Perceptual Image Hashing using Transform Domain Noise Resistant Local Binary Pattern

S. Qasim Abbas, Fawad Ahmed, Yi-Ping Phoebe Chen*

***Abstract*—A new Discrete Cosine Transform (DCT) domain Perceptual Image Hashing (PIH) scheme is proposed in this paper. PIH schemes are designed to extract a set of features from an image to form a compact representation that can be used for image integrity verification. A PIH scheme takes an image as the input, extracts its invariant features and constructs a fixed length output, which is called a hash value. The hash value generated by a PIH scheme is then used for image integrity verification. The basic requirement for any PIH scheme is its robustness to non-malicious distortions and discriminative ability to detect minute level of tampering. The feature extraction phase plays a major role in guaranteeing robustness and tamper detection ability of a PIH scheme. The proposed scheme fuses together the DCT and Noise Resistant Local Binary Pattern (NRLBP) to compute image hash. In this scheme, an input image is divided into non-overlapping blocks. Then, DCT of each non-overlapping block is computed to form a DCT based transformed image block. Subsequently, NRLBP is applied to calculate NRLBP histogram. Histograms of all the blocks are concatenated together to get a hash vector for a single image. It is observed that low frequency DCT coefficients inherently have quite high robustness against non-malicious distortions, hence the NRLBP features extracted from the low frequency DCT coefficients provide high robustness. Computational results exhibit that the proposed hashing scheme outperforms some of the existing hashing schemes as well as can detect localized tamper detection as small as 3% of the original image size and at the same time resilient against non-malicious distortions.**

***Index Terms*— Discrete cosine transform, local binary pattern, perceptual image hashing, robust hash, transform domain hashing**

I. Introduction

PERCEPTUAL Image Hashing (PIH) has become a prominent research domain primarily due to speedy developments in image modification techniques that can easily alter digital images. The improvement in digital devices and networking schemes enables a user to create, broadcast, distribute, and store digital media including images and videos daily over social media networks very easily. Digital media can be easily replicated by means of copying and hence it is easy to illegally distribute or forge data. Conventionally, multimedia content integrity is accomplished by utilization of cryptographic hashing schemes. Cryptographic hashing schemes, for example, SHA-1, SHA-256 and MD5 translate original input media, for example, an image, into a fixed size binary string. Cryptographic hashing schemes in some cases may not be appropriate for image authentication. The main reason behind cryptographic hashing schemes opposition for image authentication is their sensitiveness for a single bit alteration in the input stream. This simply means that two images having only one-bit alteration will produce hash vectors with an immense Hamming distance. Generally, images undergo non-malicious distortions, such as, lossy JPEG compression, additive and multiplicative noise, Gaussian blurring, motion blurring, gamma correction, scaling, etc. Hence traditional cryptographic hash functions do not generate similar hash vectors for perceptually identical images [1, 2]. Consequently, cryptographic hashing schemes [3-5] are not suitable for integrity verification of image content. In order to resolve this problem, PIH algorithms are utilized for image authentication [6, 7]. The main objective of a PIH scheme is to extract robust, stable and unique features available in any image [8-11]. The extracted features are then employed to compute the hash. An image hash does not implant any watermark in the image and hence has the advantage of zero image degradation [12]. Specific functions are applied to compare hash values of original content and query content for the sake of image verification [13].

S. Qasim Abbas is with the Department of Computer Science and Information Technology, La Trobe University, Melbourne, VIC 3086 Australia. (e-mail: SyedQasim.Abbas@latrobe.edu.au).

Fawad Ahmed is with the Department of Electrical Engineering, HITEC University, Taxila, Punjab Pakistan. (e-mail: fawad@hitecuni.edu.pk).

Yi-Ping Phoebe Chen is with the Department of Computer Sciences and Information Technology, La Trobe University, Melbourne, VIC 3086 Australia. (e-mail: Phoebe.Chen@latrobe.edu.au).

*Corresponding author

II. Related work

There are several interesting and novel hashing schemes proposed in the literature for image integrity verification because digital images [14, 15] are modified with ease in this current era. Broadly speaking, these schemes are categorized into three major types as descriped below.

A. Techniques Based on Statistical Data

Statistical data, such as mean, variance, higher moments, and image intensity, etc., exhibit invariance to minute variations in an image. An image statistics vector-based scheme has been proposed by Venkatesan *et al.* to generate hash through numerous sub-bands obtained by wavelet decomposition of the image [16]. The authors observed that statistics like averages of coarse sub-bands and variances of other sub-bands are invariant under many non-malicious

distortions. In this technique, a randomization is performed by first dividing each sub-band into random regions utilizing a secret key and then extracting statistics from all the regions. The quantized statistics are subsequently given to a decoding stage of a Reed-Muller error-correcting code to generate the final hash vector. Tang *et al.* [17] used histogram of color vector angles for hash generation. This scheme is robust against rotation with an arbitrary degree, but mistakenly view 17.05% different images as similar images while the ratio of correct detection of the scheme is 98% [18]. Zhao *et al.* [19] generate hash vector from Zernike moments of the inscribed circle of the pre-processed square image. The hash is robust to a number of non-malicious distortions. As the Zernike moments are computed from the inscribed circle, hence is responsible for loss of information in image corners. This phenomenon eventually reduces sensitivity to tamper detection [20]. Karsh *et al.* [21] have proposed a PIH technique that exhibits invariance to rotation, scaling and translational perturbations. The hash is formed using local and global features. Local features are extracted from salient regions of an image using Markov absorption probabilities. Global features are extracted using some statistics measure. The two set of features help in finding small and big tampered areas with good robustness against content preserving manipulations. Eskenazi *et al.* [22] generate image hashes for hybrid document security. This algorithm can secure graphical objects with good performance using a small image digest. The main contribution of this work is that the generated hash can be identified in print and scan noise environment. In this scheme, a normalization of input image is first performed followed by second-order moments computation to construct hash vector of the query image. The hash vector contains several components such as moments, index mapping and color mapping table.

B. Techniques Based on Dimensionality Reduction

These hashing schemes are based on reducing the number of random variables by acquiring a set of uncorrelated variables [23]. A robust image hashing method utilizing ring partition and Non-negative Matrix Factorization (NMF) has been presented in [18]. In this approach, the authors construct a rotation-invariant transformed image with ring partition and apply the NMF to the transformed image for hash generation. Their results show good performance to non-malicious distortions for large angle rotation. The image hash generated by dimensionality reduction methods depends on the creation of secondary images. Therefore, a trade-off between efficiency and classification performance would need to be considered when designing an image hashing algorithm using dimensionality reduction technique. Hassan *et al.* [24] proposed a secure and robust PIH algorithm by utilizing Discrete Wavelet Transform (DWT) and NMF. DWT is applied to the input image to generate image features, which are largely invariant under perceptually small non-malicious distortions. The image features are then reduced by utilizing the NMF. Their algorithm is robust against non-malicious distortions, like JPEG compression, Gaussian noise, image scaling, and filtering. Hernandez *et al.* [25] proposed an image hashing algorithm by first performing image normalization and then utilizing singular value decomposition. This scheme has very good robustness performance against geometric distortions but exhibits poor results to other non-malicious distortions [26].

C. Techniques Based on Invariant Properties in the Transformed Domains

This type of hashing technique is based on invariance in the transformed domains (like DCT, DWT, or Discrete Fourier Transform (DFT)). Different schemes use different invariant properties in different domains to construct robust image hashes. Ahmed *et al.* [12] proposed a secure and robust hashing technique for image integrity verification. The proposed technique utilizes the properties of DWT and SHA-1. This technique is robust to non-malicious distortions like JPEG compression and low pass filtering. The advantage of the scheme lies in detection of minute level malicious tampering. Swaminathan *et al.* [27] have proposed a robust PIH technique using the magnitudes of two dimensional Fourier transform coefficients as features to produce a hash vector. This algorithm is resilient to numerous non-malicious distortions like JPEG compression, filtering, and basic geometric operations up to 10° of rotation and 20% of cropping. It also exhibits high discriminative capability and can recognize malicious tampering like a cut-and-paste type of tampering. Lei *et al.* [28] have presented a robust PIH algorithm that calculates the DFT of the invariant moments of significant Radon transform coefficients and normalizes the DFT coefficients to generate hash vector for image integrity verification. Recently, Davarzani *et al.* [29, 30] have presented image hashing algorithms utilizing Center Symmetric Local Binary Pattern (CSLBP), which is applied to matrices obtained using Singular Value Decomposition (SVD) of the input image. The main drawback of CSLBP features is its weak agreement between tamper detection and robustness. This leads to an observation that CSLBP based scheme is not able to identify minute tampering in an image. Chen *et al.* [31] have utilized block truncation coding along with CSLBP for hash generation. The experimental findings exhibited in [31] shows limited robustness. Further, the authors have not elaborated tamper detection ability of their scheme.

Digital images [32, 33] can be easily altered by means of digital tools, which has been developed with the advancement of technology and hence it is quite possible to illegally tamper the image. The key concern regarding any image hashing scheme is the selection of robust features, which do not alter in case of non-malicious manipulations and at the same time vary for deliberate tampering. To accomplish these conditions, a novel PIH scheme is proposed in which a variant of the Local Binary Pattern (LBP) is applied to image structure in the DCT domain. Following are the contributions of this paper:

- We have developed a novel DCT-NRLBP PIH scheme, which exploits DCT domain's structural information for image integrity verification. The proposed DCT-NRLBP scheme identifies minute localized tampering if exists in the image under consideration.
- We have analysed the effect of variable size secondary image, which is achieved by changing the

size of DCT coefficients, on the performance of the DCT-NRLBP scheme.

- We have compared the performance of DCT-NRLBP scheme with some of the of the schemes from literature by varying content preserving manipulation parameters over a range of different values and ROC curves.

The LBP operator, as a hashing scheme, has certain drawbacks when employed in the spatial domain. One of the limitations is that it does not generate stable features required for image integrity verification against most of the content preserving manipulations (with some exceptions like gamma correction). This is due to the fact that inherently, the LBP operator does not have any noise resistive phenomenon incorporated in it. LBP code generated by the LBP operator changes considerably in case of non-malicious distortions. The effect of non-malicious distortions is to disrupt all pixel values in the image, while on the other side, the LBP code does not change a lot in case of minute malicious distortion, because the minute malicious distortion disturbs LBP code slightly. Hence, it is difficult to differentiate malicious tampering from non-malicious content preserving manipulations by merely using the LBP operator in the spatial domain, as evident from the comparative analysis section.

The variant of LBP that has been utilized to overcome the LBP drawback, is Noise Resistance Local Binary Pattern (NRLBP) and this LBP variant has inherently noise catering phenomena built in it [34]. In this paper, the DCT domain of an image, which is the transformed version of spatial domain, is referred to as secondary image and sometimes also known as transformed image. The proposed hashing technique has the ability to detect localized small-scale deliberate tampering and at the same time exhibits robustness against non-malicious distortions. Trivially, NRLBP (or any variant of LBP) is normally applied in spatial domain. One aspect of novelty of this paper is that NRLBP is applied in the DCT domain (i.e. upon secondary image), since DCT domain has certain specific structure, which can be exploited for image integrity verification [35]. The primary reason to select DCT over DFT is its inherent energy compaction capability, which allows the construction of secondary image with fewer DCT coefficients and ultimately provides the trade-off between robustness for content preserving manipulations and minute tamper detection capability. In addition, the DCT assumes the periodicity to be twice as compared to DFT for generating transformed image, which reduces the artifacts induced by image transformation due to boundary discontinuities [36]. Similarly, the DCT is preferred over DWT simply because of its high inherent energy compaction capability and computational efficiency. In case of DWT, the image is decomposed into four sub-bands known as LL, LH, HL and HH sub-bands, where LL sub-band holds approximately the same input image but having half the original spectral resolution, while LH, HL and HH sub-bands contain horizontal, vertical and diagonal edges available in the image respectively. In this paper, we are applying low level feature extraction scheme i.e. NRLBP for hash generation, so only LL sub-band of DWT is suitable for this purpose. The potential issue in generating hand crafted features after applying NRLBP to LL sub-band is poor tamper detection capability due to reduced spectral resolution of LL sub-band.

Algorithm-I: NRLBP Scheme

Input: Read gray-scaled bmp format image.
Output: NRLBP **i**mage histogram.
for All the pixels in an image:
1. Calculate 8-bit binary pattern (C_{NRLBP}) using (1).
2. Compute number of uncertain bits (u_b) in C_{NRLBP}.
2. Calculate uniformity measure (λ).
3. Construct histogram (G_{hist}):
if $u_b = 0$ and $\lambda \leq 2$;
Increment the relevant bin of C_{hist} by 1.
else
if $u_b = 0$ and $\lambda > 2$;
Increment non-uniform bin of C_{hist} by 1.
else
Calculate maximum number of possible uniform patterns (U_p) generated from C_{NRLBP}.
if $U_p = 0$;
Increment non-uniform bin of G_{hist} by 1.
else
$1/U_p$ times increment all relevant uniform bins.
end for

The comparison of the proposed scheme with SVD-NRLBP [37] is also performed and it has been found out that the proposed algorithm shows superior performance than SVD-NRLBP, because DCT domain has much more stable features than SVD domain. In [37], the secondary image formed gets disturbed more than the secondary image formed in the DCT domain in case of non-malicious distortions. Therefore, it can be said that the proposed scheme has more stable features due to DCT inherent compaction power. In addition to this, the secondary image formation in the DCT domain selects only a handful of coefficients and discards high frequency coefficients that are usually associated with non-malicious content preserving manipulations. The proposed scheme considers only a few low frequency coefficients that normally have a higher rate of change with deliberate tampering. In short, it can be stated that the proposed scheme selects more stable features while generating image hash, as compared to the schemes reported in the literature and subsequently exhibits exceptional Receiver Operating Characteristics (ROC) curves. The proposed algorithm is also compared with SVD based CSLBP which is proposed by Davarzani *et al.* [29, 30]. The authors reported in their paper that malicious deliberate tampering must at least be 10% of the original image size for positive detection. This, therefore restricts the use of the algorithm proposed in [29, 30] to identify malicious deliberate tampering in images having smaller than 10% corrupted area. In addition, it has lower values of non-malicious distortion parameters since the scheme does not have any noise resistive mechanism. This results in difficulties for suitable threshold selection to differentiate between deliberate tampering and content preserving manipulations. Consequently, the scheme proposed in [30] can work effectively if tampering is at least 10% of image size, otherwise the scheme will not detect tampering.

The hashing results in this paper exhibits the effectiveness of DCT domain based NRLBP technique. The next section elaborates the NRLBP algorithm. This is followed by the proposed scheme. Then, there is a comparative analysis

section, in which the proposed algorithm is compared with the LBP operator [38] in the spatial domain as an hashing technique, Singular Value Decomposition (SVD) domain NRLBP hashing [37], SVD based CSLBP hashing scheme [30] and Weber Local Binary Pattern Color Angle Representation (WLBP-CAR) hashing scheme [2]. The last section concludes the paper highlighting strengths and added advantage of the proposed hashing scheme.

III. Noise Resistant Local Binary Pattern (NRLBP)

In this paper, we utilize NRLBP algorithm to generate hash vector for an image. The proposed image hashing scheme can detect localized minute level deliberate tampering accompanied by exhibition of robustness against commonly prevalent non-malicious distortions.

The NRLBP scheme preserves local structure of an image in a noisy environment. This is due to the fact that NRLBP has an inbuilt phenomenon to reduce noise effect by utilizing the idea of *uncertain bits* [34]. A bit is categorized as an uncertain bit if the NRLBP scheme is unable to categorically declare it as 0 or 1. The scheme allocates a special symbol X to indicate uncertain bits and a corrective mechanism is utilized subsequently to discover the possible original state of these bits. The NRLBP code (C_{NRLBP}) is generated for every pixel available in an image under consideration. The C_{NRLBP} generation is an area processing operation with a sliding window size of 3×3 pixels. The pixel under consideration (I_c) is subtracted from all neighboring pixels (I_p) one by one in a clockwise direction. The result of each subtraction is thresholded with the help of (1) to acquire an 8-bit binary code (C_{NRLBP}). Each bit of binary code is represented by a_p^n, where n denotes total number of neighboring pixels (I_p) around I_c and p represents neighboring pixel number during subtraction operation. In an area processing operation, a kernel of 3×3 means that the total number of neighboring pixels are eight ($n = 8$), and the value of p indicates pixel number $p = 0,1,2, \ldots ,7$. The subtraction parameter d is equal to $I_c - I_p$. Let the 8-bit C_{NRLBP} is represented as $C_{NRLBP} = \{a_7^8, a_6^8, a_5^8, a_4^8, a_3^8, a_2^8, a_1^8, a_0^8\}$, where a_7^8 is the MSB and a_0^8 is the LSB of C_{NRLBP} binary code.

$$a_p^n = \begin{cases} 0 & if \quad d \le -t; \\ 1 & if \quad d \ge t \ ; \\ X & if \quad |d| < t. \end{cases} \tag{1}$$

The third condition denoted by X in (1) represents an uncertain bit, and its value is predicted after calculating 8-bit binary C_{NRLBP} code for one I_c. The algorithm assigns a value of either 0 or 1 to the uncertain bit (X). The assignment of either 0 or 1 is not random but based on the algorithm attempt to form an 8-bit uniform pattern. The 8-bit C_{NRLBP} code is considered as a uniform code pattern if the maximum value of its uniformity measure (λ) is equal to 2 [39]. The uniformity measure is defined as the number of binary bit transitions existing in a binary code in a circular order. For instance, a binary code 00010000 is uniform as there are only two binary bit transitions. In other words, the binary code pattern has a uniformity measure of 2. Similarly, in another instance, the binary code pattern 01010101 contains 8 binary transitions, therefore the λ for this code is 8. Consequently, this type of code is considered as a non-uniform. The total number of unique uniform LBP codes are 58 as illustrated in Fig. 1. A hollow circle in Fig. 1 denotes 0 and a filled circle denotes 1. All the 58 uniform codes illustrated in Fig. 1 exhibit a maximum of 2-bit transitions in a circular direction.

The histogram of NRLBP algorithm has a total of 59 bins, where 58 bins are reserved for uniform code patterns while only one bin (i.e. 59th) is for non-uniform code patterns. The contribution of all non-uniform code patterns is recorded in this 59^{th} bin. Now moving to a situation, where a C_{NRLBP} pattern has some uncertain bits (X). The NRLBP scheme will attempt to generate all likely uniform codes by replacing X bits with either 0's or 1's to make the C_{NRLBP} a uniform pattern. Hence, all generated uniform codes will increment their corresponding histogram bins by $\frac{1}{\text{Total no.of uniform codes generated}}$. Let the total number of uncertain bits in an 8-bit C_{NRLBP} code pattern be u_b and the total number of uniform patterns generated from an 8-bit C_{NRLBP} be U_p. For example, let $C_{NRLBP} = 1111X000$, the code pattern contains only one uncertain bit ($u_b = 1$). The NRLBP algorithm can generate a maximum of two (i.e. $U_p = 2$) uniform codes; i.e. 11111000 and 11110000. The increment in histogram bins is $1/U_p$ (where $U_p = 2$) relevant to these two generated uniform patterns. In a contrasting situation, the C_{NRLBP} pattern would contain some uncertain bits in such a way that due to the location of the uncertain bits, no uniform code pattern can be generated. In this situation, the algorithm increments just the non-uniform bin (i.e. the 59th bin) by 1. For example, it is impossible for $C_{NRLBP} = 0011X0X1$ to generate even one uniform code. This is because $U_p = 4$ and is treated as a non-uniform pattern. Thus, only the 59th bin is incremented by 1. In a nutshell, it can be reiterated that the NRLBP histogram generation involves comparison of each pixel's gray level to its surrounding neighbors and the number of occurrences of uniform and non-uniform patters are recorded in a histogram.

The main objective of all the PIH schemes is to select robust features. Robust features provide robustness against non-malicious tampering alongside high discriminative capability against malicious tampering. In literature, the NRLBP technique is normally applied in the spatial domain, while in this paper we are applying NRLBP algorithm to the low frequency coefficients that are acquired by calculating the

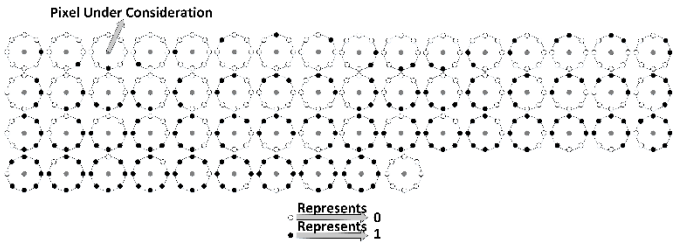


Fig. 1. The 58 uniform code patterns [39].

DCT of the gray scale image. DCT based NRLBP hashing scheme also provides features that are useful, computationally simple, have high discrimination and good robustness. In this paper, we exhibit the fusion of DCT and NRLBP schemes to generate distinctive features, which are able to detect localized small-scale tampering and at the same time exhibiting high robustness against major types of non-malicious distortions.

IV. Proposed Algorithm

The complete flow chart of the proposed algorithm is depicted in Fig. 2. There are four main steps in the hash generation phase, while image integrity verification phase has one additional step for hash comparison. During hash generation stage, the first step is pre-processing. The pre-processing step involves color space conversion, image resizing, Wiener filtering and dividing the input image into smaller portions. The second step involves conversion of image space from spatial domain to the DCT domain. In the third step, stable features are selected for robust hash generation. The fourth and last step involves combining features which are extracted in the third step for final hash generation. The image integrity verification stage involves all the steps of hash generation and an additional hash comparison step. The first four steps of integrity verification stage work the same way as the steps of hash generation. In the additional step, the hash generated locally from the input image through the proposed algorithm and the hash received are compared with each other. If both the hashes are identical or closely related, then the image is declared as authentic otherwise it is considered as forged/tampered and its authenticity is questionable. The proposed algorithm's pseudo code is shown in Algorithm-II.

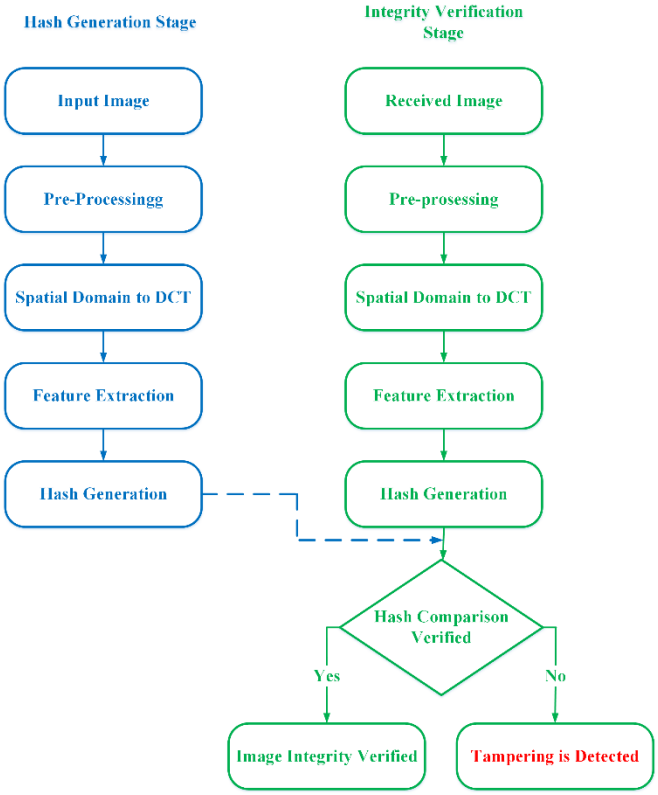


Fig. 2. The complete flow diagram of the proposed algorithm.

Algorithm-II: Proposed Image Hashing Scheme

Input: Read computer vision's general dataset // The dataset contains RGB color space, bmp format images having different dimensions.
Output: Generated image hash.
for All the images in dataset
do
1. Read input image.
2. Conversion of color space to grayscale.
3. Resize grayscale image to 256×256.
4. Divide the resulting image into non-overlapping blocks of size 32×32 pixels.
5. Apply Wiener filter at each non-overlapping block.
6. Construct DCT transformed image block of size 15×15 by using (4).
7. Apply NRLBP algorithm at each Γ_i of image under consideration to get a histogram of size 1×59.
8. Concatenate histograms of all 64 image blocks to get a final hash vector.

end for

The block diagram of the proposed DCT-NRLBP hashing scheme is illustrated in Fig. 3. There are some preprocessing steps involved in the proposed scheme, which include image resizing to 256×256 pixels, color space to gray scale conversion, and dividing into non-overlapping blocks of size 32×32 pixels. The reason for resizing input image to 256×256 pixels is to acquire consistent input image dimensions. The whole idea to uniformize image size is to acquire consistency during image sub-blocking, which is subsequently used to divide the input image into 64 non-overlapping sub-blocks, where each sub-block consists of 32×32 pixels. If the original image is not resized to standard dimensions of 256×256 pixels before sub-blocking stage, then the non-overlapping block size may vary and depends on the dimensions of input image, e.g. for an image of size 300×300 pixels produces 81 blocks of size 32×32 pixels and 9 blocks of size 12×32 pixels, 9 blocks of size 32×12 pixels and one block of size 12×12 pixels. Hence non-standardized input image size generates so many unsymmetrical non-overlapping image blocks, which produce hinderance in exhibiting uniform temper detection capability. Even if the non-overlapping block division is made adaptable to adjust variable input image sizes and having uniform number of pixels in non-overlapping blocks, still tamper detection capability of any block-based image integrity verification scheme is affected due to a trade-off between

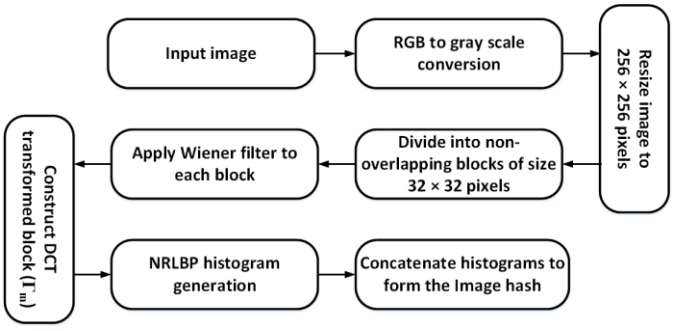


Fig. 3. The proposed image hashing scheme.

block size and tamper detection capability, as increasing block size reduces this capability and vice versa.

In order to exhibit consistent results and dividing input image to fixed non-overlapping blocks, it is necessary to resize the input image to standard dimensions of 256×256 pixels across all input images. In addition, the non-consistent input image generates variable size sub-blocks, which ultimately generates variable length concatenated NRLBP codes during hash generation stage. The generated variable length hash code violets the definition of hash itself, which states that the generated hash should have fixed size string [3]. For example, an image with size 512×512 pixels can be divided into 256 non-overlapping sub-blocks of size 32×32 pixels and the NRLBP generated code length be $L_1 = 15104$ bytes with the concatenated histogram size of 59×256. Let's assume the input image has undergone an image scaling distortion due to channel noise and the image integrity verification stage receives a resized image having dimensions of 128×128 pixels. Now the sub-blocking stage divides this received image into non-overlapping blocks of 32×32 pixels, resulting in generating a total of 16 sub-blocks. The NRLBP code length (L_2) for this recalled image having 16 sub-blocks be $L_2 = 944$ bytes with the concatenated histogram size of 59×16. Now it is not possible to compare L_1 and L_2 during hash comparison stage, although both these codes lengths correspond to same image. Similarly, it is essential for any block-based image hashing scheme to have a uniform image size during hash generation and integrity verification stage to generate consistent and comparable hash lengths. In this regard, we have uniformed the image size in hash generation and image integrity verification stages with dimensions of 256×256 pixels. In addition, image resizing does neither induce image cropping nor translation and rotation artifacts [40]. Since image resizing only aims to exhibit same image content in different dimensions that preserves the global image configuration and does not affect the robustness and tamper detection capability of the proposed DCT-NRLBP scheme. Subsequently, every pre-processed image is divided into 64 sub-blocks, each having dimensions of 32×32 pixels is transformed into DCT domain by using (2) and (3).

$$F_i(a,b) = \frac{2C(a)C(b)}{\sqrt{32 \times 32}} \sum_{x=0}^{31} \sum_{y=0}^{31} f_i(x,y) \cos\frac{(2x+1)a\pi}{2M} \cos\frac{(2y+1)b\pi}{2N}, \quad (2)$$

$$C(\beta) = \begin{cases} \frac{\sqrt{2}}{2} & if \quad \beta = 0, \\ 1 & otherwise. \end{cases}, \quad (3)$$

where $a = 0, 1, \ldots, 31, b = 0, 1, \ldots, 31$ while $f_i(x,y)$ represents the i^{th} image block of size 32×32 pixels in the spatial domain and $F_i(a,b)$ represents DCT transformation of the i^{th} image block. The primary benefit of utilizing block-based method is to locate malicious tampered areas in an image. Then, the image is processed through Wiener filter to smooth its texture. A DCT transformation is subsequently applied to each image block of size 32×32 pixels.

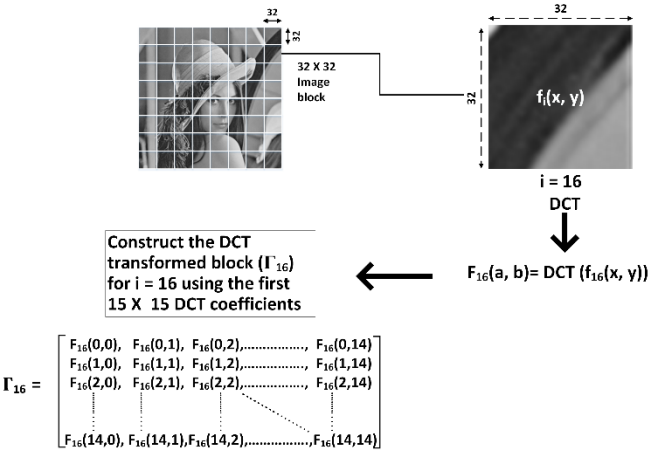


Fig. 4. Example of DCT transformed block illustrating transformation of the 16th image block.

Since each image block $f_i(x,y)$ is of size 32×32 pixels, therefore the size of $F_i(a,b)$ is also 32×32. It is important to decide which DCT coefficients should be selected to form the DCT transformed block (Γ_i). Since DCT is an energy compaction technique, therefore its low frequency coefficients along with a few high frequency coefficients generally preserve the image structure [41]. It is also important to note that if all the DCT coefficients (i.e. 32×32) are collected from the i^{th} block of size 32×32 pixels to form Γ_i, then the robustness of the proposed scheme would decrease. On the contrary, tamper detection ability of the hashing scheme deteriorates if very few DCT coefficients are selected. Hence, the selection of DCT coefficients plays vital part in the performance of the proposed scheme. It is observed after a lot of experimentations that if the first 15×15 DCT coefficients are selected, then in terms of tamper detection capability and robustness to non-malicious operations of proposed scheme exhibits exceptionally good results. The first 15×15 DCT coefficients of i^{th} image block are used to form DCT transformed block (Γ_i), as given by (4).

$$\Gamma_i = \begin{bmatrix} F_i(0,0) & F_i(0,1) & F_i(0,2) & \ldots & F_i(0,14) \\ F_i(1,0) & F_i(1,1) & F_i(1,2) & \ldots & F_i(1,14) \\ F_i(2,0) & F_i(2,1) & F_i(2,2) & \ldots & F_i(2,14) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ F_i(14,0) & F_i(14,1) & F_i(14,2) & \ldots & F_i(14,14) \end{bmatrix} \quad (4)$$

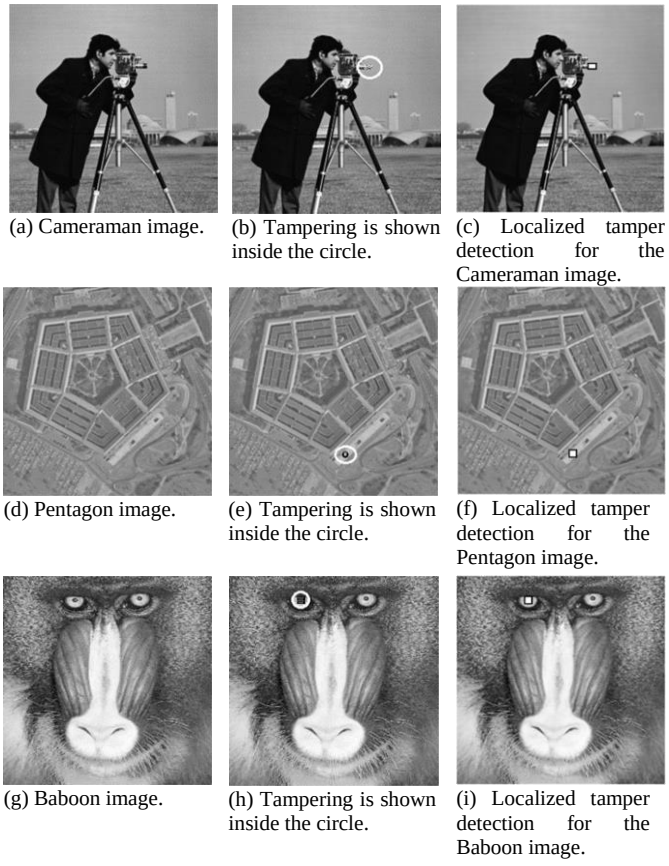
The DCT transformed block Γ_i contains a stable structure of the image block i that would provide robustness to non-malicious distortions and localized minute level tamper detection capability. Equation (4) illustrates the collection of DCT coefficients to form the transformed image block Γ_i. For illustration, the transformation procedure of the 16th image block ($i = 16$) is shown in Fig. 4.

The size of the DCT transformed block (Γ_i) is significantly small in comparison to the size of the original image block. The NRLBP algorithm is applied to the DCT transformed blocks. After rigorous experiments with abundant images, it has been observed that the value of t in (1) should be selected as 40 for effectively applying NRLBP in the DCT domain. The selection of an appropriate value of t is extremely vital, as the robustness and tamper detection ability of the proposed

scheme depends on it. It is important to note that a high value of t tends to generate high number of uniform code patterns (U_p). Consequently, the contribution of one C_{NRLBP} code to a single bin will be very marginal as well as its spread will be above much wider histogram bins. This eventually decreases tamper detection ability of the proposed algorithm because of histogram distribution. Similarly, small value of t will exhibit small number of uncertain bits (u_b), resulting in fewer number of uniform code patterns generated from the C_{NRLBP}. This results in reduction of inherent noise resistive phenomenon and consequently the robustness capability of the proposed scheme will decrease. We have observed that by taking $t = 40$, it is possible to achieve high level of robustness and at the same time minute level of localized malicious tamper detection ability.

V. Experimental Results

There are two basic characteristics of a good image hashing scheme, robustness against non-malicious distortions and localized tamper detection ability. The content preserving manipulations may include, for example, lossy JPEG compression, additive noise, blurring, luminance changes, scaling, etc. To compare hash vectors coming from two sets of images, the normalized correlation coefficient is used. The



(a) Cameraman image. (b) Tampering is shown inside the circle. (c) Localized tamper detection for the Cameraman image.

(d) Pentagon image. (e) Tampering is shown inside the circle. (f) Localized tamper detection for the Pentagon image.

(g) Baboon image. (h) Tampering is shown inside the circle. (i) Localized tamper detection for the Baboon image.

Fig. 5. Original images along with respective tampering. (a) Cameraman image. (b) Malicious tampering of the Cameraman image. (c) Localized tamper detection for the Cameraman image. (d) Pentagon image. (e) Malicious tampering of the Pentagon image. (f) Localized tamper detection for the Pentagon image. (g) Baboon image. (h) Malicious tampering of the Baboon image. (i) Localized tamper detection for the Baboon image.

TABLE I
CHARACTERISTICS OF GENERAL-100 DATASET COLLECTED FROM CVONLINE: IMAGE DATABASES

Number of images	Image Format	Color space	Minimum resolution	Maximum resolution
100	BMP (uncompressed)	RGB	131 × 112	710 × 704

normalized correlation coefficient, r is defined as: [30]:

$$r = \frac{\sum_u \sum_v \left((H'_{uv} - \mu')(H''_{uv} - \mu'')\right)}{\sqrt{\sum_u \sum_v ((H'_{uv} - \mu')^2) \times \sum_u \sum_v ((H''_{uv} - \mu'')^2)}} \quad , \qquad (5)$$

where H' is the hash vector of the original image block, μ' is the mean value of this hash vector (H'), H'' is the hash vector of the distorted/tampered image block and μ'' is the mean value of this hash vector (H''). The length of each hash vector is 1×59 for an arbitrary image block of size 32×32. Generally, the expected value of normalized correlation coefficient is approximately equal to 1 for two visually identical image pairs, while its value starts to decrease with the increase in variances between image pairs. An appropriate value of r must be selected between 0 and 1 to distinguish deliberate tampering and non-malicious manipulations. Let the value of r that discriminate deliberate tampering from content preserving manipulations be represented by the threshold, t_r. The non-malicious manipulations produce less alteration in an image block than deliberate tampering. This means that the value of r decides whether there is deliberate tampering or non-malicious manipulations occur, such that the value of r must be greater than the threshold t_r for successful authentication and less than t_r when deliberate tampering exists in the image under consideration.

In our experiments, we have used computer vision's online General-100 dataset containing variable resolution images available online [42]. The characteristics of this database are given in Table I. All the images in this dataset are of good quality with clear edges.

A. Tamper Detection

To establish the tamper detection ability of the proposed technique, the Cameraman, Pentagon and the Baboon images are taken. These images are shown in Fig. $5(a)$, Fig. $5(d)$ and Fig. $5(g)$, respectively. In case of the Cameraman image, a minute tampering in the lens of the camera was made as shown in Fig. $5(b)$. In case of the Pentagon image, a minute tampering in the lower end is made as shown in Figure $5(e)$ and in case of the Baboon image, the left eyeball was tampered as shown in Figure $5(h)$. One of the novelties of this paper is the ability of the hashing algorithm to detect minute level tampering. Therefore, malicious tampering area in the images are restricted to only 3% of the total image area.

All three of the tampering are successfully detected as exhibited in Fig. $5(c)$, Fig. $5(f)$ and Fig. $5(i)$, respectively. The reason to select these three images as a test case is due to the texture available in these images, as Fig. $5(a)$, shows light texture, Fig. $5(d)$ shows moderate texture and Fig. $5(g)$

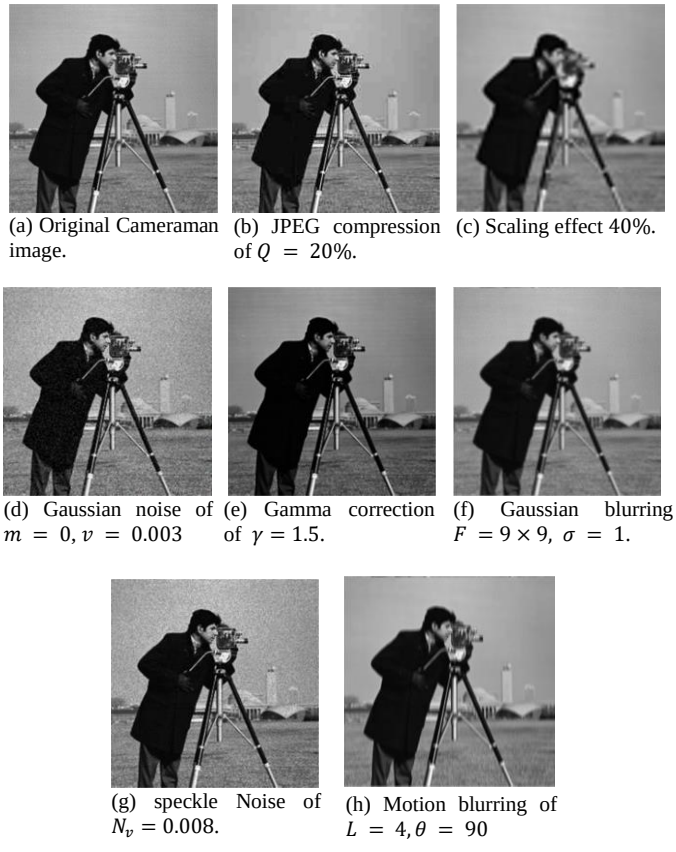
shows rich texture. The value of normalized correlation coefficient for malicious tampering in case of the Cameraman, Pentagon and Baboon images were 0.4643, 0.4416 and 0.2638, respectively.

B. Robustness

A comparison of the hash vector between an undistorted untampered image and its corresponding distorted version is performed to illustrate the robust characteristics of the proposed scheme. The Cameraman, Pentagon and Baboon images are exposed to certain non-malicious manipulations. For the purpose of illustration, the original Cameraman image and its non-malicious distorted manipulations are shown in Fig. 6. As there are 64 blocks in a single image of size 256×256, hence there are 64 values of r for each image under consideration. The minimum value of r for a block out of all the 64 blocks for the Cameraman, Pentagon and the Baboon images after applying non-malicious manipulations are given in Table II. The minimum value of r in all listed non-malicious manipulations for three test images is 0.5747. This result suggests that the value of threshold (t_r) must be less than 0.5747 for positive authentication.

C. Threshold Selection

The minimum value of r for Cameraman, Pentagon and the Baboon images for content preserving distortions is 0.5747, while the maximum value of r among these three images for malicious tampering is 0.4643. It is visible that a remarkable gap of 0.1104 is available between malicious tampering and non-malicious manipulations. Consequently, it becomes a trivial procedure to select threshold t_r to differentiate between malicious tampering and content preserving manipulations. The value of t_r may be adjusted between 0.4643 and 0.5747. To reach a solid conclusion, the proposed hashing scheme was applied to the image set given in [42], the results suggest that $t_r = 0.53$ is suitable to differentiate between malicious tampering and content preserving manipulations.



(a) Original Cameraman image. (b) JPEG compression of $Q = 20\%$. (c) Scaling effect 40%.

(d) Gaussian noise of $m = 0, v = 0.003$ (e) Gamma correction of $\gamma = 1.5$. (f) Gaussian blurring $F = 9 \times 9,\ \sigma = 1$.

(g) speckle Noise of $N_v = 0.008$. (h) Motion blurring of $L = 4, \theta = 90$

Fig. 6. Non-malicious distorted versions of the Cameraman image. (a) Original Cameraman image. (b)~(h) non-malicious distortions. (b) JPEG compression. (c) Scaling effect. (d) Gaussian noise. (e) Gamma correction. (f) Gaussian blurring. (g) Speckle noise. (h) Motion blurring.

D. Localized Tamper Detection Capability

Images can easily be modified to change their original contents with the help of image alteration software. A number of techniques are utilized to detect localized tampered regions, for example, passive forgery detection and fragile watermarking, etc; [43, 44]. The key benefit of the proposed scheme is that it does not degrade image content. The localized tamper detection in this paper is accomplished by employing block-based comparison of hash values. In block-based comparison, each image is first divided into non-overlapping blocks. Then, the hash vector of each image block is generated with any PIH scheme and is embedded into the header of that image. During the image integrity verification stage, the hash of each image block is computed again from the image blocks and compared with the hash vector in the header file.

The selection of a suitable block size is very vital in the localized tamper detection. The block size manages the tradeoff between the hash size and the size of localized tampered region, as well as between the hash size and tamper detection performance. A larger block size generates hash of small size as an advantage, but large localized region and high false detection as a disadvantage, and vice versa. Hence, the selection of a suitable block size is very essential. In the proposed algorithm, a block size of 32×32 pixels is selected in order to have suitable hash size, appropriate localized tampering and low false detection [29, 30]. Figure 7 shows the Lena image, its tampered version (splicing image forgery) and localized tamper detection. It is important to note that the proposed scheme identifies the localized tampered regions despite small tampering in the image.

TABLE II
MINIMUM CORRELATION COEFFICIENT VALUE R FOR THE IMAGE BLOCK OUT OF THE 64 BLOCKS.

Non-malicious distortions along with their selected parameters	Correlation Coefficient (r)		
	Cameraman Image	Pentagon Image	Baboon Image
JPEG compression: $Q = 20\%$	0.8701	0.6735	0.8495
Gaussian noise: m $= 0$, v $= 0.003$	0.8445	0.7350	0.7859
Speckle noise: $N_v = 0.008$	0.8578	0.7640	0.8060
Gaussian blurring: $F_s = 9 \times 9, \sigma = 1$	0.7372	0.5859	0.6150
Motion blurring: L $= 4, \theta = 90$	0.7496	0.6151	0.6390
Gamma correction: $\gamma = 1.5$	0.6622	0.8471	0.7928
Scaling: s = 40%	0.5747	0.5838	0.6529

(a) Original Lena image. (b) Tampering is shown inside the circle. Maximum tampered area is approximately 3% of the image (c) Localized tamper detection.

Fig. 7. (a) Lena image. (b) Tampered version of Lena image. (c) Localized tamper detection.

E. Receiver Operating Characteristics Curve

Receiver Operating Characteristics (ROC) analysis is used to gauge the performance of the proposed algorithm in terms of robustness and tamper detection. The ROC curve is a plot between false positive probability (P_{FP}) and false negative probability (P_{FN}) as the threshold is varied. These two probabilities are defined by Equations (6) and (7), respectively [12].

$$P_{FP} = \frac{N_A^T}{NT} \tag{6}$$

$$P_{FN} = \frac{N_T^A}{NA} \tag{7}$$

In (6), N_A^T denotes the total number of tampered image blocks categorized as true, whereas NT denotes the total number of tampered image blocks. Likewise, in (7), N_T^A denotes the total number of true image blocks detected as tampered and NA denotes the total number of true image blocks.

There is always a tradeoff between P_{FP} and P_{FN}. This trade-off is the basis to quantify tamper detection capability of any PIH scheme. The P_{FP} and the P_{FN} probabilities are inversely proportional. Consequently, it becomes challenging to select an appropriate value of t_r as both the probabilities need to be balanced. For a hashing system having a higher false positive probability implies that there is a risk of wrong image integrity verification. Similarly, a system having a higher false negative probability would reject genuine samples frequently. There is a need to balance robustness and tamper detection capability at some desired level. The operating point for the ROC curve may vary depending upon the application scenario of a hashing system. For instance, if a user wants the hashing system to have zero false positive probability so that a tampered image block would never get authenticated, then the false negative probability would increase. The ROC operating point for the proposed system is selected in such a way that both the probabilities are small enough to use it in real life image integrity verification applications.

Figure 8 shows the ROC performance of the proposed algorithm for different types of content preserving distortions. The database in [42] is used to obtain the ROC curves. It is quite encouraging that for low P_{FP}, low P_{FN} is accomplished. In cases of JPEG compression, Gaussian noise, speckle noise, Gaussian blurring and motion blurring, if we operate at values of $P_{FP} = 0.035$ then P_{FN} is less than 0.04. Similarly, for image scaling and gamma correction at $P_{FP} = 0.05$, the P_{FN} is

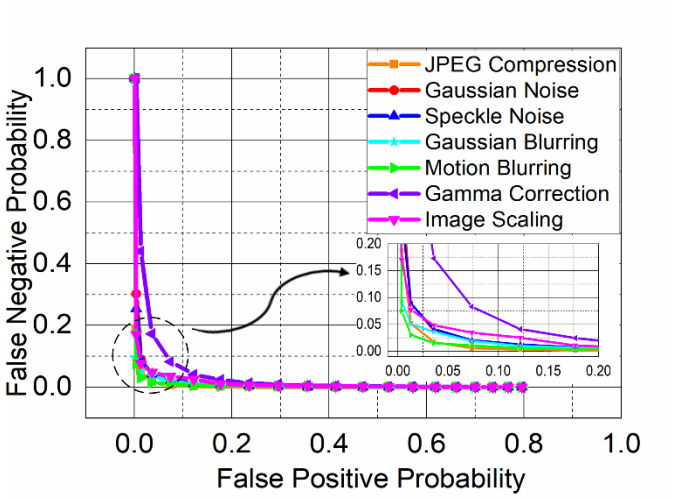


Fig. 8. The receiver operating characteristics curves for non-malicious distortions.

approximately equal to 0.04 and 0.125, respectively. In short, the values of P_{FP} and P_{FN} are much better for JPEG compression, Gaussian noise, speckle noise, Gaussian blurring, motion blurring and image scaling, while the values of P_{FN} are a bit higher in case of gamma correction. It is also important to note that in the current scenario, the false positive probabilities and false negative probabilities are calculated for a block of size 32×32 pixels, taken from an image of size 256×256 pixels. Hence, the false acceptance of the proposed scheme, for a complete image of size 256×256 pixels would be very small than the individual block's false acceptance probability because all the 64 blocks need to be falsely accepted for a false verification of the complete image.

F. DCT coefficient selection

The selection of appropriate number of DCT coefficients for each image sub-block is very important parameter, which affects the performance characteristics of the proposed DCT-NRLBP hashing scheme. We have selected first 15×15 DCT coefficients for forming Γ_i according to (4). The main reason to select these particular coefficients is to achieve best robustness and minute tamper detection capability. In this regard, we observe the performance of the DCT-NRLBP scheme against varying number of DCT coefficients, and

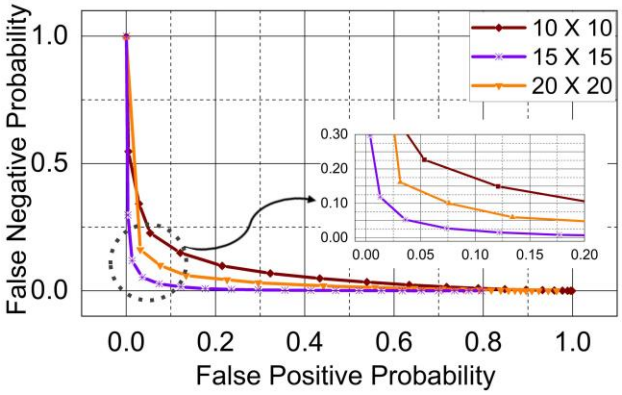


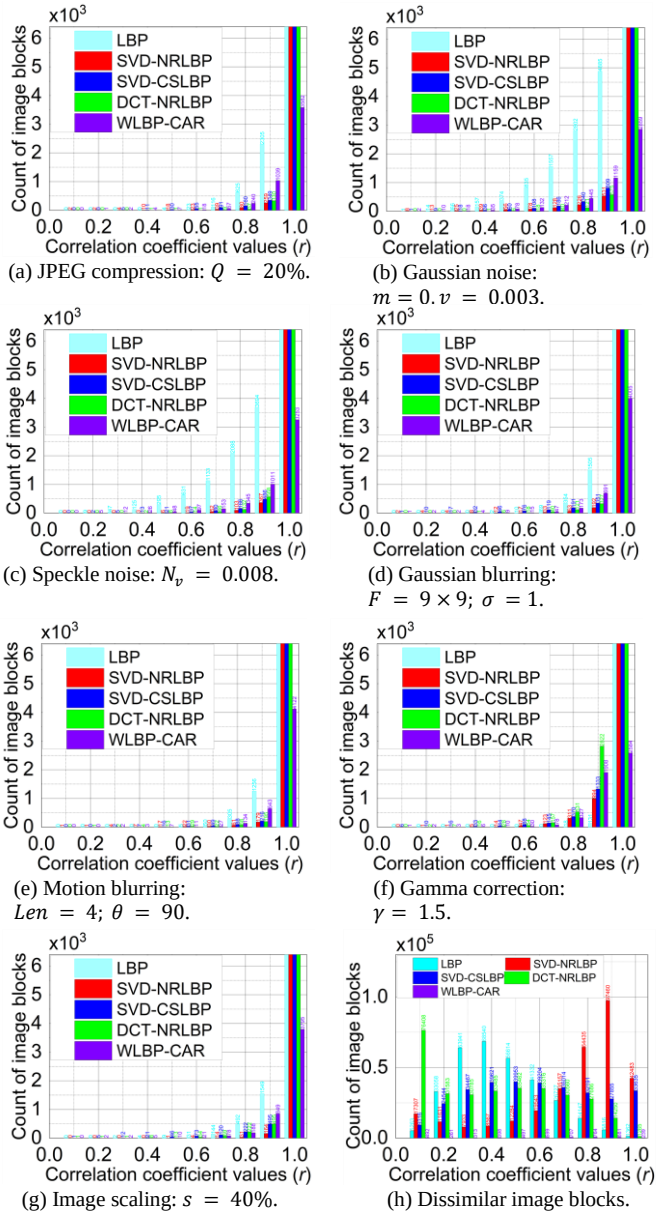
Fig. 9. The ROC performance comparison by changing size of DCT coefficients. The curves indicate best performance when first 15×15 DCT coefficients are selected for an image sub-block of size 32×32 pixels.

accomplish the best ROC performance when the first 15×15 DCT coefficients are selected for an image sub-block of size 32×32 pixels as shown in Fig. 9. The curves in Fig. 9 are plotted with three different number of DCT coefficients, i.e. $10 \times 10, 15 \times 15$ and 20×20. All these coefficients that form secondary image blocks are generated using (4). The P_{FN} in Fig. 9 is computed by assuming original images [42] and their non-malicious distorted versions as pair of similar images. The employed parameters to generate non-malicious distorted versions are the same as given in Table II. The P_{FP} is calculated by assuming each original image to be visually different from all other images available in [42]. This means that each sub-block in one image acts as tampered sub-block for the other image. Then ROC performance is plotted between P_{FP} and P_{FN} with different dimensions of Γ_i as shown in Fig. 9. In Fig. 9, it is evident that the best performance is achieved when the size of Γ_i be selected as 15×15 coefficients. It is also important to note Γ_i always include low frequency coefficients and exclude high frequency coefficients because low frequency DCT coefficients are primarily responsible for preserving image structure [41], and their exclusion will not represent the actual image semantics.

VI. Comparative Analysis

A. Performance Comparison using Distribution of Correlation Coefficient

The performance comparison using distribution of correlation coefficients is performed to reinforce the fact that the value of t_r is able to differentiate between deliberate tampering and non-malicious manipulations. In this regard, a comparison is made to evaluate the performance of the proposed algorithm DCT-NRLBP with competing schemes namely LBP, SVD-NRLBP, SVD-CSLBP and WLBP-CAR in terms of distribution of correlation coefficients. To assess robustness against non-malicious distortions and minute tamper detection capability a comparison among the distribution of correlation coefficient is performed with the LBP [38], SVD-NRLBP [37], SVD-CSLBP [30], WLBP-CAR [2] and the proposed DCT-NRLBP scheme. For the sake of simplicity, each image in the dataset [42] is modified by non-malicious distortions like JPEG compression, Gaussian noise, speckle noise, Gaussian blurring, motion blurring, gamma correction and image scaling as per non-malicious distortion parameters listed in first column of Table II. All the original images and their non-malicious distorted versions are considered as pair of similar images. Due to the fact that the LBP [38], SVD-NRLBP [37], SVD-CSLBP [30] and the proposed DCT-NRLBP schemes are block based, hence for the sake of evaluation, each image is first subdivided into blocks (block size 32×32) and then each block is converted to its corresponding hash code, while WLBP-CAR [2] scheme takes the whole image as input and does not divide into blocks for computing hash code. The correlation coefficient (r) given by (5) is calculated between the hash of the original image block and the hash of its corresponding non-malicious distorted version (for example, JPEG compression, etc.). There are 64 blocks of size 32×32 pixels for comparison between the original image and its non-malicious distorted form for [30, 37, 38] and proposed DCT-NRLBP.



(a) JPEG compression: $Q = 20\%$. (b) Gaussian noise: $m = 0. v = 0.003$.
(c) Speckle noise: $N_v = 0.008$. (d) Gaussian blurring: $F = 9 \times 9$; $\sigma = 1$.
(e) Motion blurring: $Len = 4$; $\theta = 90$. (f) Gamma correction: $\gamma = 1.5$.
(g) Image scaling: $s = 40\%$. (h) Dissimilar image blocks.

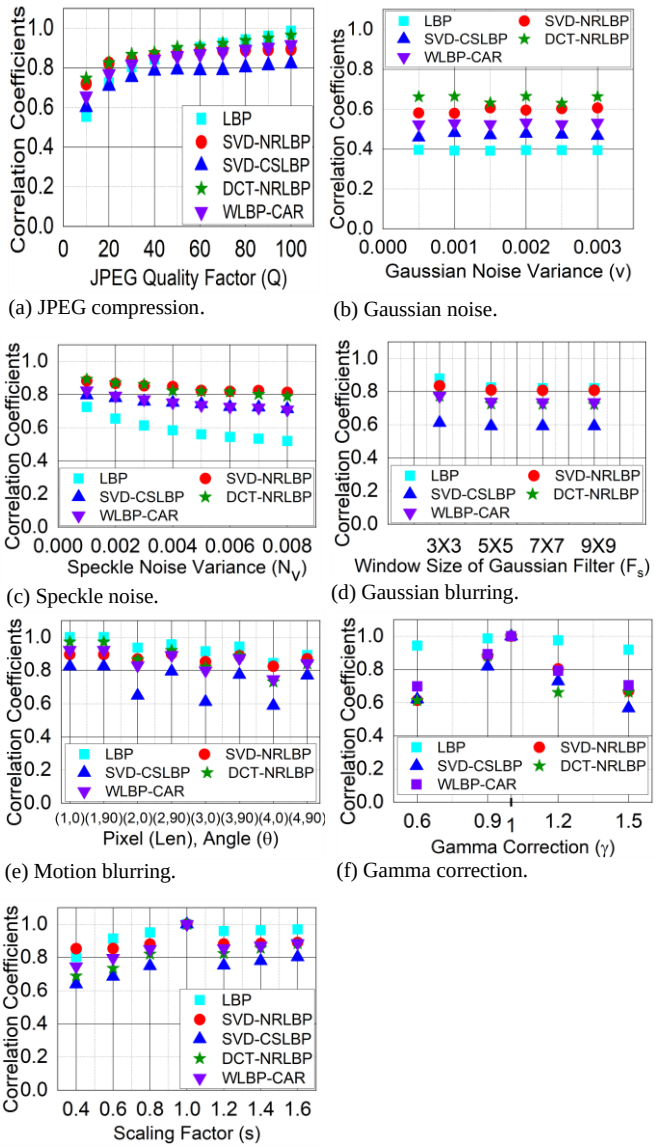
Fig. 10. Distribution of correlation coefficients for LBP, SVD-NRLBP, SVD-CSLBP, DCT-NRLBP and WLBP-CAR PIH schemes. (a)~(g) Distribution of correlation coefficients between the original image blocks and perceptually similar image blocks for different non-malicious distortions. (h) Distribution of correlation coefficients between dissimilar image blocks.

Subsequently, the total number of blocks (B_N) are counted against a particular value of r. The values of r are quantized to the following discrete steps $\{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0\}$. In the end, a bar graph is plotted between the quantized values of r against B_N. The distribution of correlation coefficients for [2, 30, 37, 38] and DCT-NRLBP is shown in Fig. 10. As WLBP-CAR hashing scheme [2] is not a block based scheme. This results a reduction in total number of entries by factor of 64 incomparison to [38], [37], [30] and proposed DCT-NRLBP scheme. which makes a bit doubous to compare quantity of correlation coefficients of [2] with [30, 37, 38] and proposed DCT-NRLBP but nevertheless the overall distribution of correlation coefficients for [2] is illustrated in Fig. 10.

Figure $10a{\sim}10g$ shows the distribution of correlation coefficients for JPEG compression, Gaussian noise, speckle noise, Gaussian blurring, image scaling, motion blurring and gamma correction, respectively.Similarly, the distribution of correlation coefficient for dissimilar image pairs is computed as shown in Fig. $10h$. The x-axis represents quantized values of r and the y-axis represents B_N. In case of dissimilar image blocks as shown in Fig. $10h$, the bar graph should be in such a way that it shows high concentration of image blocks close to $r = 0.1$ and B_N should decrease towards increasing values of r. The rate of decay for B_N for different images should be fast, so that there are small number of dissimilar blocks having high value of correlation coefficient (r), or in other words high similarity index. It is evident from the Fig. $10h$ that the proposed scheme exhibits lower concentration of B_N for distinct image pairs for higher values of r, indicating low P_{FP} as compared to other algorithms [30, 37, 38]. On the other hand, a good PIH scheme should have highest concentration of image blocks close to $r = 1$ for non-malicious distortions and the concentration of blocks should increase towards higher values of r, as visually similar images should have high similarity index. It is quite clear from Fig. $10(a){\sim}(d)$ that the proposed scheme has highest rate of decay for JPEG compression, Gaussian noise, speckle noise and Gaussian blurring, while in case of motion blurring, gamma correction and image scaling Fig. $10(e){\sim}(g)$ B_N decays at such fast rate that there are very few blocks left beyond t_r value. It is also noted that in case of gamma correction, the LBP scheme exhibits exceptional performance having small values of B_N other than at $r = 1$.

B. Performance Comparison by Varying Non-malicious Distortion Parameters

The performance comparison by varying non-malicious distortion parameters is performed to demonstrate the effectiveness of the DCT-NRLBP over a range of different non-malicious parameter settings. Fig. 11 shows the scatter plot for the proposed DCT-NRLBP scheme alongside with some schemes from the literature [2, 30, 37, 38] to determine the maximum bounds of robustness against varying non-malicious distortions. The x-axis represents varying non-malicious distortion parameter and the y-axis depicts average minimum correlation coefficient value. Each non-malicious distortion parameter is varied numerous times to validate the performance of the DCT-NRLBP algorithm. In Fig. 11, JPEG quality factor, Gaussian noise variance, speckle noise variance, Gaussian blurring, motion blurring, gamma correction and image scaling are varied $10, 6, 8, 4, 8, 5$ and 7 times respectively to check the robustness of the proposed DCT-NRLBP scheme. For a single image under evaluation, there exists 64 image blocks to be compared for [30, 37, 38] and proposed DCT-NRLBP scheme while WLBP-CAR is not a block based scheme, so it produces a single value of r for one image under consideration. This means, there are be 64 correlation coefficients for one comparison involving two images, each having a size of 256×256 pixels for [30, 37, 38] and DCT-NRLBP scheme. Only single value corresponds to minimum correlation coefficient out of 64 values is taken (to illustrate worst case scenario). After calculating minimum



(a) JPEG compression. (b) Gaussian noise.

(c) Speckle noise. (d) Gaussian blurring.

(e) Motion blurring. (f) Gamma correction.

(g) Image scaling.

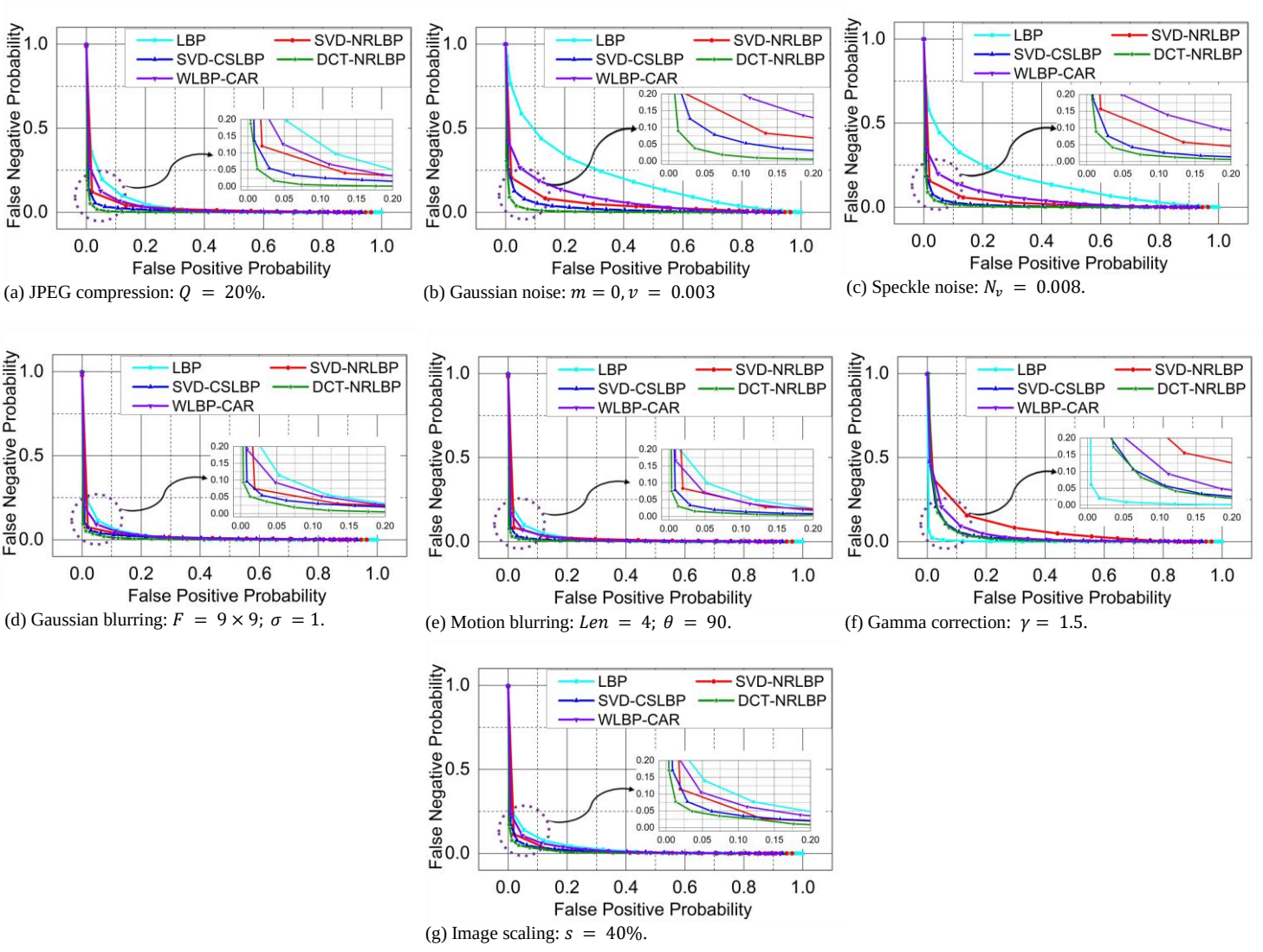
Fig. 11. Performance comparison of LBP, SVD-NRLBP, SVD-CSLBP, DCT-NRLBP and WLBP-CAR by varying content preserving manipulations parameters over a range of values. The x-axis and y-axis correspond to variable non-malicious distortion parameters and average of minimum block correlation coefficients respectively.

correlation coefficients for all the images of dataset [42], the average value was computed to plot the average minimum correlation coefficient against a set of varying non-malicious parameters. The value of r against all these contents preserving manipulation should ideally be 1, or close to 1, but in practical scenarios it is always less than 1 and at the same time must always be greater than the threshold (t_r) as a good performance benchmark. It is observed that average minimum block correlation coefficients for JPEG compression, Gaussian noise, and Speckle noise for the proposed algorithm is better when compared to other hashing schemes [2, 30, 37, 38] as shown in Fig. 11. In case of Gaussian blurring, motion blurring, gamma correction and image scaling the value of r is always greater than the selected t_r. If we compare the proposed scheme with the LBP operator [38], it looks like that in some situations like Fig.

$11f$ and $11g$, the LBP operator shows better performance as the values of r are higher than their counterparts. However, the overall performance can only be revealed through the ROC graphs, presented in the next sub-section due the false positive constraint of any algorithm. As, in case of LBP operator there are high values of P_{FP}. Similarly, the average minimum block correlation coefficients for the SVD-NRLBP scheme should always be above 0.65, as the reported threshold for this algorithm is $t_r = 0.65$. However, it is visible from Fig. $11b$ that in case of Gaussian noise, the value of r is less than 0.65 at all varying noise variance levels. Finally, in case of SVD-CSLBP's and WLBP-CAR schemes, the results always show smaller values of r against all sort of non-malicious distortions in all situations, potentially indicating poor performance in terms of robustness.

C. Performance Comparison using the ROC Curves

The Receiver operating characteristics (ROC) is an excellent way to visualize the best performing scheme under defined malicious and non-malicious parameters. ROC curves measure the tradeoff between robustness and tamper detection ability of a PIH technique. Figure 12 provides a comparison between the proposed DCT-NRLBP and previously reported hashing schemes [2, 30, 37, 38] in terms of the ROC curves. The DCT-NRLBP scheme exhibits high level of supremacy over the other three schemes. It is quite clear from the ROC curves that the DCT-NRLBP scheme demonstrates superior performance against competing schemes for JPEG compression (Fig. $12a$), Gaussian noise (Fig. $12b$), speckle noise (Fig. $12c$), Gaussian blurring (Fig. $12d$) motion blurring (Fig. $12e$) and image scaling (Fig. $12g$). In case of gamma correction (Fig. $12f$), the LBP operator outperforms others by a fine margin. The reason for LBP operator's exceptional performance in this case is hidden in its ability to cancel the effect of constant level gray scale added or subtracted from the image, provided that the image does not get saturated (i.e. either becomes full white or full black). As gamma correction distortion is the one which controls the brightness of the image, hence any change in brightness effect is cancelled by inherent ability of the LBP operator, indicating



(a) JPEG compression: $Q = 20\%$. (b) Gaussian noise: $m = 0, v = 0.003$ (c) Speckle noise: $N_v = 0.008$.

(d) Gaussian blurring: $F = 9 \times 9$; $\sigma = 1$. (e) Motion blurring: $Len = 4$; $\theta = 90$. (f) Gamma correction: $\gamma = 1.5$.

(g) Image scaling: $s = 40\%$.

Fig. 12. The ROC comparison for LBP, SVD-NRLBP, SVD-CSLBP, DC-NRLBP and WLBP-CAR. Proposed DCT-NRLBP scheme demonstrates superior performance against competing schemes for (a) JPEG compression, (b) Gaussian noise, (c) speckle noise, (d) Gaussian blurring, (e) motion blurring and (g) image scaling. In case of (f) gamma correction, the LBP operator outperforms all competing techniques.

TABLE III
HASH LENGTH COMPARISON BETWEEN LBP, SVD-NRLBP, SVD-CSLBP, WLBP-CAR AND DCT-NRLBP IMAGE HASHING SCHEMES.

Hashing scheme	Hash Length (bytes)
LBP [38]	16384
SVD-NRLBP [37]	3776
SVD-CSLBP [30]	4096
WLBP-CAR [2]	90
DCT-NRLBP (proposed)	3776

excellent performance against gamma correction distortion Fig. $12(f)$. The reason why our scheme does not outperform LBP operator is due to the fact that the proposed scheme takes DCT of input image and the first component of DCT domain represents DC level available in an image, hence any change in brightness of image may affect the DC coefficient, although we have incorporated NRLBP alongside DCT but any distortion coming from brightness changes is not nullified as efficiently as done by the LBP operator. It is also due to the fact that we are only looking for uniform patterns in the code while the LBP operator considers all the available 256 patterns in an image. As the noise in case of gamma correction is only due to brightness change and the relevant LBP code does not get affected by brightness change in the image, hence LBP outperforms the DCT-NRLBP scheme for gamma correction as evident from Fig. $12f$. This is the only scenario where LBP operator outperforms the DCT-NRLBP scheme, while in all other situations, the proposed DCT-NRLBP scheme performs well above the performance of LBP operator. This is due to the fact that the proposed scheme does not only cater spatial domain variations through DCT domain's AC coefficient but also utilizes its DC coefficient that holds information regarding image's gray level available in spatial domain, which is essential for robustness during JPEG compression, gaussian blurring, motion blurring and image scaling type of non-malicious distortions.

D. Comparison in-terms of Hash Length

In order to generate hash using LBP operator [38], there are 64 histograms of size 1×256 corresponding to 64 image blocks (the size of each image block is 32×32 pixels). The length of the hash vector for a single image block is 1×256 because there are $2^8 = 256$ unique labels that exist in the LBP scheme. Consequently, the total hash length of an input image having 256×256 pixels will be 64×256 (16384 bytes). In case of SVD-NRLBP [37] and the proposed DCT-NRLBP image hashing schemes, there are 64 histograms of size 1×59 because there are only 59 bins available in the NRLBP algorithm, hence the length of the hash vector for a single image block of size 32×32 pixels is 1×59. The length of hash vector for the input image of size 256×256 pixels would be 64×59 (3776 bytes). Similarly, in case of SVD-CSLBP [30] scheme, there are a total of 64 histograms corresponding to 64 image blocks and the length of hash vector for each block is 1×64 as reported in [30], therefore, the hash length for a complete image of size 256×256 is 4096. The authors reported a 90 digit long hash length for WLBP-CAR [34] hashing scheme. A comparison on hash lengths between LBP operator [38], SVD-NRLBP [37], SVD-CSLBP [30], WLBP-CAR [34] and the proposed DCT-NRLBP is given in Table III, which indicates that the hash length of proposed DCT-NRLBP is smaller than hash lengths of schemes reported [30, 38] and is equal to scheme reported in [37], while the hash length of scheme reported in [2] is smaller than DCT-NRLBP, because the reported scheme in [2] is not a block based scheme.

VII. CONCLUSION

In this paper, a novel DCT-NRLBP PIH scheme is proposed that utilizes block based NRLBP features. Experimental results reveal that the proposed scheme exhibits good robustness to non-malicous manipulations and can detect minute level tampering with tamper localization. The ROC curves suggest that the proposed scheme is able to differentiate between deliberate malicious tampering and non-malicious manipulations, provides high robustness and tamper detection capability. To the best of our knowledge, this is the first time that NRLBP method is employed in the DCT domain for image hashing. The proposed algorithm can detect localized deliberate malicious tampering as small as 3%. of the image size successfully. The proposed DCT-NRLBP technique is observed to be robust against JPEG compression, Gaussian noise, speckle noise, Gaussian blurring, motion blurring, gamma correction and image scaling. The DCT-NRLBP calculates image hash by analyzing complete image irrespective of the fact that there is any texture available or not, unlike the PIH technique proposed in [45] that exploits only a specific image region where feature points are used to calculate an image hash.

The comparative analysis using the ROC curves reveals that the proposed DCT-NRLBP scheme's threshold can be selected in such a way that both the probability of false positive and probability of false negative are minimal. The selection of a suitable threshold becomes easy because there is sufficient gap between malicious tampered images and non-malicious distorted versions. The scatterplot for varying content preserving manipulation parameters exhibits that the proposed PIH algorithm can withstand a wide range of content preserving manipulations. The hash size comparison shows that the proposed scheme requires less memory to store hash values in comparison to other block based schemes.

REFERENCES

[1] M. Wu, Y. Mao, and A. Swaminathan, "A signal processing and randomization perspective of robust and secure image hashing," in *2007 IEEE/SP 14th Workshop on Statistical Signal Processing*, 2007, pp. 166-170: IEEE.

[2] C. Qin, Y. Hu, H. Yao, X. Duan, and L. J. I. A. Gao, "Perceptual Image Hashing Based on Weber Local Binary Pattern and Color Angle Representation," *IEEE Access*, vol. 7, pp. 45460-45471, 2019.

[3] W. Stallings, *Cryptography and network security: principles and practice*. Pearson Upper Saddle River, 2017.

[4] M. Paul, R. K. Karsh, and F. A. Talukdar, "Image Hashing based on Shape Context and Speeded Up Robust Features (SURF)," in *2019 International Conference on Automation, Computational and Technology Management (ICACTM)*, 2019, pp. 464-468: IEEE.

[5] J. Holmgren and A. Lombardi, "Cryptographic hashing from strong one-way functions (or: One-way product functions and their

applications)," in *2018 IEEE 59th Annual Symposium on Foundations of Computer Science (FOCS)*, 2018, pp. 850-858: IEEE.

[6] H. Yang, J. Yin, and Y. Yang, "Robust Image Hashing Scheme Based on Low-Rank Decomposition and Path Integral LBP," *IEEE Access*, vol. 7, pp. 51656-51664, 2019.

[7] F. Khelaifi and H. He, "Perceptual image hashing based on structural fractal features of image coding and ring partition," *Multimedia Tools and Applications*, pp. 1-20, 2020.

[8] Z. Tang, Y. Yu, H. Zhang, M. Yu, C. Yu, and X. Zhang, "Robust image hashing via visual attention model and ring partition," *Mathematical Biosciences and Engineering*, 2019.

[9] M. Sajjad, I. U. Haq, J. Lloret, W. Ding, and K. Muhammad, "Robust Image Hashing based Efficient Authentication for Smart Industrial Environment," *IEEE Transactions on Industrial Informatics*, 2019.

[10] Y. Li, L. Wan, T. Fu, and W. Hu, "Piecewise supervised deep hashing for image retrieval," *Multimedia Tools and Applications*, vol. 78, no. 17, pp. 24431-24451, 2019.

[11] L. Du, Z. Chen, and A. T. Ho, "Binary multi-view perceptual hashing for image authentication," *Multimedia Tools and Applications*, pp. 1-23, 2020.

[12] F. Ahmed, M. Y. Siyal, and V. U. J. S. P. Abbas, "A secure and robust hash-based scheme for image authentication," *Signal Processing, Elsevier*, vol. 90, no. 5, pp. 1456-1470, 2010.

[13] H. Liu, A. Kadir, and J. Liu, "Keyed Hash Function Using Hyper Chaotic System With Time-Varying Parameters Perturbation," *IEEE Access*, vol. 7, pp. 37211-37219, 2019.

[14] C. Chaudhary, P. Goyal, N. Goyal, and Y.-P. P. Chen, "Image retrieval for complex queries using knowledge embedding," *ACM Transactions on Multimedia Computing, Communications, Applications*, vol. 16, no. 1, pp. 1-23, 2020.

[15] C. Chaudhary, P. Goyal, D. N. Prasad, and Y.-P. P. Chen, "Enhancing the Quality of Image Tagging Using a Visio-Textual Knowledge Base," *IEEE Transactions on Multimedia*, vol. 22, no. 4, pp. 897-911, 2019.

[16] R. Venkatesan, S.-M. Koon, M. H. Jakubowski, and P. Moulin, "Robust image hashing," in *Proceedings 2000 International Conference on Image Processing (Cat. No. 00CH37101)*, 2000, vol. 3, pp. 664-666: IEEE.

[17] Z. Tang, Y. Dai, X. Zhang, and S. Zhang, "Perceptual image hashing with histogram of color vector angles," in *International Conference on Active Media Technology*, 2012, pp. 237-246: Springer.

[18] Z. Tang, X. Zhang, and S. Zhang, "Robust perceptual image hashing based on ring partition and NMF," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 3, pp. 711-724, 2013.

[19] Y. Zhao, S. Wang, X. Zhang, H. Yao, and security, "Robust hashing for image authentication using Zernike moments and local features," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 55-63, 2012.

[20] L. S. Sebastian, A. Varghese, and T. Manesh, "Image authentication by content preserving robust image hashing using local and global features," *Procedia Computer Science*, vol. 46, pp. 1554-1560, 2015.

[21] R. K. Karsh, A. Saikia, and R. H. Laskar, "Image authentication based on robust image hashing with geometric correction," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25409-25429, 2018.

[22] S. Eskenazi, B. Bodin, P. Gomez-Krämer, and J.-M. Ogier, "A perceptual image hashing algorithm for hybrid document security," in *2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR)*, 2017, vol. 1, pp. 741-746: IEEE.

[23] S. T. Roweis and L. K. Saul, "Nonlinear dimensionality reduction by locally linear embedding," *Science*, vol. 290, no. 5500, pp. 2323-2326, 2000.

[24] A. M. Hassan, Y. M. Hasan, and M. A. Wahab, "Robust visual hashing for image authentication," in *International Conference on Communications and Information Technology Computing*, 2012, pp. 763-767.

[25] R. A. P. Hernandez, M. N. Miyatake, and B. M. Kurkoski, "Robust image hashing using image normalization and SVD decomposition," in *2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*, 2011, pp. 1-4: IEEE.

[26] Y. Liu and Y. Xiao, "A robust image hashing algorithm resistant against geometrical attacks," *Radioengineering*, vol. 22, no. 4, pp. 1072-1082, 2013.

[27] A. Swaminathan, Y. Mao, M. Wu, and security, "Robust and secure image hashing," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 215-230, 2006.

[28] Y. Lei, Y. Wang, and J. Huang, "Robust image hash in Radon transform domain for authentication," *Signal Processing: Image Communication*, vol. 26, no. 6, pp. 280-288, 2011.

[29] R. Davarzani, S. Mozaffari, and K. Yaghmaie, "Image authentication using LBP-based perceptual image hashing," *Journal of AI and Data Mining*, vol. 3, no. 1, pp. 21-30, 2015.

[30] R. Davarzani, S. Mozaffari, and K. Yaghmaie, "Perceptual image hashing using center-symmetric local binary patterns," *Multimedia Tools and Applications*, vol. 75, no. 8, pp. 4639-4667, 2016.

[31] X. Chen, C. Qin, and P. Ji, "Perceptual image hashing using block truncation coding and local binary pattern," in *2015 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, 2015, pp. 856-859: IEEE.

[32] H. Lee and Y.-P. P. Chen, "Cell morphology based classification for red cells in blood smear images," *Pattern Recognition Letters*, vol. 49, pp. 155-161, 2014.

[33] H. Lee and Y.-P. P. Chen, "Image based computer aided diagnosis system for cancer detection," *Expert Systems with Applications*, vol. 42, no. 12, pp. 5356-5365, 2015.

[34] J. Ren, X. Jiang, and J. Yuan, "Face and facial expressions recognition and analysis," in *Context Aware Human-Robot and Human-Agent Interaction*: Springer, 2016, pp. 3-29.

[35] E. Armas Vega, A. Sandoval Orozco, L. García Villalba, and J. Hernandez-Castro, "Digital Images Authentication Technique Based on DWT, DCT and Local Binary Patterns," *Sensors*, vol. 18, no. 10, p. 3372, 2018.

[36] R. Gonzalez and R. Woods, "Digital image processing, 4th edn. ISBN: 9780133356724," ed: Pearson, 2017.

[37] S. Q. Abbas, F. Ahmed, N. Živić, and O. Ur-Rehman, "Perceptual image hashing using SVD based noise resistant local binary pattern," in *2016 8th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2016, pp. 401-407: IEEE.

[38] T. Ojala, M. Pietikäinen, and D. Harwood, "A comparative study of texture measures with classification based on featured distributions," *Pattern recognition*, vol. 29, no. 1, pp. 51-59, 1996.

[39] M. Pietikäinen, A. Hadid, G. Zhao, and T. Ahonen, *Computer vision using local binary patterns*. Springer Science & Business Media, 2011.

[40] Y. Niu, F. Liu, X. Li, and M. Gleicher, "Image resizing via non-homogeneous warping," *Multimedia Tools Applications*, vol. 56, no. 3, pp. 485-508, 2012.

[41] X. Liu, C. Sun, and L. T. Yang, "DCT-based objective quality assessment metric of 2D/3D image," *Multimedia Tools and Applications*, vol. 74, no. 8, pp. 2803-2820, 2015.

[42] C. Dong, C. C. Loy, and X. Tang, "Accelerating the Super-Resolution Convolutional Neural Network," in *European Conference on Computer Vision*, Cham, 2016, pp. 391-407: Springer International Publishing.

[43] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digital Investigation*, vol. 10, no. 3, pp. 226-245, 2013.

[44] J.-D. Chang, B.-H. Chen, and C.-S. Tsai, "LBP-based fragile watermarking scheme for image tamper detection and recovery," in *2013 International Symposium on Next-Generation Electronics*, 2013, pp. 173-176: IEEE.

[45] V. Monga and B. L. Evans, "Perceptual image hashing via feature points: performance evaluation and tradeoffs," *IEEE Transactions on Image Processing*, vol. 15, no. 11, pp. 3452-3465, 2006.