forged sections. We will develop efficient pre-processing techniques for forgery detection. These techniques include the utilization of high-pass filtering with histogram equalization, the combination between single image super-resolution and histogram equalization, and the decomposition with additive wavelet transform (AWT) and homomorphic image enhancement.

3.1 High-Pass Filtering and Histogram Equalization

This technique combines two stages: the high-pass filter and the histogram equalization [39]. First, the image passes through the 2-D high-pass filter. Then, the high-pass filter detects the new high-contrast pixel values by processing the incoming image with a 3 × 3 convolution mask. The resulting images are sharper and contain more details. Eq. (1) shows the mask of the high-pass filter used in the proposed algorithm. The sum of the coefficients in a sharpening operator is also commonly taken to preserve amplitudes in regions of constant gray levels.

$$The\ \ mask = \begin{bmatrix} 0 & -1 & 0 \\ -1 & 5 & -1 \\ 0 & -1 & 0 \end{bmatrix} \tag{1}$$

After that, the histogram of the resulting image from the first stage is stretched through the spectrum (0 – 255) to increase the contrast of the images and provide more details. The normalized histogram can be estimated by the probability density function PDF mentioned in [39].

3.2 *Single Image Super-Resolution and Histogram Equalization*

The undesired motion may occur on the medium between the imaging system and the scene in many cases. This motion produces shifts between pixels and generates a low-resolution image. The missing information can be obtained from the generation of a high-resolution image. Also, several techniques are based on the assumption that the available low-resolution input images are produced by warping, blurring, or down-sampling of the high-resolution scene. High-resolution images are used in several applications such as medical image processing, satellite, and aerial imaging, fingerprint image enhancement, iris recognition, and text image enhancement.

Super-resolution techniques are classified into two categories: multiple image super-resolution and example-based super-resolution. Multiple image super-resolution techniques depend on combining several images, and each image has different information of the same scene. Example-based super-resolution techniques have databases formed by the correspondence between low- and high-resolution image patches. These techniques apply the learning rules between patches to find the missing data. The scaling up of the images leads to more image details by adding more pixels predicted by their neighbors.

The main idea adopted in the Single Image Super-Resolution (SISR) algorithms is to use only the low-resolution images available [40,41]. This means that the algorithm can generate a high-resolution image without the need for an external database. Super-resolution [40] needs only the original low-resolution image and its blurred versions. In this type of algorithm, first the image is up-sampled with bicubic interpolation, the algorithms depend on the down-sampled version and the deblurred version to obtain the required high-resolution image. Finally, Gaussian Process Regression (GPR) is used as a predictor for the new high-resolution image. The choice of the proper covariance function provides soft clustering of pixels for improvement of the edge recovery. The details of the single-image super-resolution technique are indicated in [40]. It aims to increase the number of extracted features in test images. Increasing the resolution of an image gives more key points. So, the small-size forged regions can be detected. Also, good descriptors are obtained to improve the matching process. The block diagram of the proposed model is illustrated in Fig. 1. It combines histogram equalization and SISR in the pre-processing step.

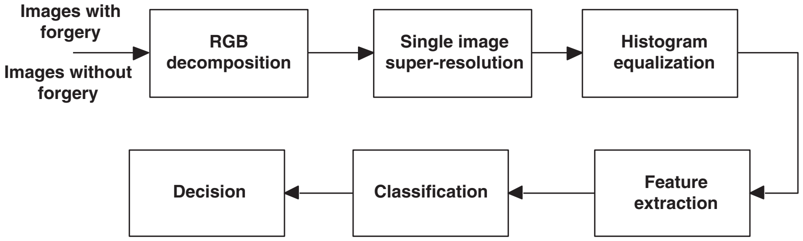

Figure 1: Super-resolution with histogram equalization

3.3 *Homomorphic Enhancement with Additive Wavelet Transform*

A pre-processing technique based on the AWT is proposed for image enhancement. This technique begins with the decomposition of images by the AWT and then applies the homomorphic transform on each sub-band, as shown in Fig. 2. Next, the AWT decomposes the image into different sub-bands, and each sub-band is enhanced with the homomorphic algorithm [42]. In the final step, these homomorphic enhanced sub-bands are subjected to an inverse additive wavelet transform to get an image with better visual details. The homomorphic filtering technique is one of the most common ways used to improve the quality of digital images. It has been used in many imaging applications such as medical applications and robotic vision [39,42,43].

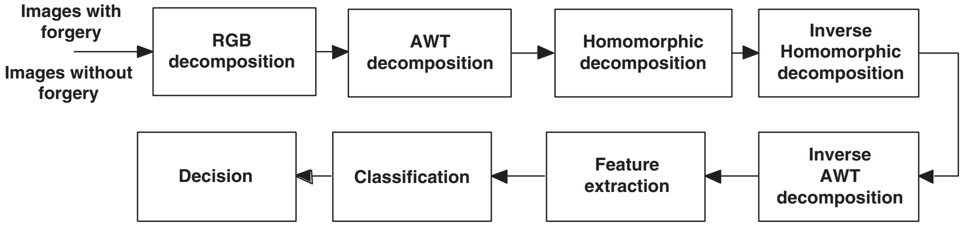

Figure 2: The homomorphic enhancement pre-processing technique

The steps of the enhancement method are shown in Fig. 3 and can be explained as follows [44]:

1) The images are decomposed into R, G, B color channels.
2) For each channel, the wavelet sub-bands $w_1, w_2, w_3, \ldots, w_n$ contain the detailed high-frequency components, and the approximation low-frequency component $I_{N\ \text{is}}$ generated.
3) For each wavelet sub-band, the illumination and reflectance components are separated using a logarithmic operation.
4) The reflectance and the illumination components are multiplied with α, and β, respectively, where $\alpha > 1$ and $\beta < 1$.
5) An exponential function is applied to reconstruct each sub-band and then reconstruct the enhanced image.

4 Proposed Forgery Detection Algorithms

4.1 Proposed Splicing Forgery Detection with Homomorphic Technique

The proposed technique aims at discriminating between the original and forgery images. It extracts the features from the histogram derivative for the illumination components. The homomorphic filtering separates the low-frequency illumination components from the high-frequency reflectance components of the image. This filtering technique can be implemented by applying a logarithm operation on the image to change the multiplication relation of illumination and reflectance to a sum relation.

The illumination components can be separated using a low-pass filter applied on the logarithm of the image intensity as indicated in [39,42]. On the other hand, the reflectance components can be produced using a high-pass filter. Firstly, the illumination histogram for authentic and forged images is differentiated, and then the Probability Density Functions (PDFs) are estimated for peaks of histogram derivatives for a set of images. Finally, the threshold is determined based on the PDFs for the histogram derivative peak distributions in the presence and absence of forgeries. The proposed technique relies heavily on determining the PDFs for each separated channel in two color models: IHS and RGB, and specifies the most sensitive channel for forgeries. The proposed model is implemented in two phases: the training phase and the testing phase.

The proposed model can be implemented through the following steps.

1) Choosing the training dataset and specifying the color system.
2) Selection of original and tampered images from the dataset.
3) Taking the logarithm of the image intensity.
4) Getting the illumination components by utilization of a low-pass filter.

5) Estimating the illumination histogram.
6) Determining the absolute maximum of the derivative of the illumination histogram.
7) For each set of the original and tampering images, the PDFs of the absolute peaks of the derivative histogram are estimated separately.
8) Determining the forgery detection threshold.
9) Testing this threshold with the testing dataset to obtain the performance of the proposed model.

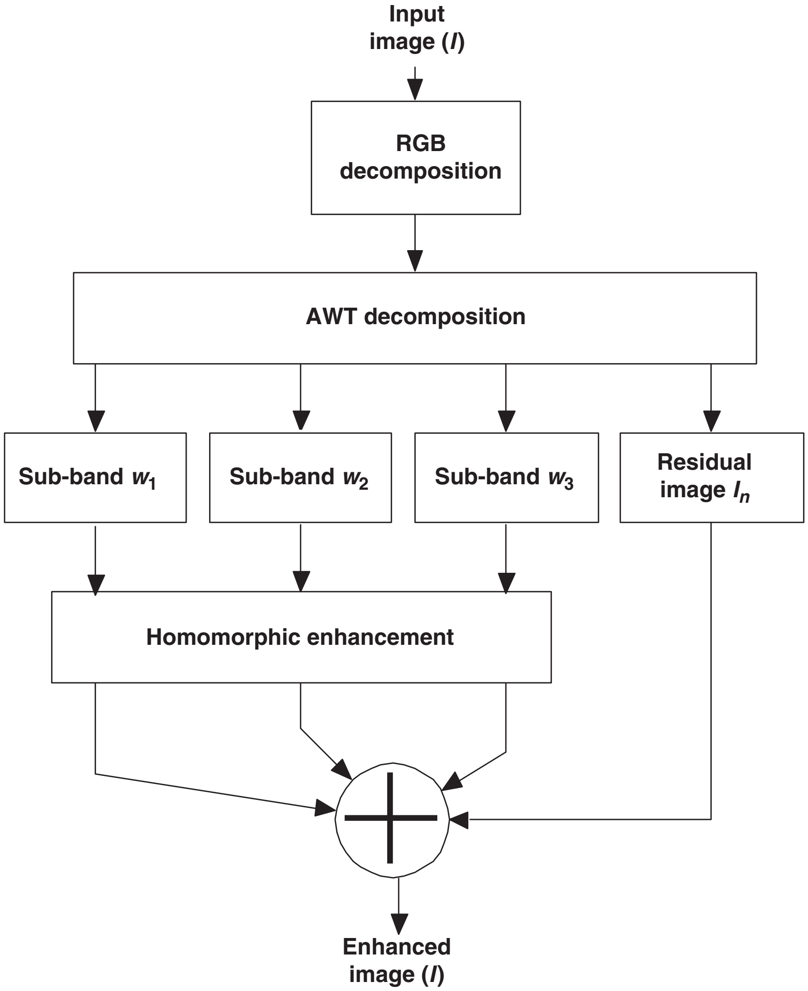

Figure 3: The block diagram of the AWT enhancement

4.2 Proposed Copy-Move Forgery Detection with Pre-Processing and Speeded Up Robust Features Key-Points

In this section, the SURF key points are utilized for the copy-move forgery detection. In addition, the Histogram equalization (HE) and SISR are applied as pre-processing techniques to improve the images before extracting the SURF key points to improve the copy-move forgery detection.

SIFT is used for extracting the distinguishing invariant features from the images. The SIFT features present a powerful tool in many applications, such as reliable matching between different views of a 3-D scene and object recognition in computer vision. Furthermore, SIFT transform provides robust, reliable features to photometric changes such as scaling, rotation, distortion, and addition of noise. There are four main steps for extracting SIFT features: scale-space extrema detection, key-point localization, orientation assignment, and key-point descriptor. In this paper, the SURF technique is used for reducing the time cost of computations and feature matching, which is the main advantage of using it. More explanation of the SURF is provided in [29].

Fig. 4 introduced the block diagram of the proposed model that aims to increase the number of extracted features in test images. Increasing the resolution of an image gives more key points. So, the small-size forged regions can be detected. Also, good descriptors are obtained to improve the matching process.

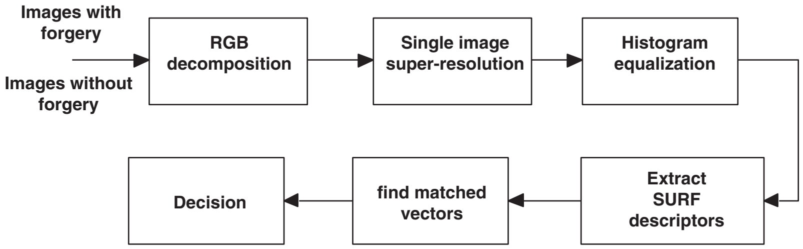

Figure 4: The proposed SURF-based technique for forgery detection

The matching process for a test image is performed as follows; a set of key-points $S=\{s_1, s_2, s_3, \ldots, s_n\}$ with their corresponding SURF descriptors $F\{f_1, f_2, f_3, \ldots, f_n\}$ is extracted. Then, a matching process is performed in the SURF space among the vectors F of each key-point to identify similar local patches in the test image.

Euclidean distance [44] is proposed to find the best candidate match for each key point. Similar local patches are determined with minimum Euclidean distance and minimum threshold (th_1) [45]. The threshold (th_1) lies between 0 and 1. If th_1 is set to a value closer to 0, the results will be highly corrected but with fewer matches. If th_1 is set to a value closer to 1, the results will have more matches, but they will be lower correct, increasing the number of false matches. The Euclidean distance is defined by:

$$d(q,p) = \sqrt{(q_1 - p_1)^2 + (q_2 - p_2)^2 + \ldots (q_n - p_n)^2} \tag{2}$$

So, agglomerative hierarchical clustering is used to neglect the false matches and find the matched descriptors. Then, groups of close descriptors are combined together. The hierarchical clustering (HC) algorithm [46] starts by assigning each key point to a cluster; then, it computes all the reciprocal spatial distances among clusters, finds the closest pair of clusters, and finally merges them into a single cluster. Such computation is repeated until a final merging scenario is achieved. Then, the matching process is performed on clusters.

5 Simulation Results and Performance Evaluation

5.1 Simulation Setup

Two datasets have been used to test the proposed homomorphic algorithm. The first is a realistic database composed of 70 original images and 70 tampered images. Images are subdivided into the training data consisting of 15 original images and 15 tampered images. The testing data contains 55 original images and 55 tampered images. The Photoshop program has been used to generate the tampered images. The tampered images have been generated by tacking a copy of an image part from an image and pasting this part into another image.

The second database is CASIA 2.0 v2 [47]. This database contains samples of spliced color images of different sizes. It comprises 120 original images and 120 tampered images sub-divided into 20 original images and 20 tampered images for training and 100 original images and 100 tampered images for testing.

5.2 Performance Evaluation for Image Splicing Forgery Detection Algorithm

In the first simulation experiment, each RGB and IHS system have examined the proposed detection algorithm. The performance of the proposed model has been determined by the calculation of the True Positive Rate (TPR), which is defined as the sensitivity, the True Negative Rate (TNR), which is defined as the specificity, the False Positive Rate (FPR), and the Accuracy. These metrics are estimated with Eqs. (3)–(6). Sensitivity is related to the ability of the algorithm to detect a tampered image correctly as being tampered. Specificity is associated with the ability of the algorithm to identify an authentic image correctly as authentic. Hence, high values of sensitivity and specificity imply the better performance of the system, where:

- *TP* (True Positive): Tampered image successfully detected as being tampered.
- *FP* (False Positive): Authentic image detected as being tampered.
- *TN* (True Negative): Authentic image successfully detected as authentic.
- *FN* (False Negative): Forged image detected as authentic.

$$Sensitivity = \frac{TP}{TP + FN} \tag{3}$$

$$Specificity = \frac{TN}{TN + FP} \tag{4}$$

$$FPR = \frac{No.\ of\ original\ images\ detected\ as\ forged}{No.\ \ of\ original\ images} \tag{5}$$

$$\begin{aligned} Accuracy = \ & (No.\ \ of\ tampered\ images\ detected\ as\ being\ tampered \\ & +No.\ \ of\ original\ images\ detected\ as\ being\ original)/(No.\ of\ tampered\ images \\ & +\ No.\ \ of\ original\ images) \end{aligned}$$

A comparison among red, green, blue, and intensity channels for the manually obtained dataset is shown in Tab. 1. The red channel gives the highest accuracy, equals 90. A comparison among red, green, blue channels for the CASIA dataset is shown in Tab. 2. Blue channel achieves the highest accuracy of 74.5%.

Table 1: Comparison between red-green-blue channels and intensity channels on the first dataset

Channel	Sensitivity (%)	FPR (%)	Specificity (%)	Accuracy (%)
RED	85.45	5.4	94.5	**90**
BLUE	50.91	3.64	96.36	**73.6**
GREEN	76.36	5.4	94.5	**85.45**
INTENSITY	70.91	7.2	92.72	**81.8**

Table 2: Comparison between red-green-blue channels on the CASIA dataset

Channel	Sensitivity (%)	FPR (%)	Specificity (%)	Accuracy (%)
RED	68	32	68	**68**
BLUE	78	29	71	**74.5**
GREEN	70	33	67	**68.5**

In the second simulation experiment, the effect of pre-processing on the proposed detection algorithm is tested. Pre-processing techniques are utilized to enhance the visual quality of the image. In addition, it helps in forgery detection as the details of tampered regions in the images are reinforced. The pre-processing operations applied with the proposed model are High pass filter (HPF), HE, Histogram Matching (HM), and SISR.

The proposed enhancement approach for forgery detection has been tested on the CASIA dataset [47], and each channel of the RGB system has been used. A comparison between pre-processing techniques for forgery detection on the different channels is given in Tabs. 3–5. The feasibility of using different pre-processing techniques is illustrated in the results. The accuracy is increased with all pre-processing techniques except the high-pass filtering. The specificity with a blue channel is increased from 71% to 76%. This may be attributed to the smaller wavelength range of the green channel compared to the red and green channels, as shown in Fig. 5. This performance of the forgery detection process with high-pass filtering can be explained based on the idea of the operation of the high-pass filtering process. The high-pass filter can be used to make the image sharper and emphasize fine details in the image, but it attenuates the low-frequency components of the image, and it also amplifies noise. It is obvious to note that HE gives the highest accuracy from all tested techniques. The accuracy on the red channel is increased from 68% to 83%. The accuracy on the green channel is increased from 68.5% to 82.5%, and on the blue channel, from 74.5% to 82%. The reason is that the histogram equalization stretches the dynamic range of the image, and hence all details of forgery can be enlarged.

The high-pass filter and histogram equalization are combined together for the enhancement of the forgery detection process. Tab. 6 shows the effect of HPF with HE on red, green, blue channels for the second dataset [47]. The accuracy on the red channel is increased from 68% to 85.5%. All channels achieve close values of accuracy.

Table 3: Forgery detection results with pre-processing techniques on the red channel

Pre-processing on the red channel	Sensitivity (%)	FPR (%)	Specificity (%)	Accuracy (%)
Without pre-processing	68	32	68	68
High-pass filter	76	67	33	54.5
Histogram equalization	79	13	87	83
Histogram matching	79	17	83	81
Single image super-resolution	71	28	72	71.5

Table 4: Forgery detection results with pre-processing techniques on the green channel

Pre-processing on the green channel	Sensitivity (%)	FPR (%)	Specificity (%)	Accuracy (%)
Without pre-processing	70	33	67	68.5
HPF	71	44	56	63.5
HE	77	12	88	82.5
HM	84	20	80	82
SISR	71	31	69	70

Table 5: Forgery detection results with pre-processing techniques on the blue channel

Pre-processing on the blue channel	Sensitivity (%)	FPR (%)	Specificity (%)	Accuracy (%)
Without pre-processing	78	29	71	74.5
HPF	69	24	76	72.5
HE	79	15	85	82
HM	71	16	84	77.5
SISR	70	16	84	77

SISR is combined with HE as a pre-processing technique to enhance the forgery detection results. A comparison of forgery detection performance with and without pre-processing on red, green, and blue channels is given in Tab. 7. The accuracy of forgery detection on red, green, and blue channels indicates the effect of pre-processing; therefore, clear discrimination between the tampered and original images is provided. In addition, the combination between resolution enhancement and histogram equalization increased the accuracy of forgery detection from green, blue, and red channels to 79.5%, 80.5%, and 78.5% from 68.5%, 74.5%, and 68%, respectively.

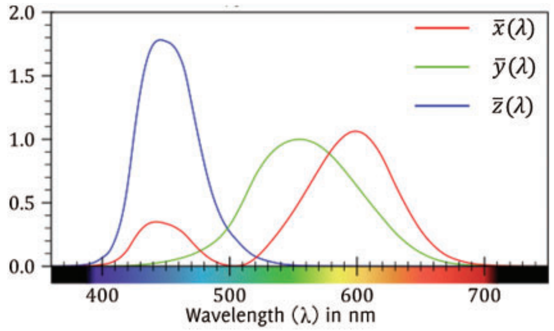

Figure 5: The wavelength range of red, green, and blue channels in the RGB color system

Table 6: Forgery detection results from all channels with the HPF and HE combined technique

Technique	Sensitivity (%)	Specificity (%)	AUC (%)	Accuracy (%)
Red channel without pre-processing	68	68	73.6	68
Red channel after HPF and HE	91	8	92.295	85.5
Green channel without pre-processing	70	67	73.66	68.5
Green channel after HPF and HE	84	86	92.455	85
Blue channel without pre-processing	78	71	79.745	74.5
Blue channel after HPF and HE	79	92	92.895	85.5

Table 7: Results of SISR and HE pre-processing technique on red, green, and blue channels

Technique	Sensitivity (%)	Specificity (%)	AUC (%)	Accuracy (%)
Red channel without pre-processing	68	68	73.6	68

(Continued)

Table 7: Continued

Technique	Sensitivity (%)	Specificity (%)	AUC (%)	Accuracy (%)
Red channel after SISR and HE	79	78	84.285	78.5
Green channel without pre-processing	70	67	73.66	68.5
Green channel after SISR and HE	75	84	85.2	79.5
Blue channel without pre-processing	78	71	79.745	74.5
Blue channel after SISR and HE	74	87	83.97	80.5

Finally, the homomorphic enhancement is tested in the AWT Domain for forgery detection. The simulation experiments have been performed on the blue channels with variable values of α and β as weighing factors of the enhancement process to test the performance of the proposed enhancement algorithm. The results of the experiments are given in Tab. 8. The range of β is started from 0.8 to 0.99, and the range of α starts from 1.2 to 2. Both sensitivity and specificity vary with the change of α and β. The accuracy is increased from 77% to 83.5%. The best results are obtained with β set to 0.99 and α set to 2.

After applying homomorphic enhancement in the AWT domain on each sub-band performance for red, green, and blue channels on the second dataset, the simulation results are given in Tab. 9. The accuracy results on the green, blue, and red channels indicate the proposed pre-processing benefit. The combination between AWT and homomorphic transform increases the accuracy values on red, green, and blue channels to 73.5%, 79%, and 83.5% from 68%, 68.5%, and 74.5%.

5.3 Performance Evaluation for Copy Move Based on SURF Forgery Detection Algorithm

The SURF-based algorithm has been evaluated on two datasets: MICC_F600 [48] and CoMoFoD [49]. MICC-F220 contains copy-move color images of different sizes. This database is composed of 110 original images and 110 tampered images. The CoMoFoD database consists of 40 original images and 200 tampered images. The size of the images is 512 × 512. This dataset has small size forgeries and multiple forgeries.

Fig. 6 shows the effect of different pre-processing techniques on the tampered image 002-F from the CoMoFoD database. The number of key points is increased from 192 using SURF without pre-processing to 6219 after applying histogram equalization and single-image super-resolution. Histogram equalization produces the largest number of discriminative key-points because it increases the contrast between pixels, as shown in Fig. 6c.

Tab. 10 introduces a comparison of applying HE, SISR, and a hybrid algorithm of HE and SISR for the number of extracted key points for four images in MICC_F600 datasets. It can be noted that the hybrid algorithm of HE and SISR gives a better investigation of key points. In addition, the performance of the hybrid algorithm has been tested on 40 images selected from the CoMoFoD database. Finally, the TPR is measured as shown in Tab. 11. The results prove that the combination of histogram equalization and single-image super-resolution enhances the TPR from 57.5% to 85%.

Table 8: Effect of changing β and α on the forgery detection performance from the blue channel

Values of β and α	Sensitivity (%)	Specificity (%)	AUC (%)	Accuracy (%)
β=0.8, α=1.2	80	74	81.2	77
β=0.99, α=1.5	74	86	85.14	81
β=0.99, α=1.7	78	86	85.6	82
β=0.99, α=1.8	76	87	86	81.5
β=0.99, α=2	83	84	87	83.5

Table 9: Forgery detection results with and without homomorphic enhancement in the AWT domain from all channels

Forgery detection method	Sensitivity (%)	Specificity (%)	AUC (%)	Accuracy (%)
Red channel without pre-processing	68	68	73.6	68
Red channel after homomorphic enhancement in the AWT domain	64	83	0.77	73.5
Green channel without pre-processing	70	67	73.66	68.5
Green channel after homomorphic enhancement in the AWT domain	73	86	83	79
Blue channel without pre-processing	78	71	79.7	74.5
Blue channel after homomorphic enhancement in the AWT domain	83	84	87	83.5

The copied part in the image may be rotated, scaled, and modified before being pasted in another region. The SURF algorithm is tested against rotation, scaling, distortion, and combination between these operations, as shown in Fig. 7. It is clear that the pre-processing gives more reliable results with each operation. The overall accuracy is calculated for two datasets, and the results are shown in Fig. 8. The accuracy on the MICC_F220 dataset is 99%, and the accuracy on the CoMoFoD database dataset is 92.5%.

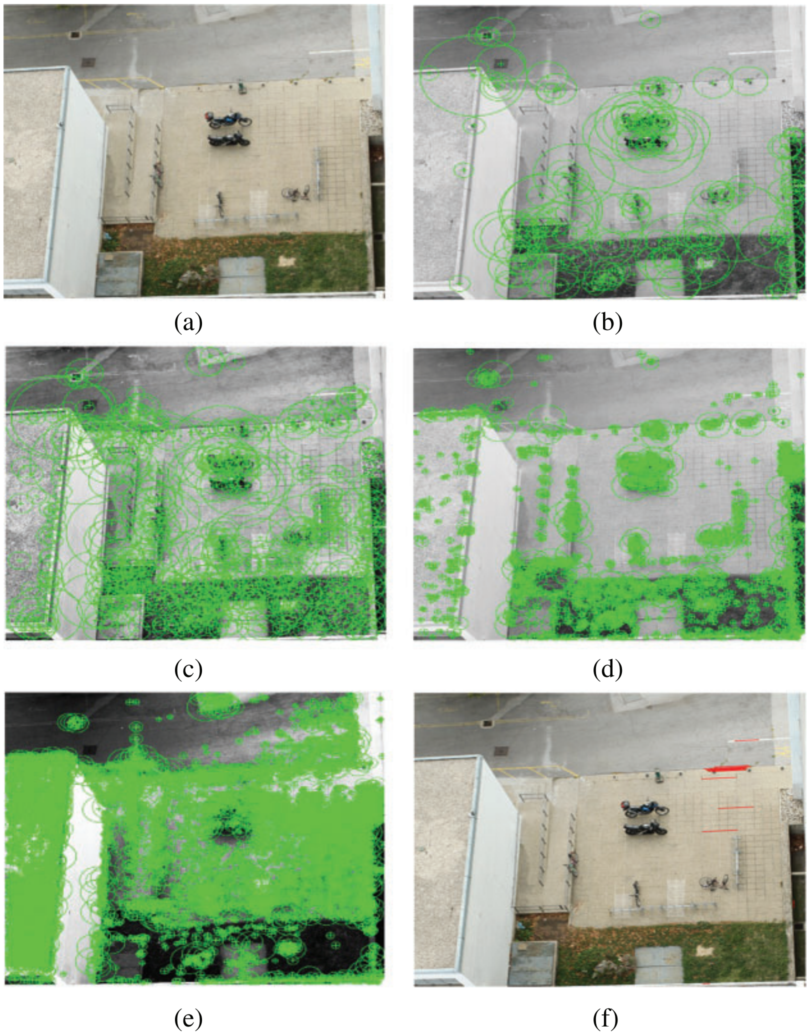

Figure 6: Key-points extraction from an image with forgery (002-F) from CoMoFoD database (a) The image with forgery (002_F), (b) SURF key-points, (c) Key-points after HE, (d) Key-points after SISR, (e) Key-points after HE and SISR, (f) The MH features

Table 10: Comparison between numbers of key-points at different pre-processing algorithms

Test images	Number of key-points			
	Without pre-processing	After HE	After SISR	After HE and SISR
Image 002_F	192	724	1812	6219
Image 026_F	555	1280	2208	7726
Image 009_F	131	188	327	2294
Image 005_F	267	463	1530	6818

Table 11: TPR values of the proposed SURF-based technique for 40 images

Pre-processing algorithm	TPR (%)
without pre-processing	57.5
HE	75
SISR	73
HE and SISR	85

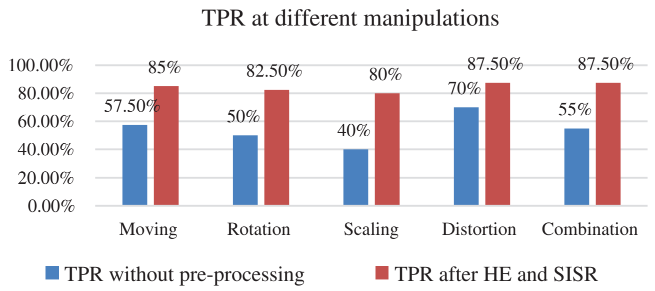

Figure 7: Comparison of SURF-based forgery detection with and without pre-processing in the presence of some manipulations of copied areas

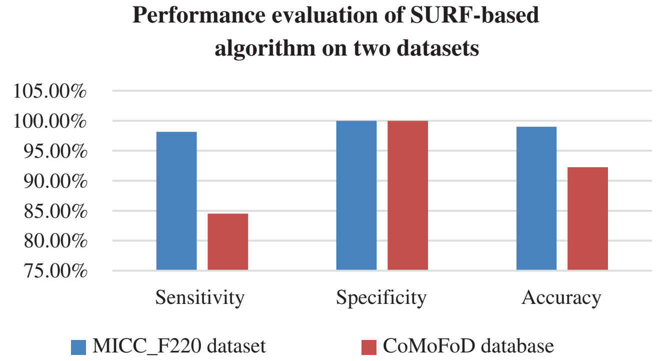

Figure 8: Performance evaluation of the proposed SURF-based algorithm on two different datasets

6 Conclusion and Future Work

The main motivation behind this research was the enhancement of image forgery detection performance. This paper discussed two types of image forgery algorithms: copy-move forgery and splicing forgery. These algorithms presented effective and robust models to discriminate between tampered images and authentic images. The enhancement based on pre-processing stages is used to reinforce the details of the images before the forgery detection process. The detail reinforcement process can achieve high classification accuracy. In this paper, high-pass filtering, histogram equalization, resolution enhancement, and adaptive wavelet transform are used individually and in combination as pre-processing stages.

For the splicing forgery, image pre-processing and homomorphic enhancement presented an efficient image forgery detection model. The illumination component is semi-constant in normal images, and hence the histogram of the illumination is close to a single-valued histogram. Otherwise, if there is a forgery in the image, it is expected that due to making some mixes with the image, the lighting conditions may differ, and hence the illumination component may have abrupt changes that are reflected in its histogram as an abnormal change. Abnormal changes can be detected through the first-order derivative; however, there is no large effect on the reflectance component.

Different tampered and untampered image sets have been used for the test. The proposed algorithms have been tested using the different channels of the RGB system, and the detection threshold is determined for each. The blue channel gave the maximum detection accuracy of 74.5% for the proposed detection algorithm without pre-processing. Nevertheless, the detection accuracy became 85.5% after high-pass filtering and histogram equalization. High-pass filtering and histogram equalization pre-processing combined significantly affect the red channel results as the detection accuracy changed from 68% to 85.5%. Moreover, homomorphic enhancement in the AWT domain led to an accuracy of 100% from the red channel. The resolution enhancement pre-processing technique gave a small change in the detection accuracy, and the detection accuracy became 78.5%.

Image pre-processing and SURF-based feature extraction constituted a robust and effective image forgery detection model for the copy-move forgery. The HE and SISR are employed before extracting the SURF key-points to improve the accuracy of the copy-move forgery detection process. This strategy aims to increase the number of SURF key points to efficiently discover the copied regions. As a result, the true positive rate is improved from 64% to 85%. The true positive rate with pre-processing and SURF-based detection has been investigated against scaling, rotation, and distortion attacks.

In addition, histogram equalization and single-image super-resolution together with SURF-based detection achieved good results in the presence of copied segment manipulations. In future work, the proposed forgery detection algorithms can be examined for video and other multimedia data formats.

Acknowledgement: The authors would like to thank the support of the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University.

Funding Statement: This research was funded by the Deanship of Scientific Research at Princess Nourah Bint Abdulrahman University through the Fast-track Research Funding Program.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. Al-Afandy, W. El-Shafai, E. El-Rabaie, F. Abd El-Samie, O. Faragallah *et al.,* "Robust hybrid watermarking techniques for different color imaging systems," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25709–25759, 2018.

[2] M. Ramya, P. Soman and L. Deepthi, "A novel approach for image security using reversible watermarking," in *Proc. of IEEE Int. Conf. on Advances in Computing, Communications and Informatics (ICACCI)*, Udupi, India, pp. 338–343, 2017.

[3] N. Surse and P. Jani, "A comparative study on recent image steganography techniques based on DWT," in *Proc. of IEEE Int. Conf. on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, pp. 1308–1314, 2017.

[4] N. Soliman, M. Khalil, A. Algarni, S. Ismail, R. Marzouk *et al.,* "Efficient HEVC steganography approach based on audio compression and encryption in QFFT domain for secure multimedia communication," *Multimedia Tools and Applications*, vol. 80, no. 3, pp. 4789–4823, 2021.

[5] A. Alarifi, S. Sankar, T. Altameem, K. Jithin, M. Amoon *et al.,* "A novel hybrid cryptosystem for secure streaming of high efficiency H. 265 compressed videos in IoT multimedia applications," *IEEE Access*, vol. 8, pp. 128548–128573, 2020.

[6] L. Liu, S. Hao, J. Lin, Z. Wang, X. Hu *et al.,* "Image block encryption algorithm based on chaotic maps," *IET Signal Processing*, vol. 12, no. 1, pp. 18–22, 2018.

[7] M. Jwaid and T. Baraskar, "Study and analysis of mopy-move & splicing image forgery detection techniques," in *Proc. of IEE Int. Conf. on IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Tamilnadu, India, pp. 697–702, 2017.

[8] O. Faragallah, A. Afifi, H. El-Sayed, M. Alzain, J. Al-Amri *et al.,* "Efficient HEVC integrity verification scheme for multimedia cybersecurity applications," *IEEE Access*, vol. 8, pp. 167069–167089, 2020.

[9] S. Mushtaq and A. H. Mir, "Digital image forgeries and passive image authentication techniques: A survey," *International Journal of Advanced Science and Technology*, vol. 73, pp. 15–32, 2014.

[10] M. Ansari, S. Ghrera and V. Tyagi, "Pixel-based image forgery detection: A review," *IETE Journal of Education*, vol. 55, pp. 40–46, 2014.

[11] O. Faragallah, H. El-sayed, A. Afifi and W. El-Shafai, "Efficient and secure opto-cryptosystem for color images using 2D logistic-based fractional Fourier transform," *Optics and Lasers in Engineering*, vol. 137, pp. 1–15, 2021.

[12] K. Abdelwahab, S. Abd El-atty, W. El-Shafai, S. El-Rabaie and F. Abd El-Samie, "Efficient SVD-based audio watermarking technique in FRT domain," *Multimedia Tools and Applications*, vol. 79, no. 9, pp. 5617–5648, 2020.

[13] L. Roldan, M. Hernandez, M. Miyatake, H. Meana and B. Kurkoski, "Watermarking-based image authentication with recovery capability using halftoning technique," *Signal Processing: Image Communication*, vol. 22, no. 1, pp. 69–83, 2013.

[14] W. El-Shafai, F. Mohamed, H. Elkamchouchi, M. Abd-Elnaby and A. ElShafee, “Efficient and secure cancelable biometric authentication framework based on genetic encryption algorithm,” *IEEE Access*, vol. 9, pp. 1–25, 2021.

[15] W. El-Shafai, I. Almomani and A. Alkhayer, “Optical bit-plane-based 3D-JST cryptography algorithm with cascaded 2D-FrFT encryption for efficient and secure HEVC communication,” *IEEE Access*, vol. 9, pp. 35004–35026, 2021.

[16] X. Wang, J. Xue, Z. Zheng, Z. Liu and N. Li, “Image forensic signature for content authenticity analysis,” *Journal of Visual Communication and Image Representation*, vol. 23, no. 5, pp. 782–797, 2012.

[17] W. El-Shafai, E. El-Rabaie, M. El-Halawany and F. Abd El-Samie, “Efficient multi-level security for robust 3D color-plus-depth HEVC,” *Multimedia Tools and Applications*, vol. 77, no. 23, pp. 30911–30937, 2018.

[18] O. Faragallah, A. Afifi, W. El-Shafai, H. El-Sayed, M. Alzain *et al.,* “Efficiently encrypting color images with few details based on RC6 and different operation modes for cybersecurity applications,” *IEEE Access*, vol. 8, pp. 103200–103218, 2020.

[19] R. Kaur and A. Kaur, “A review of copy-move forgery detection techniques,” *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, vol. 6, no. 2, pp. 249–253, 2016.

[20] T. Sarode and N. Vaswani, “Copy–move forgery detection using orthogonal wavelet transforms,” *International Journal of Computer Applications*, vol. 88, no. 8, pp. 41–45, 2014.

[21] R. Maind, A. Khade and D. Chitre, “Image copy move forgery detection using block representing method,” *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 4, no. 2, pp. 49–53, 2014.

[22] O. Faragallah, W. El-Shafai, A. Sallam, I. Elashry, E. EL-Rabaie *et al.,* “Cybersecurity framework of hybrid watermarking and selective encryption for secure HEVC communication,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 2, pp. 1–25, 2021.

[23] A. Alarifi, M. Amoon, M. Aly and W. El-Shafai, “Optical PTFT asymmetric cryptosystem-based secure and efficient cancelable biometric recognition system,” *IEEE Access*, vol. 8, pp. 221246–221268, 2020.

[24] A. Gupta, N. Saxena and S. Vasistha, “Detecting copy move forgery using DCT,” *International Journal of Scientific and Research Publications*, vol. 3, no. 5, pp. 1–4, 2013.

[25] A. Algarni, G. El Banby, S. Ismail, W. El-Shafai, F. El-Samie *et al.,* “Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications,” *Entropy*, vol. 22, no. 12, pp. 13–61, 2020.

[26] R. Rajkumar and M. Singh “Digital image forgery detection using SIFT feature,” in *Proc. of IEEE Int. Symposiwn on Advanced Computing and Communication (ISACC)*, Silchar, India, pp. 186–191, 2015.

[27] B. Usutbioglu, G. Muzaffer and G. Uluts, “A novel keypoint based forgery detection method based on local phase quantization and SIFT,” in *Proc. of IEEE Int. Conf. on Electrical and Electronics Engineering (ELECO)*, Bursa, Turkey, pp. 185–189, 2015.

[28] W. El-Shafai, F. Khallaf, E. El-Rabaie and F. Abd El-Samie, “Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 3, pp. 1–29, 2021.

[29] O. Faragallah, H. El-Sayed and W. El-Shafai, “Efficient opto MVC/HEVC cybersecurity framework based on arnold map and discrete cosine transform,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, pp. 1–16, 2021.

[30] V. Babu, A. Paulose and S. Krishna, “Digital image forgery detection using SURF,” *IOSR Journal of Computer Engineering*, vol. 18, no. 6, pp. 144–146, 2016.

[31] I. Badr, A. Radwan, E. El-Sayed, L. Said, G. El Banby *et al.,* “Cancellable face recognition based on fractional-order Lorenz chaotic system and Haar wavelet fusion,” *Digital Signal Processing*, vol. 5, pp. 1–22, 2021.

[32] I. Amerini, R. Caldelli and A. Bimbo, “A SIFT-based forensic method for copy–move attack detection and transformation recovery,” *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 1099–1110, 2011.

[33] Y. Fan, P. eCarré and C. F. Maloigne, “Image splicing detection with local illumination estimation,” in *Proc. of IEEE Int. Conf. on Image Processing (ICIP)*, Quebec, Canada, pp. 2940–2944, 2015.

[34] A. Alahmadi, M. Hussain, H. Aboalsamh, G. Muhammad and G. Bebis, "Splicing image forgery detection based on DCT and local binary pattern," in *Proc. of IEEE Global Conf. on Signal and Information Processing (GlobalSIP)*, Austin, TX, USA, pp. 253–256, 2013.

[35] S. El-Meadawy, A. Farghal, H. Shalaby, N. Ismail, F. Abd El-Samie *et al.,* "Efficient and secure bit-level chaos security algorithm for orbital angular momentum modulation in free-space optical communications," *IEEE Access*, vol. 9, pp. 1–25, 2021.

[36] E. Nancy and S. Kaur, "Image enhancement techniques: A selected review," *IOSR Journal of Computer Engineering*, vol. 9, no. 6, pp. 84–88, 2013.

[37] W. El-Shafai, S. El-Rabaie, M. El-Halawany and F. Abd El-Samie, "Proposed optimized hybrid error recovery techniques for performance improvement of wireless 3D-MVC communication," *Journal of King Saud University-Computer and Information Sciences*, vol. 31, no. 4, pp. 469–480, 2019.

[38] E. El-Bakary, W. El-Shafai, S. El-Rabaie, O. Zahran and F. Abd El-Samie, "Efficient hybrid framework for transmission enhancement of composite 3D H. 264 and H. 265 compressed video frames," *Multimedia Tools and Applications*, vol. 78, no. 9, pp. 11337–11368, 2019.

[39] A. Baumy, M. Abdalla, N. Soliman and F. Abd El-Samie, "Efficient implementation of pre-processing techniques for image forgery detection," in *Proc. of IEEE Japan-Africa Conf. on Electronics, Communications and Computers (JAC-ECC)*, Alexandria, Egypt, pp. 53–56, 2017.

[40] H. He and W. Siu, "Single image super-resolution using Gaussian process regression," in *Proc. of IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, Colorado, USA, pp. 449–456, 2011.

[41] E. El-Bakary, W. El-Shafai, S. El-Rabaie, O. Zahran, M. El-Halawany *et al.,* "Proposed enhanced hybrid framework for efficient 3D-MVC and 3D-HEVC wireless communication," *Multimedia Tools and Applications*, vol. 78, no. 11, pp. 14173–14193, 2019.

[42] W. El-Shafai, "Pixel-level matching based multi-hypothesis error concealment modes for wireless 3D H. 264/MVC communication," *3D Research*, vol. 6, no. 3, pp. 1–11, 2015.

[43] A. Kaissis, R. Makowski, D. Rückert and F. Braren, "Secure, privacy-preserving and federated machine learning in medical imaging," *Nature Machine Intelligence*, vol. 2, no. 6, pp. 305–311, 2020.

[44] F. Abd El-Samie, R. Nassar, M. Safan, M. Abdelhamed, A. Khalaf *et al.,* "Efficient implementation of optical scanning holography in cancelable biometrics," *Applied Optics*, vol. 60, no. 13, pp. 3659–3667, 2021.

[45] A. Mahmoud, W. El-Shafai, T. Taha, S. El-Rabaie, O. Zahran *et al.,* "A statistical framework for breast tumor classification from ultrasonic images," *Multimedia Tools and Applications*, vol. 80, no. 4, pp. 5977–5996, 2021.

[46] S. El-Gindy, A. Hamad, W. El-Shafai, A. Khalaf, S. El-Dolil *et al.,* "Efficient communication and EEG signal classification in wavelet domain for epilepsy patients," *Journal of Ambient Intelligence and Humanized Computing*, vol. 3, pp. 1–16, 2021.

[47] CASIO 2.0 v2 Database, [Online]. Available: http://forensics.idealtest.org:8080/indexv2:html, last access on 1-07-2021.

[48] G. Serra, "MICC-F600 dataset," [Online]. Available: http://giuseppeserra.com/content/sift-based-forensic-method-copymove-detection, last access on 1-07-2021.

[49] D. Tralic, I. Zupancic, S. Grgic and M. Grgic, "CoMoFoD: New database for copy-move forgery detection," in *Proc. of IEEE Int. Symposium of ELMAR*, Zadar, Croatia, pp. 49–54, 2013.