



An approach for anti-forensic contrast enhancement detection using grey level co-occurrence matrix and Zernike moments

Neha Goel¹ · Dinesh Ganotra¹

Received: 9 September 2022 / Accepted: 18 February 2023 / Published online: 16 March 2023

© The Author(s), under exclusive licence to Bharati Vidyapeeth's Institute of Computer Applications and Management 2023

Abstract The present paper aims to detect contrast enhancement when forensic fingerprints are removed by anti-forensic attacks. The methodology employed in this study exploits statistical anomalies in the frequency domain by using second-order statistics determined from grey-level co-occurrence matrix (GLCM). The magnitude of first 36 Zernike moments (ZMs) of column-wise Fourier transform of the GLCM is used to generate the feature vector. A support vector machine (SVM) classifier is employed to distinguish between original and altered images. To evaluate the performance of presented model, we plot receiver operating characteristic (ROC) curve and calculate true positive rate (TPR), false positive rate (FPR), and accuracy of the model. The results show that in the presence of an anti-forensic attack, the TPR reaches 92.0%, and the FPR reaches 91.1%. Thus, the results verify the effectiveness of the proposed approach for detecting contrast enhancement when anti-forensic attacks are removing forensic fingerprints. The proposed method is also robust against Gaussian white noise and losses due to compression.

Keywords Contrast-enhancement · Anti-forensics · Grey level co-occurrence matrix · Statistical fingerprints · Zernike moments

1 Introduction

Contrast enhancement is a common technique used in digital image manipulation to acquire a more realistic image.

✉ Neha Goel
neha.goel22oct@gmail.com

¹ Indira Gandhi Delhi Technical University for Women, Applied Sciences and Humanities, Delhi, India

In image forgery like cut-paste [1] and copy-move [1, 2], due to the possibility that two altered images may have been captured with diverse cameras and under differing lighting conditions, the forgers are forced to utilize several pixel modelling techniques on the altered image. Contrast enhancement, which can be accomplished through gamma correction or histogram stretching, is the most often utilized pixel modelling technique. Contrast-enhancing operations have an impact on the statistical characteristics of the modified images. Digital image forensics [3, 4] alleviate this challenge by identifying the provenance of digital content using statistical imprints left behind by contrast enhancement operations. Contrast-enhanced images can be produced by applying the gamma correction given by Eq. (1) as

$$O(p, q) = \text{round} \left(255 \left(\frac{I(p, q)}{255} \right)^\gamma \right) \quad (1)$$

where, $I(p, q)$ is the original image and $O(p, q)$ is the gamma-corrected image with gamma value γ .

The majority of contrast enhancement forensic techniques [5–8] for identifying changes in image contrast rely on primary statistics derived from image histograms, i.e., these methodologies had investigated the peak and gap artefacts introduced in the image histogram as a result of such malicious operations. Methods for detecting contrast enhancement include first-order statistics based [6], conventional neural networks (CNN) based [9], and statistical moments [10] based techniques. Primary statistics-based techniques [5–8] are particularly successful at detecting contrast enhancement when no anti-forensic attacks are present. The development of image forensic technology has also led to the development of numerous anti-forensic techniques. The goal of these anti-forensic attacks [11–15] is to remove

statistical abnormalities from altered image's histograms, rendering the fundamental statistics-based forensic detection unreliable.

The removal of peak and gap artefacts from image histograms is the main objective of anti-forensic techniques. Consequently, the detection of contrast enhancement is now more challenging in images that use anti-forensic algorithms like total variation (TV) optimization [14] and universal anti-forensic scheme [12]. These attacks decreased the efficacy of particular contrast enhancement detectors, resulting in the development of more advanced systems. The anti-forensic attacks smoothen the histogram of the enhanced images by removing the statistical artefacts, i.e. peak and gap artefacts. Figure 1 demonstrates how the anti-forensic attacks smoothened the histogram, making fundamental statistical footprint-based techniques unreliable.

The anti-forensics technologies have made contrast enhancement forensics methods more challenging. Additionally, the performance of contrast enhancement detectors is significantly impacted by JPEG compression. Thus, for maintaining image integrity and authenticity, it is crucial to provide contrast enhancement detection methods that work well when anti-forensic attacks are present. As a result, several trustworthy contrast enhancement forensics techniques [16–19] have been introduced within the past year to deal with anti-forensic attacks and defeat JPEG compression. The anti-forensic contrast enhancement forensic detectors have been devised to solve the

problem of detecting contrast enhancement in the presence of aforementioned anti-forensic attacks. These include pixel and histogram domain CNN's based approach [19], Laplace derivative histogram-based method [16], and second order statistics based method [17]. Ultimately, these techniques did not successfully defend against the aforementioned anti-forensic attack described in [14]. The anti-forensic attack presented by Barni et al. [12] was successfully countered by the methods detailed in [17]. However, their approach could not effectively combat an anti-forensic algorithm created by Ravi et al. [14]. The contrast enhancement detector described in [16] produced a good sensitivity for detecting enhanced images against the anti-forensic attack offered by Ravi et al. [14]. Nevertheless, the detection accuracy still has some scope for improvement. The anti-forensic contrast enhancement detection is still ill-posed problem. The aim of this paper is to detect contrast enhancement forensics in the presence of anti-forensic attacks through second-order statistics using GLCM and ZMs. Our methodology achieves better classification accuracy in the framework of anti-forensic attack proposed in [14]. The present method performs very well as compared to traditional algorithms and produces state-of-the-art results. A brief introduction to GLCM and ZMs is given below:

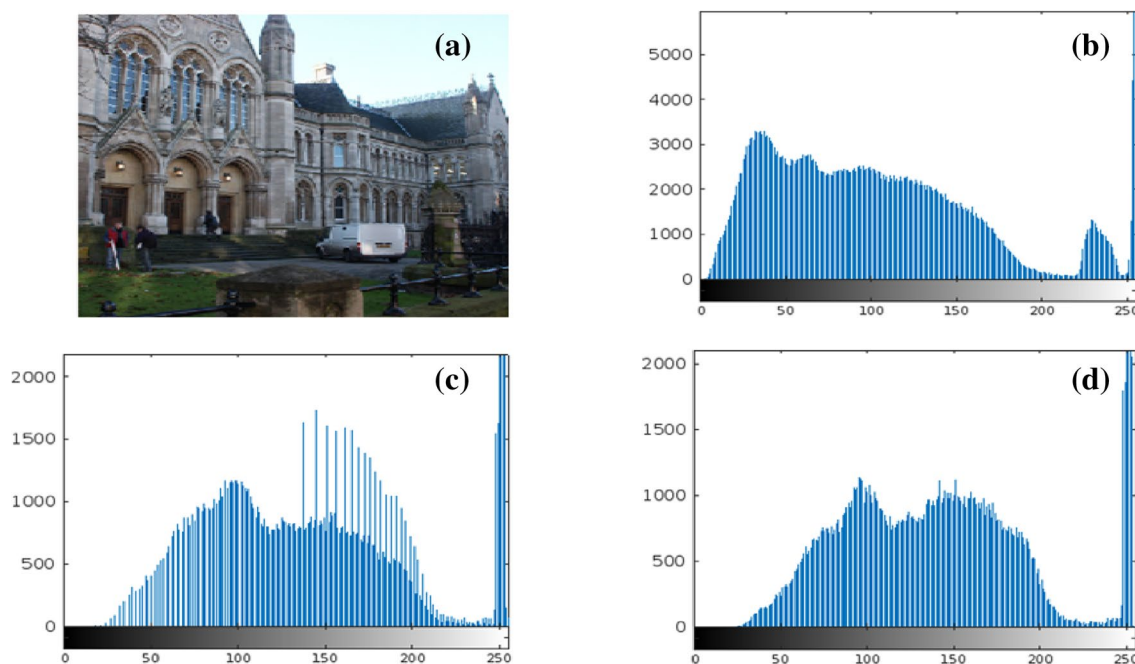


Fig. 1 a Sample image from UCID dataset b histogram of original image c histogram of the image after gamma correction d histogram of the image after anti-forensic attack

1.1 Grey level co-occurrence matrix

GLCM has been employed in texture analysis [20], medical image classification [21] for extracting features based on second-order statistics. The GLCM is a histogram of co-occurring grayscale values in an image at a given direction to calculate spatial dependency. It examines the spatial relationship among pixels and evaluates how frequently a specific combination of pixels appears in an image in a given direction and distance d . The co-occurrence matrix C [17] for a given grayscale image $I(p, q)$ of size $M \times N$ pixels is given by Eq. (2) and written as

$$C_{\Delta x, \Delta y}(i, j) = \sum_{p=1}^M \sum_{q=1}^N \mathbb{I}\{I(p, q) = i \wedge I(p + \Delta x, q + \Delta y) = j\} \tag{2}$$

where Δx and Δy are spatial shifts in the x and y directions, respectively, and function $\mathbb{I}(\cdot)$ returns 1 when the argument is valid and 0 otherwise. There are 256 possible grey levels for an 8-bit image, resulting in a 256×256 pixels' GLCM. Figure 2 shows the construction of a GLCM for a 3-bit image with specified grey level intensities and spatial shift [0,1], i.e., in the horizontal direction. The GLCM dimension for a 3-bit image is 8 by 8.

1.2 Zernike moments

Statistical moments such as orthogonal invariance moments [22] for image analysis, Gaussian-Zernike moments [23] for edge detection, Chebyshev polynomials [24] for edge detection in contrast-enhanced images and ZMs [25–27] were used to determine the features of the grayscale image for various applications. ZMs have been widely used to analyze the test images without considering changes in position, size, and orientation. ZMs have the following properties that are

preferable to other moments for feature extraction. (1) The Zernike polynomials represent visual distortions that are balanced. Specifically, they are optically balanced to give the least variance over the pupil plane. (2) The sum of the squares of ZMs represents the variance of overall distortions.

ZMs are the transformation of an image into a set of orthogonal complex basis functions in polar coordinates. These can represent image attributes with no ambiguity or overlap of information between the moments. The Zernike basis function [26] forms a complete set over the interior of a unit circle and is given by Eq. (3) written as

$$V_{nm}(\rho, \theta) = R_{nm}(\rho)e^{im\theta} \tag{3}$$

where $V_{nm}(\rho, \theta)$ is the Zernike polynomial, the radial polynomials are given by Eq. (4) as

$$R_{nm}(\rho) = \sum_{s=0}^{(n-m)/2} \frac{(-1)^s (n-s)!}{s! \left(\frac{n+m}{2} - s\right)! \left(\frac{n-m}{2} - s\right)!} \rho^{n-2s} \tag{4}$$

The moment order with the repetition of m is denoted by n . The relationship between n and m is defined as

$$n - |m| = \text{even} \ \& \ |m| \leq n \tag{5}$$

n and m are non-negative integers.

Equation (6) can be used to compute the ZMs for a digital image.

$$Z_{nm} = \frac{n+1}{\pi} \sum_{\rho} \sum_{\theta} I(\rho, \theta) V_{nm}^*(\rho, \theta) \tag{6}$$

for $\rho \leq 1$

where $I(\rho, \theta)$ denotes the image function in polar coordinates.

Fig. 2 a Gray level intensities; b Corresponding GLCM



$$C(i, j) = C(1, 2) = 2$$

In this paper, we propose a robust anti-forensic contrast enhancement algorithm based on second-order image statistics which have good classification accuracy against anti-forensic attacks. We have investigated the impact of contrast enhancement on images by analyzing the co-occurrence matrix in the frequency domain. The second-order statistics in the frequency domain are then explored to detect contrast enhancement and examine their efficiency in the framework of anti-forensic attacks described in [12, 14]. The feature vector has been constructed using the ZMs of column-wise Fourier transform of the GLCM. The proposed contrast enhancement detection approach is validated on a contrast-enhanced image data set and contrasted images associated with anti-forensic attacks. In addition, the proposed approach has high precision in noise and losses due to compression.

The proposed method has overcome certain limitations of previous anti-forensic contrast enhancement detection method. The key objectives of proposed method are given below.

- Anti-forensic contrast enhancement using GLCM and ZMs.
- The First phase is obtaining the GLCM of input image, which is the histogram of co-occurring grayscale values in an image at a given direction.
- The next phase is feature extraction, ZMs and Fourier transform is used to extract the features from GLCM.
- Finally, SVM Classifier is used for the evaluation of the method.

The detailed architecture of the proposed method is shown below in Fig. 3:

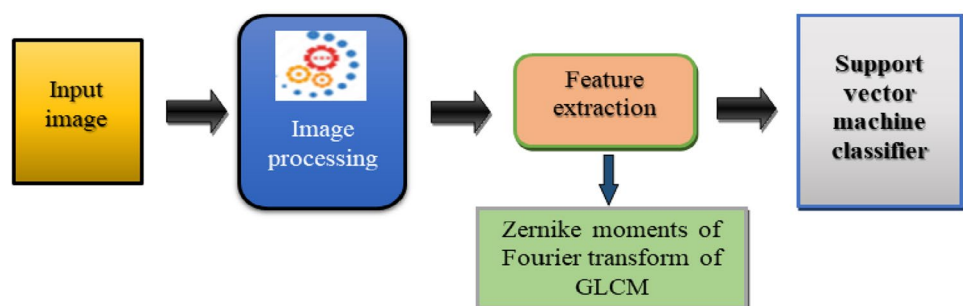
The rest of this paper is organized as follows. First, the existing framework of contrast enhancement forensic detection is described in Sect. 2. Section 3 introduces a new contrast enhancement detection approach for identifying contrasted images in the presence of anti-forensic attacks. The results and performance of the proposed approach are discussed in Sect. 4, where it is compared to existing contrast enhancement detection methodologies. Finally, Sect. 5, and 6 summarizes this paper's main conclusions and future scope.

2 Related methods

Numerous techniques have been put forth so far from the viewpoint of image forensics to determine whether or not an image has undergone contrast enhancement. Mostly the initial suggested methodologies for contrast enhancement forensics detection are based on first order statistics [5–8, 28, 29]. Blind forensics using image histogram [5], forensic detection of image manipulation using statistical intrinsic fingerprints [6] are some of the most prevalent techniques.

Stamm and Liu [5] demonstrated a blind method for detecting global contrast enhancement and histogram equalization. They claimed that histograms of original images have a smooth envelope, whereas peak and gap artefacts are incorporated into the histogram of enhanced images. These histogram discontinuities were attributed to high-frequency components that increased as a result of contrast enhancement operation. The authors were used the Fourier transforms to identify the contrast-enhanced images. These methods do not identify contrast enhancement in the previously low-quality JPEG-compressed images, since the presumption of a smooth surface is no longer valid. To address this issue, Cao et al. [7] suggested a global contrast enhancement detection method that also works well in poor-quality images. They investigated the introduced peaks and gaps in the image histogram due to contrast enhancement. They employed the number of gaps to detect contrast enhancement as a distinguishing feature. They set a decision threshold value in advance. If the number of gaps exceeded a certain threshold, contrast enhancement was detected; otherwise, it was not. They had used zero-gap bins to identify distinguishing features for recognizing changes in image contrast. Their method was also used to detect tampered areas in splicing by employing peak and gap bins. Shabanifard et al. [10] proposed a method based on pixel pair histograms and ZMs. They extracted some relevant features using the pixel pair histogram and its binary counterparts and some other features using a distribution of Fourier transform in polar coordinates. Their method distinguished four categories: original, noisy, histogram equalized, and contrast-enhanced. Lin et al. [30] proposed a method for determining contrast enhancement in color images. They claimed a correlation

Fig. 3 Architecture of the proposed algorithm



between the R, G, and B channels, i.e., the number of samples in the G channel was twice as large as the number of samples in the R and B channels. This inter-channel correlation was disrupted by the contrast-enhanced process. They developed a metric to assess the relationship between high-frequency components in different color channels in original and modified images. Their method was limited to color images originating from cameras and failed with compressed images, making it inappropriate for a large number of images. Two identically enhanced approaches were presented by Lin et al. [31]. In their method, Lin's approach [30] was modified to incorporate a linear-threshold scheme and Stamm's algorithm's [6] cut-off frequency was switched with a quadratic weighting function. Wang et al. [8] investigated how gamma transformation applications influence image histograms. They created a feature vector from the difference between zero value bins and image adjoining histogram bins to recognize original and altered images. In addition to these methods, many other methods, such as enhancement detection in MRI images [32], underwater haze enhancement [33], image enhancement and matching techniques [34], and histogram based digital watermarking approach [35] have been proposed. In [33], the authors proposed a method to increase the visibility of deburred images taken underwater that are distorted by elements that permeate throughout them. They used gradient-guided strain and the dark channel to remove mist prior to processing the image due to radiance events. After that, they used a gradient-guided filter to produce a smooth border with more variation. By completely preventing halo formation, their method outperforms the traditional methods. These techniques were not sufficient to produce a good classification results in the framework of anti-forensic attacks.

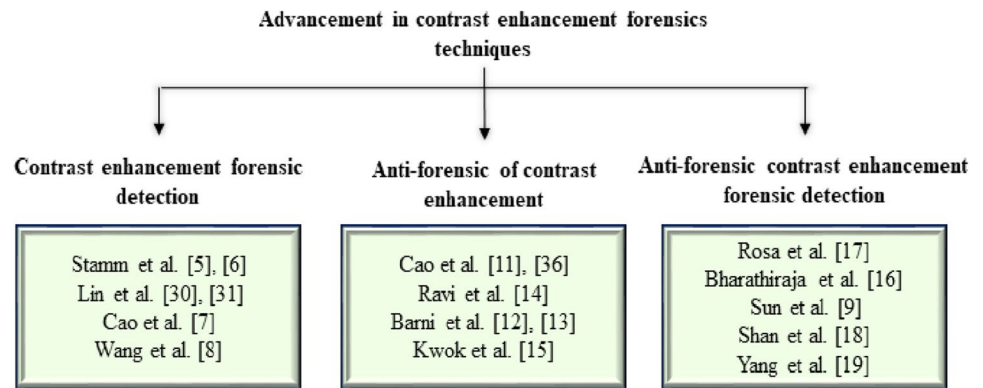
Numerous anti-forensic techniques [11–15, 36–38] to deceive histogram-based forensic tools have been put forth from the adversary's point of view. Most of these techniques are targeted, aiming to erase the traces left behind by a particular forensic procedure. A universal anti-forensic technique has been presented in [12, 13] that attempts to replicate the statistical characteristics of unaltered contents. In [12], Barni et al. established a universal anti-forensic methodology for histogram-based image forensics. They proposed that adding Gaussian noise to contrast-enhanced images makes the histogram smoother, leaving the transformation unidentifiable by the aforementioned method. They first generated a set of histograms for the original images, and then they searched the original dataset for contrast-enhanced images that had good matches in their histograms. Finally, the histogram of the altered image was mapped to the histogram of the original image. An optimization problem was solved to

estimate the remapped pixels for a modified image. They produced an output image with good visual quality that was undetectable by contrast enhancement detectors. Cao et al. [11] developed an approach against conventionally contrast enhancement detectors to eliminate the peaks and gaps using local random dithering. They calculated PSNR metric for the manipulated image to preserve the image quality. Ravi et al. [14] proposed a TV norm optimization-based anti-forensic attack against histogram-based and GLCM-based contrast enhancement detectors. Kwok et al. [15] proposed an anti-forensic method to eliminate peak-gap artefacts using the internal bit depth method. Their method has good PSNR between conventional enhanced images and attacked images.

To overcome the problem of anti-forensic attack, Rosa et al. [17] demonstrated a method for determining contrast enhancement utilizing second-order statistics. They used variance-based features to identify whether a particular image has undergone contrast enhancement. To combat the CE detector proposed in [17], Ravi et al. [14] proposed an anti-forensic system based on TV norm optimization.

Bharatiraja et al. [16] presented a method for detecting forgery manipulations by evaluating image derivatives. They investigated the impact of contrast enhancement on average saturation level of the derivatives of natural images. They determined lower and upper cut-off threshold limits whose span identifies forgery falsification even in the existence of anti-forensic attacks. Their method has good classification accuracy against the attack described in [14], has some scope of improvement. Additionally, detectors based on CNN [9, 18, 19] have also been presented. Some of these employed a histogram and pixel-domain CNN [19], whereas [9, 18] combine GLCM and CNN. An approach based on deep learning similar to enhancement is proposed in [39] for image compression and restoration. In [9], Sun et al. suggested a convolutional neural network (CNN) based detector that fed GLCM to the CNN to boost performance against anti-forensic attacks. The suggested CNN can extract a range of relevant characteristics to identify manipulation by learning hierarchical feature representations and maximizing classification outcomes. Shan et al. [18] proposed a modified CNN-based contrast enhancement forensic approach. The enhanced image is fed into the first layer of their architecture, and the result is GLCM, which contains contrast enhancement fingerprints. For noise reduction in GLCMs, a cropping layer was utilized. Their method was applied for global or local contrast enhancement detection and compression losses. CNN-based detectors have a high computational cost despite having good accuracy. Advancement in the technology of contrast enhancement forensic detection is categorized in the Fig. 4.

Fig. 4 The categorization of contrast enhancement forensic detection techniques



3 Proposed method

First, we have briefly discussed the motivation behind the selection of the GLCM and ZMs for the feature extraction for anti-forensic contrast enhancement detection.

3.1 Selection of GLCM and Zernike moments

Our objective is to use second-order statistics in the frequency domain to identify the existence of contrast enhancement. The critical disadvantage of utilizing the first-order statistics from image histograms is their limited sensitivity to pixel mapping alterations. For example, suppose mapping transformations eliminate one of an 8-bit image's grey-scale intensity levels. In that case, just one component of the image histogram is altered, contrary to GLCM, where the effect is visible throughout the image. As a result, in the suggested method, we use GLCM rather than a conventional histogram to perform better than earlier works in the same field.

An example of GLCM of an unaltered natural image with offsets $(\Delta x, \Delta y) = (0, 1)$ has been shown in Fig. 5. Rosa et al. [17] explained that due to the significant correlation between neighboring pixels in natural images, intensities pairs around the main diagonal appear more

frequently, as shown in Fig. 5 a. Figure 5 b illustrates the GLCM of gamma-transformed image with a gamma value of 0.8. As a consequence of gamma correction, the GLCM has a significantly wider spread. Consequently, several unoccupied rows and columns appear in GLCM, corresponding to peak and gap abnormalities in the image histogram.

The impact of the anti-forensic attack [12] on GLCM has been displayed in Fig. 5 c. These attacks suppress the gap and peak anomalies from the image histogram. Therefore, there are no unoccupied rows or columns. Even though the histograms of original and attacked images are comparable, the GLCM still contains noticeable attributes. As a result, we intend to utilize second-order statistics to investigate for evidence of histogram-based analysis.

Stamm and Liu [6] suggested that when an image undergoes pixel transformation, such as contrast enhancement, the integral values of the grey-level intensities are used, increasing the energy of high-frequency components of the image histogram. Based on these effects, it was claimed that the Fourier spectrum of natural image histograms must be a strictly low pass. Transforming the GLCM into a frequency spectrum makes it easy to filter specific frequencies.

An image moment is a specific weighted average of image pixel intensities. Moments were chosen extensively

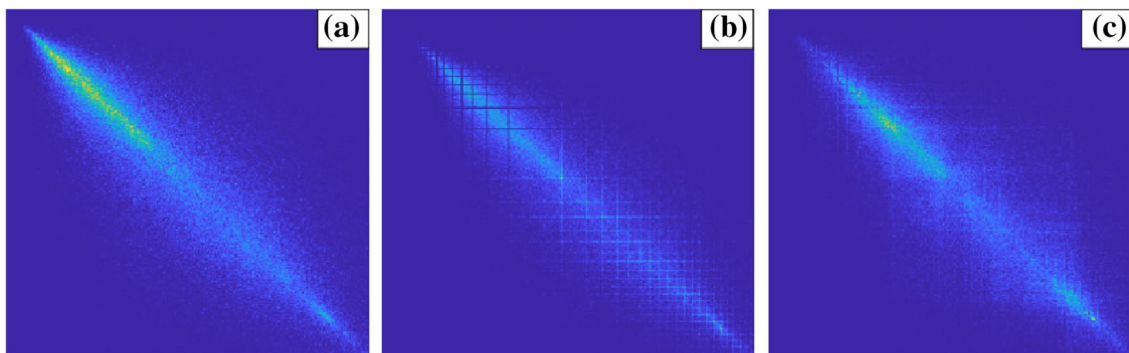


Fig. 5 GLCM of **a** original image **b** same image after gamma correction **c** after an anti-forensic attack []

for highlighting an image's appealing feature or interpretation. According to the uniqueness theorem, the image function has a unique set of moment values. Image characteristics can be uniquely inferred from moments. The impact of gamma correction on an image is also referred to as image distortion. The first 36 ZMs depict the primary order defects; moments represent secondary or higher-order defects beyond this value. As intensity variations occur during the contrast enhancement process, they can be investigated using primary moments. As a result, the first 36 ZMs were employed as a feature vector retrieved from the co-occurrence matrix's column-wise Fourier transform. The column-wise Fourier transform can be calculated using Eq. (7), given as

$$F_{LAF} = \log(1 + \text{abs}(\text{FFT}(O(p, .)))) \quad (7)$$

The present research has studied anti-forensic contrast enhancement detection, that is as follows:

3.2 Present anti-forensic contrast enhancement approach

Anti-forensic contrast enhancement is the process of concealing the statistical artefacts in image histograms arising due to the contrast enhancement operation. In this present method, the SVM classifier is used for the detection of contrast enhancement in the presence of anti-forensic attacks. In this method, first, the original and tampered images are taken as input, then the next phase is pre-processing, in order to convert the image pixels into gray level co-occurrences pre-processing is used, then the next phase is feature extraction for extracting the features from the pre-processed images. Listing 1. Explains the algorithm for the proposed anti-forensic contrast enhancement detection method.

In this model, the input images are cropped to square images and converted to grayscale. Then, the image database of original images, contrast-enhanced images, histogram stretched and the attacked images using two anti-forensic attacks [12, 14] are generated. For changing the contrast of an image, the gamma correction given by Eq. (1) is used. The ZMs features are extracted from the Fourier transform of GLCM, and different class labels are assigned. The model is trained by using these feature vectors to the corresponding labels. The model is trained using RBF kernel-based SVM classifier. Two different image datasets often used for contrast enhancement detection are utilized to evaluate the proposed model. The flow chart of the proposed algorithm is shown in Fig. 6.

To validate the extracted features, we have studied the influence of features on original and contrast-enhanced images in the following. We apply principal component analysis to reduce the high dimensions data to low dimensions to visualize the data. Figure 7 depicts a scatter plot of the principal component of each 500 original images and enhanced images. The contrast-enhanced images are generated by gamma correction to the unmodified image with gamma values spanning between [0.2, 2.2]. The figure illustrates that our features could clearly distinguish between original and contrast-enhanced images, implying that these features can be used to detect changes in image contrast.

In the following subsection, the metrics used to evaluate the performance of the proposed method are discussed.

3.3 Performance evaluation metrics

To evaluate the performance of the classifier, the ROC curve between TPR and FPR is plotted. TPR and FPR can be calculated using the formulas given in Eq. (8) and (9).

Algorithm 1 ANTI-FORENSIC CONTRAST ENHANCEMENT DETECTION

Input: A test image X .

Output: Image is changed by contrast enhancement operations or not

Steps:

- i. Convert input image X to grayscale and square it, get X_{sq} .
 - ii. Compute $C_{\Delta x, \Delta y}$ of X_{sq} using Eq. (2), get X_{glcm} .
 - iii. Calculate F_{LAF} , the FT of X_{glcm} using Eq. (7), and get X_{FT} .
 - iv. Find input features X_{in} , the ZMs of the X_{FT} using Eq. (6).
 - v. Load the SVM model for CE and pass in the X_{in} . This will give the output label Y_{CE} .
 - vi. If ($Y_{CE} == 1$)
 image is subjected to contrast enhancement.
 else
 image is not subjected to contrast enhancement
-

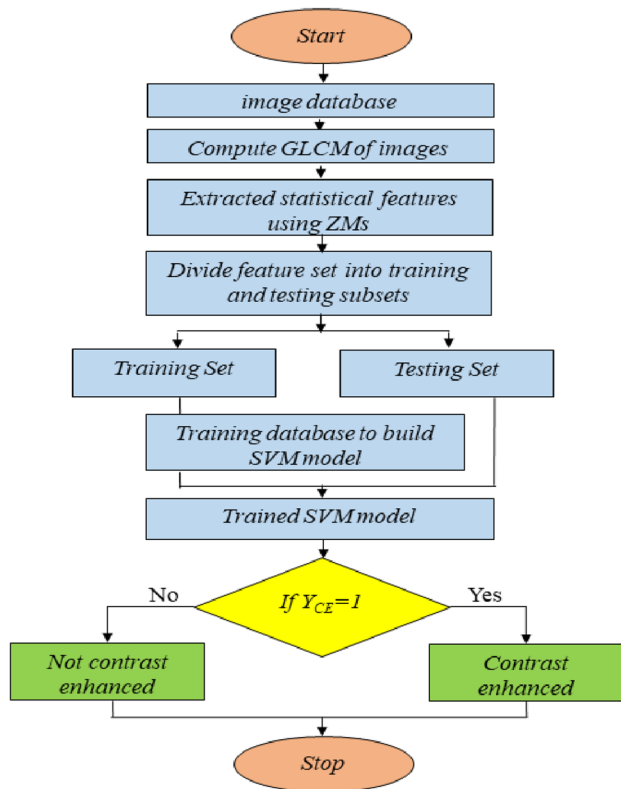


Fig. 6 Flow chart for the Proposed Algorithm

$$TPR = \frac{TP}{TP + FN} \quad (8)$$

$$FPR = \frac{FP}{FP + TN} \quad (9)$$

where TP = True positives, FP = False positives, FN = False negatives, and TN = True negatives.

Precision and recall are important metrics to evaluate the effectiveness of machine learning models. Precision is used to estimate how good our model is in identifying the positives and calculated as given in Eq. (10)

$$Precision = \frac{TP}{TP + FP} \quad (10)$$

and Recall measures, how many positive outcomes our model was able to identify correctly and calculate as given in Eq. (11)

$$Recall = \frac{TP}{TP + FN} \quad (11)$$

Equation (12) can be used to calculate the accuracy of the model

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP} \quad (12)$$

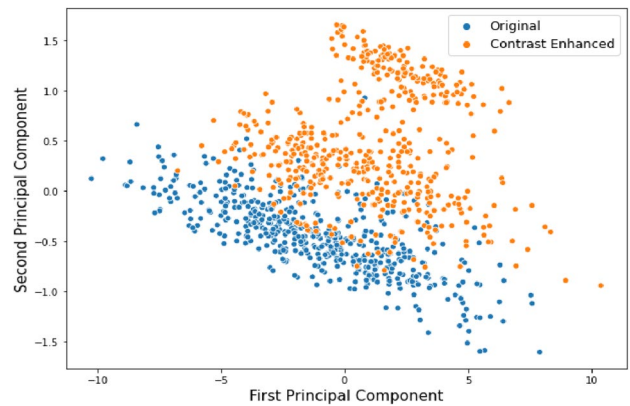


Fig. 7 Scatter plot of principal components for original and enhanced images

4 Results and discussion

We evaluate the performance of the proposed method in this section. The algorithm is tested on two datasets, i.e., UCID dataset [40], and BossBase dataset [41]. The contrast-enhanced dataset (X_{CE}) is then generated by performing gamma correction with gamma values {0.6, 0.8, 1.2, and 1.4} chosen at random using Eq. (1). We also created the histogram stretched dataset (X_{HS}) by stretching the histogram. Our histogram stretching operation saturates 1% of input pixel values at 0 and 1% at 255. The anti-forensic approach described in [12] is then applied to enhance images with maximum absolute pixel distortion $D_{max} = 4$, yielding the anti-forensic contrast-enhanced dataset (X_{AFCE}) and anti-forensic histogram stretched dataset (X_{AFHS}). The anti-forensic image datasets are also generated using the scheme described in [14]. The classification results are discussed in the following subsection:

4.1 Classification results for contrast-enhanced and attacked images

To evaluate the performance of the proposed method, we use the SVM classifier with RBF kernel. To maintain consistency, we first analyzed different scales to remap the data within a range recommended for different machine learning algorithms. We then choose MinMax Scaler, which scaled the data into (0,1) and utilized the same scale for all datasets. After scaling the data, the binary class SVM classifier with RBF kernel was employed with parameters $C = 4$ and $\gamma = 1$. For classification, we kept 20% of the data for evaluation (test data) and utilized the other 80% for training the model.

The algorithm is first tested on the UCID dataset [40], containing 384×512 pixels of uncompressed color images. Since ZMs may be estimated for square images, cropped images to 384×384 pixels and grayscale. The dataset

Table 1 Performance comparison of the proposed method

Contrast enhancement detection techniques	TPR		FPR		Accuracy	
	Gamma corrected (%)	Histogram stretched (%)	Gamma corrected (%)	Histogram stretched (%)	Gamma corrected (%)	Histogram stretched (%)
Original vs. contrast-enhanced images						
Stamm and Liu [5]	88.5	89.9	95.8	97.6	95.4	90.2
Stamm and Liu [6]	89.6	89.8	98.4	96.9	96.4	92.6
Cao et al. [7]	85.5	86.6	97.7	97.8	85.9	85.5
Wen et al. [29]	97.7	95.0	94.4	93.8	94.2	94.2
Rosa et al. [17]	98.5	96.0	97.4	87.8	93.8	94.6
Present work	98.6	96.4	98.5	98.4	95.2	94.9
Original vs anti-forensic contrast-enhanced images with attack [12]						
Stamm and Liu [5]	48.1	42.2	18.2	17.2	53.2	40.8
Stamm and Liu [6]	49.9	46.8	13.5	13.9	58.1	43.2
Cao et al. [7]	55.8	56.0	46.3	46.7	46.5	46.6
Wen et al. [29]	64.8	65.2	62.4	64.3	68.8	69.8
Rosa et al. [17]	67.8	93.2	81.6	91.1	76.3	92.1
Present work	94.3	97.1	97.0	96.6	95.7	96.9
Original vs anti-forensic contrast-enhanced images with attack [14]						
Stamm and Liu [5]	49.1	48.8	65.7	64.3	60.4	58.9
Stamm and Liu [6]	45.8	50.9	68.1	67.7	40.4	40.9
Cao et al. [7]	50.6	52.0	30.5	32.0	38.6	38.6
Wen et al. [29]	63.8	63.7	61.2	63.3	59.5	59.3
Rosa et al. [17]	53.1	69.4	59.1	71.1	58.3	70.7
Present work	82.4	89.2	83.9	84.9	83.3	86.7

Maximum values of TPR, FPR, and accuracy are highlighted as bold

generated of original, contrast enhanced and anti-forensic contrast enhanced images, consists of 6202 images (886 originals, 1772 contrast-enhanced, and 3544 attacked images with two anti-forensic schemes described in [12, 14]).

To evaluate the efficacy of our suggested method, we calculated the TPR and FPR using Eq. (8) and (9), which are commonly used machine learning measures. Table 1 shows the performance comparison of present method with contrast-enhanced images, and in the presence of anti-forensic attacks described in [12], and [14]. Table 1 illustrates that when anti-forensic approaches are employed, our suggested method outperforms the existing method while maintaining performance for non-attacked contrast-enhanced images.

To measure the effectiveness of the proposed method further, we plot ROC curves of each dataset group for present work and for method described in [17] as their method has comparable results to our method. As the method described in [17]. In the first group, we examine the proposed method’s performance for X_{CE} and X_{HS} , where no anti-forensic approaches are utilized to remove the artefacts. The ROC curve (Fig. 8a) demonstrates that our method performs comparably with the method proposed in [17]. In the second group, we use the X_{AFCE} and X_{AFHS} datasets when employing the anti-forensic technique described in [12]. The ROC curve (Fig. 8b) is plotted to compare our method’s results

with the approach described in [17]. The curve shows that our technique outperforms and can detect attacked images with a low false-positive rate. Finally, when the anti-forensic technique proposed in [14] is used, the results for the X_{AFCE} and X_{AFHS} are examined in the third group. Although both approaches are affected by anti-forensic attacks, as seen in the ROC Curve (Fig. 8c), our strategy performs significantly better than the method employed in [17].

The performance of the suggested method is further examined on other dataset to ensure its validity. For this, 200 images are randomly chosen to generate the original image database from BossBase-1.01 [41], then apply gamma correction to original images with gamma values {0.2, 0.4, 0.6, 1.8, 2.0, and 2.2} to create the X_{CE} . Also, we generated X_{AFCE} dataset using anti-forensic schemes described in [12]. Table 2 highlights the proposed system’s performance against successful detectors. Table 2 illustrates that while the proposed anti-forensic contrast enhancement detector responds similarly to the conventional contrast enhancement detectors but has improved accuracy against the anti-forensic approach.

Again, we have calculated the TPR and true negative rates (TNR) for the proposed method and compare it with existing methods with anti-forensic scheme [14]. The comparison of classification results is shown in Table 3.

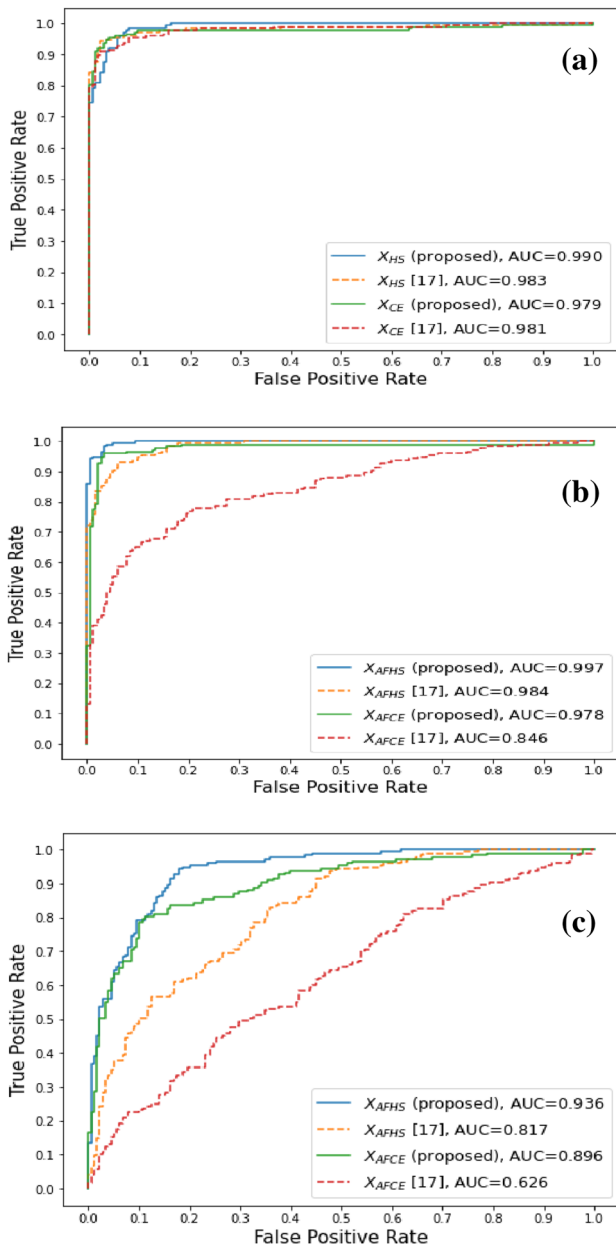


Fig. 8 ROC curves between original and **a** enhanced images **b** attacked images with anti-forensic scheme given in [12] **c** attacked images with anti-forensic scheme given in [14]. X_{HS} Histogram Stretched Dataset, X_{CE} : Contrast-Enhanced Dataset, AUC Area under the Curve, X_{AFHS} Anti-Forensic Histogram Stretched Dataset, X_{AFCE} Anti-Forensic Contrast -Enhanced Dataset

In the following subsection, we have discussed the robustness of the proposed method against noise and compression losses.

4.2 Robustness against noise and compression losses

We also tested the performance of the proposed method when Gaussian noise and compression losses are added

Table 2 Detection accuracy of the proposed method

Method	%			
	$\gamma=0.6$	$\gamma=0.8$	$\gamma=1.2$	$\gamma=1.4$
Original images vs contrast enhanced images				
Stamm and Liu [5]	96.8	95.6	93.2	94.0
Stamm and Liu [6]	98.2	96.8	94.0	95.2
Cao et al. [7]	93.8	93.9	80.2	81.4
Wen et al. [29]	94.2	84.8	75.3	74.0
Rosa et al. [17]	94.0	84.5	78.3	74.1
Yang et al. [19]	94.7	89.0	78.0	86.0
Present work	98.7	98.2	93.7	95.0
(Original vs. anti-forensic contrast-enhanced images with attack [12])				
Stamm and Liu [5]	59.0	64.9	78.4	79.8
Stamm and Liu [6]	67.4	68.8	80.2	80.4
Cao et al. [7]	62.3	70.4	79.4	81.2
Wen et al. [29]	67.8	65.2	62.9	64.2
Rosa et al. [17]	69.8	66.0	62.2	64.4
Yang et al. [19]	98.6	97.5	97.8	97.0
Present work	97.5	97.6	97.3	97.2

Maximum accuracy values at different gamma values are highlighted as bold

Table 3 Classification results for contrast-enhanced images with anti-forensic scheme [14]

Method	True positive rate (%)	True negative rate (%)
Stamm and Liu [5]	58.0	60.0
Stamm and Liu [6]	61.4	62.2
Wen et al. [29]	60.1	61.7
Rosa et al. [17]	33.1	67.2
Bharathiraja et al. [16]	90.6	90.8
Present work	92.0	91.1

Maximum values of TPR and TNR are highlighted as bold

to the enhanced images. We created the new noisy dataset by adding Gaussian noise with varying variances to the enhanced images and then tested the trained SVM with the newly obtained noisy dataset. We also test the trained SVM for losses due to compression. Table 4 shows the classifier’s performance in identifying each category. The proposed technique produces high classification rates, as observed. Compression losses weaken signal components at high frequencies, emphasizing the difference between original and modified images.

Table 4 Detection accuracy of the proposed method for different noise variances and quality factor

Gamma value	The variance of Gaussian noise		Value of quality factor	
	0.001 (%)	0.003 (%)	50 (%)	70 (%)
$\gamma=0.2$	99.9	99.8	99.8	99.6
$\gamma=0.4$	99.8	99.4	99.0	99.2
$\gamma=0.6$	99.7	98.6	97.7	97.5
$\gamma=0.8$	97.5	97.2	96.4	97.7
$\gamma=1.2$	97.2	97.2	96.9	96.6
$\gamma=1.4$	97.3	96.2	97.9	96.9
$\gamma=1.6$	97.5	97.7	97.2	97.4
$\gamma=1.8$	98.2	98.2	98.0	97.6
$\gamma=2.0$	98.5	98.7	98.2	99.2
$\gamma=2.2$	99.2	99.5	99.4	99.7

5 Conclusion

This paper has improved classification accuracy to detect contrast enhancement of images over two anti-forensic approaches proposed in [12, 14]. The proposed forensic algorithm detects the changes in the contrast of images by examining second-order statistics in the frequency domain. 36 elements feature vector is created using the ZMs of Fourier transform of the GLCM. The ROC curves and recall-precision scores are calculated to evaluate the performance of the proposed method. The results reveal that the details in our feature vector can better classify original and tampered images, even when anti-forensic attacks are present. The proposed method is further evaluated on compression losses and noisy image datasets, and it performed well against these operations. Finally, the algorithm is tested on different datasets to verify the proposed methodology's accuracy. This method achieves good classification results and surpasses existing techniques when forgers attempt to conceal traces using various anti-forensic schemes.

6 Future scope

In the future, the current work can be combined with other methods to enhance the outcomes in places where it is lacking in the current study. We will try to detect contrast enhancement forensics of color images in the presence of anti-forensic attacks of chromatic aberrations. We will also investigate multi-operation image anti-forensic approaches with a CNN-based contrast enhancement detector using our feature vector as the input instead of an image.

Author contributions All authors contributed to the study conception and design. Material preparation, numerical simulations and analysis were performed by Neha Goel. The first draft of manuscript was written by Neha Goel and both the authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding No funding was received for conducting this study.

Availability of data and material Image dataset used in this research was available online.

Code availability Not applicable.

Declarations

Conflicts of interest The authors declare no conflicts of interest.

References

- Rathod G, Chodankar S, Deshmukh R, Shinde P, Pattanaik SP (2016) Image forgery detection on cut-paste and copy-move forgeries. *Int J Adv Electron Comput Sci* 3(6):13–19
- Huang HY, Ciou AJ (2019) Copy-move forgery detection for image forensics using the superpixel segmentation and the Helmert transformation. *Eurasip J Image Video Process* 1:2019. <https://doi.org/10.1186/s13640-019-0469-9>
- Redi JA, Taktak W, Dugelay JL (2011) Digital image forensics: a booklet for beginners. *Multimed Tools Appl* 51(1):133–162. <https://doi.org/10.1007/s11042-010-0620-1>
- Ferreira WD, Ferreira CBR, da Cruz Júnior G, Soares F (2020) A review of digital image forensics. *Comput Electr Eng*. <https://doi.org/10.1016/j.compeleceng.2020.106685>
- Stamm M, Liu KJR (2008) Blind forensics of contrast enhancement in digital images. *Proceedings of the international conference image process. ICIP. IEEE*, pp 3112–3115. <https://doi.org/10.1109/ICIP.2008.4712454>
- Stamm MC, Liu KJR (2010) Forensic detection of image manipulation using statistical intrinsic fingerprints. *IEEE Trans Inf Forensics Secur* 5(3):492–506. <https://doi.org/10.1109/TIFS.2010.2053202>
- Cao G, Zhao Y, Ni R, Li X (2014) Contrast enhancement-based forensics in digital images. *IEEE Trans Inf Forensics Secur* 9(3):515–525. <https://doi.org/10.1109/TIFS.2014.2300937>
- Wang P, Liu F, Yang C, Luo X (2018) Blind forensics of image gamma transformation and its application in splicing detection. *J Vis Commun Image Represent* 55(September 2017):80–90. <https://doi.org/10.1016/j.jvcir.2018.05.020>
- Sun JY, Kim SW, Lee SW, Ko SJ (2018) A novel contrast enhancement forensics based on convolutional neural networks. *Signal Process Image Commun* 63:149–160. <https://doi.org/10.1016/j.image.2018.02.001>
- Shabanifard M, Shayesteh MG, Akhaee MA (2013) Forensic detection of image manipulation using the Zernike moments and pixel-pair histogram. *IET Image Process* 7(9):817–828. <https://doi.org/10.1049/iet-ipr.2012.0717>
- Cao G, Zhao Y, Ni R, Tian H (2010) Anti-forensics of contrast enhancement in digital images. *MM Sec 10-Proc ACM SIGMM Multimed Secur Work*. <https://doi.org/10.1145/1854229.1854237>

12. Barni M, Fontani M, Tondi B (2012) A universal technique to hide traces of histogram-based image manipulations. *MM Sec 12-Proc 14th ACM Multimed Secur Work*. <https://doi.org/10.1145/2361407.2361424>
13. Barni M, Fontani M, Tondi B (2013) A universal attack against histogram-based image forensics. *Int J Digit Crime Forensics* 5(3):35–52. <https://doi.org/10.4018/jdcf.2013070103>
14. Ravi H, Subramanyam AV, Emmanuel S (2016) ACE—an effective anti-forensic contrast enhancement technique. *IEEE Signal Process Lett* 23(2):212–216
15. Kwok CW, Au OC, Chui SH (2012) Alternative anti-forensics method for contrast enhancement. *Lect Notes Comput Sci* 7128:398–410. https://doi.org/10.1007/978-3-642-32205-1_32
16. Bharathiraja S, Rajesh Kanna B (2019) Anti-forensics contrast enhancement detection (AFCED) technique in images based on Laplace derivative histogram. *Mob Netw Appl* 24(4):1174–1180. <https://doi.org/10.1007/s11036-019-01255-1>
17. De Rosa A, Fontani M, Massai M, Piva A, Barni M (2015) Second-order statistics analysis to cope with contrast enhancement counter-forensics. *IEEE Signal Process Lett* 22(8):1132–1136. <https://doi.org/10.1109/LSP.2015.2389241>
18. Shan W, Yi Y, Huang R, Xie Y (2019) Robust contrast enhancement forensics based on convolutional neural networks. *Signal Process Image Commun* 71:138–146. <https://doi.org/10.1016/j.image.2018.11.011>
19. Yang P, Ni R, Zhao Y, Cao G, Zhao W (2018) Robust Contrast Enhancement Forensics Using Pixel and Histogram Domain CNNs [Online]. Available: <http://arxiv.org/abs/1803.04749>
20. Dwaich HA, Abdulbaqi HA (1804) Signature texture features extraction using GLCM approach in android studio. *J Phys Conf Ser* 1:2021. <https://doi.org/10.1088/1742-6596/1804/1/012043>
21. Mall PK, Singh PK, Yadav D (2019) GLCM based feature extraction and medical X-RAY image classification using machine learning techniques. 2019 IEEE Conf Inf Commun Technol CICT 2019:1–6. <https://doi.org/10.1109/CICT48419.2019.9066263>
22. Lin H, Si J, Abousleman GP (2008) Orthogonal rotation-invariant moments for digital image processing. *IEEE Trans Image Process* 17(3):272–282. <https://doi.org/10.1109/TIP.2007.916157>
23. Li X, Song A (2010) A new edge detection method using Gaussian-Zernike moment operator. *CAR 2010–2010 2nd Int Asia Conf Informatics Control Autom Robot* 1:276–279. <https://doi.org/10.1109/CAR.2010.5456847>
24. Acharya K, Ghoshal D (2022) Edge detection using adjusted Chebyshev polynomials on contrast-enhanced images by modified histogram equalization. *Int J Inf Technol* 14:3031–3038
25. Li S, Lee MC, Pun CM (2009) Complex Zernike moments features for shape-based image retrieval. *IEEE Trans Syst Man Cybern Part A Systems Humans* 39(1):227–237. <https://doi.org/10.1109/TSMCA.2008.2007988>
26. Khotanzad A, Hong YH (1990) Invariant image recognition by Zernike moments. *IEEE Trans Pattern Anal Mach Intell* 12(5):489–497. <https://doi.org/10.1109/34.55109>
27. Kim WY, Kim YS (2000) Region-based shape descriptor using Zernike moments. *Signal Process Image Commun* 16(1):95–102. [https://doi.org/10.1016/S0923-5965\(00\)00019-9](https://doi.org/10.1016/S0923-5965(00)00019-9)
28. Gang Cao RN, Zhao Y (2010) Forensic estimation of gamma correction in digital images. In: *Proceedings of 2010 IEEE 17th International Conference on Image Processing*, pp 2097–2100.
29. Wen L, Qi H, Lyu S (2018) Contrast enhancement estimation for digital image forensics. *ACM Trans Multimed Comput Commun Appl* 14(2):1–21. <https://doi.org/10.1145/3183518>
30. Lin X, Li CT, Hu Y (2013) Exposing image forgery through the detection of contrast enhancement. 2013 IEEE International Conference on Image Processing. IEEE, pp 4467–4471. <https://doi.org/10.1109/ICIP.2013.6738920>
31. Lin X, Wei X, Li C-T (2014) Two improved forensic methods of detecting contrast enhancement in digital images. *Media Watermarking Secur Forens* 9028:90280X-1-90280X-10. <https://doi.org/10.1117/12.2038644>
32. Gupta S, Gupta R, Singla C (2017) Analysis of image enhancement techniques for astrocytoma MRI images. *Int J Inf Technol* 9(3):311–319
33. Jiji AC, Nagaraj R (2020) A novel imaging system for underwater haze enhancement. *Int J Inf Technol* 12:85–90
34. Kumar M, Priyanka (2019) Various image enhancement and matching techniques used for fingerprint recognition system. *Int J Inf Technol* 11:767–772
35. Malik S, Reddlapalli RK (2019) Histogram and entropy based digital image watermarking scheme. *Int J Inf Technol* 11:373–379
36. Cao G, Zhao Y, Ni RR, Tian HW, Yu LF (2014) Attacking contrast enhancement forensics in digital images. *Sci China Inf Sci* 57(5):1–13. <https://doi.org/10.1007/s11432-013-4928-0>
37. Sharma S, Ravi H, Subramanyam AV, Emmanuel S (2020) Anti-forensics of median filtering and contrast enhancement. *J Vis Commun Image Represent* 66:102682. <https://doi.org/10.1016/j.jvcir.2019.102682>
38. Barni M, Tondi B (2013) The source identification game: an information-theoretic perspective. *IEEE Trans Inf Forensics Secur* 8(3):450–463
39. Nair RS, Domnic S (2022) Deep-learning with context sensitive quantization and interpolation for underwater image compression and quality image restoration. *Int J Inf Technol* 14:3803–3814
40. Stich G, Schaefer M (2004) UCID—uncompressed colour image database. *Proc SPIE* 5307 Storage Retr Methods Appl Multimedia 5307:472–480
41. BossBase image dataset (2023) [Online]. Available: [Index of / data/projects/stegodata](http://agents.fel.cvut.cz/stegodata/). <http://agents.fel.cvut.cz/stegodata/>. Accessed 7 Oct 2020

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.