Turkish Journal of Electrical Engineering & Computer Sciences

http://journals.tubitak.gov.tr/elektrik/

Research Article

Turk J Elec Eng & Comp Sci
(2021) 29: 648 – 662

doi:10.3906/elk-2002-6

Robust image hashing based on structural and perceptual features for authentication of color images

Muhammad Farhan KHAN[1,*], **Syed Muhammad MONIR**[2], **Imran NASEEM**[3,4]
[1]Graduate School of Science and Engineering, Karachi Institute of Economics and Technology, Karachi, Pakistan
[2]Department of Electrical Engineering, Mohammad Ali Jinnah University, Karachi, Pakistan
[3]College of Engineering, Karachi Institute of Economics and Technology, Karachi, Pakistan
[4]School of Electrical, Electronic and Computer Engineering, The University of Western Australia, Crawley, Australia

Received: 02.02.2020 • **Accepted/Published Online:** 22.09.2020 • **Final Version:** 30.03.2021

Abstract: Image hashing is one of the most celebrated techniques regarding the discipline of image forensics, image retrieval, image indexing, content verification, and zero watermarking. For such sensitive and complex problems, generation of a unique and robust image hash is an utmost prerequisite for an image identifier driven from the perceptual contents of an image. As a design perspective, it is essential for an image hash to have robustness and optimized discriminative capability. We propose a robust image hashing technique by acquiring perceptual features based on a novel distance magnitude profile utilizing color pixel incongruity among the contiguous pixels, as well as producing a structural image for discrimination. The combination of both results provide a state-of-the-art robust profile that has efficient discriminative capacity and is impervious to usual signal processing violations.

Key words: Image hashing, image authentication, image encryption, structural features, perceptual features, color difference

1. Introduction

Image hashing is the process of image identifier generation on the basis of the image's perceptual contents. Image hashing has found many applications, such as image forensics, image retrieval, image indexing, content verification, and zero watermarking. A unique and robust image hash is needed for most of the applications. Digital image hashing has been used since the end of the last century [1, 2]. Initially, the first secure hashing algorithm (SHA-1) based on digital signature algorithm (DSrA) was used for authentication of messages [1]. SHA-1 was further enhanced for media applications by many researchers and a family of security and hashing schemes was developed based on SHA and message digest algorithm (MDA) [3].

Use of images has been increasing drastically in the field of social media and the internet. Therefore, the need of image authentication, identification, tamper detection, and copyright protection etc. is also increasing exponentially. To fulfill these requirements, image processing solutions such as image hashing, digital image watermarking, and zero-watermarking can be applied. Image hashing is a fast and efficient way for image authentication and related applications. An image hash is a set of robust image features through which a particular image can be truly identified among a big set of images. High true-positive rate for robustness, small hash size for saving memory, and low computational cost for fast searching are the characteristics of a good

*Correspondence: farhanazeemi@hotmail.com

image hashing technique. To achieve a high degree of these characteristics is a challenging problem and the proposed study provides a solution.

Image- and video-based multimedia abounds in this era of digital age where every piece of information is perceived virtually and is extending vastly in every field. Although signal processing is resolving and easing many aspects of digital media, the media contents are vulnerable to various perils of forgery and needless transformations. Such unpredictable malformities could be JPEG conversion, geometric transforms, format conversion, cropping, color contrast, or intensity change. There are many techniques to cater for such situations of image forgery [4]. Image hashing, being one of them, has proved its importance in many areas of digital image processing, i.e. fast identification of images can be carried out easily with the help of small image hashes, image hashes of a digital image library can help in copyright protection, detailed image hashes can be used for image retrieval, or fragile image hashes are used for tamper detection and localization [5] etc. In [6], the dithered lattice vector quantization (LVQ)-based scheme is used for robust hashing with several desirable features, including rotation-invariant filtering, better trade-off between robustness and discrimination, and secrecy, which are then validated by analytical and experimental results. In [7], feature extraction is carried out through randomized ring partition with a secret key, then features are quantized through dithered LVQ. Deep neural networks (DNNs) are also used for training hash codes. Image hashing proposed in [8] is based on deep network models for learning binary hash codes to produce image representations under both unsupervised and supervised manners. A similar method in [9] is presented for training very deep neural networks for supervised learning of hash codes. A method of hashing utilizing color vector angles with discrete wavelet transform (DWT) is proposed in [10]. The method involves resizing and blurring the input image through Gaussian low-pass filter. A method proposed in [11] uses ring partition and DWT to generate perceptual hash value. A secondary image immune to rotation is created by ring partition and DWT is applied to obtain the final hash. Discrete Fourier transform (DFT) is also used for authentication and retrieval [12]. Image is regularized by various procedures such as resizing, rotation, and projection of the image results in a secondary image which is further used to extract robust features using DFT. The approach proposed in [13] utilizes DCT-based hashing to implement various applications such as creating face descriptors for face retrieval, image authentication, and detection of image corruption. The techniques proposed in [14–16] use Canny filter and edge detection for robust image hashing. Image hashing techniques presented in [17] are used for retrieval of encrypted media. Image hashing based on nonnegative matrix factorization (NMF) is discussed in [18]. The hashes are reportedly rotation-invariant, robust, and are useful against image security. A robust technique proposed in [19] extracts global and local features using projected gradient nonnegative matrix factorization (PNMF) for content preserving objective and localization of the affected area. The propositions in [20] concern local binary pattern (LBP), noise-resistant local binary pattern (NRLBP), and center-symmetrical local binary pattern (CSLBP) with singular value decomposition (SVD) for prevention of image tampering.

Review of image hashing shows that researchers have worked on various image hashing techniques such as LVQ, DNN, DWT, DFT, DCT, NMF, SVD, and CSLBP. They have reported robustness of their algorithm, discriminative capability, and invariance of generated hash against well-known image processing attacks. Limitation and advantages of previous techniques are also reviewed with the proposed solution. The proposed method is based on the evaluation of color differences of pixels. Previous methods for evaluation of color difference are reviewed in [21]. A similar work is proposed in [14], where the authors used Canny operator [22] and color vector angles to achieve a high value of robustness but there is a limitation of computational

time which is approximately twice of the proposed technique. It is because they formulated color angle profile for extracting color features. This process creates a higher computational delay. Another limitation of [14] is a bigger hash length. They achieved more robustness, i.e. a little better area under ROC curve (AUC) than the proposed method. Another similar approach is presented in [23], where a perceptual hashing scheme for color images with hybrid feature extraction mechanism is proposed, which generates shorter hash lengths than [14] with slightly lower AUC but the limitation is the much lengthy hybrid hashing steps which make the computational time very high. A robust image hashing method based on partial sum of histogram bins is elaborated in [24] as histogram hashing. This method has poor hash length, AUC, and computational efficiency because of its sensitive behavior against content changing manipulations. A multidimensional scaling (MDS) image hashing is presented in [25] with high robustness because of its higher values of AUC than others but it has very poor results in terms of computational time and especially hash length because of the limitation of very rich featured hash. The results are also presented in Tables 5 and 6.

In view of the above limitations of previous techniques, the proposed image hashing mechanism provides a high degree of robustness with efficient hash length and computational delay. In the proposed algorithm, the host image is processed in two paths. On the one hand, we have considered the host image as a perceptual model against human eye for the extraction of robust image features, while, on the other hand, the host image is considered to develop a unique image structure that could achieve the maximum discrimination capability. The perceptual model is based on a novel color difference profile generated by Euclidean distance of color vectors. The method is designed to make it computationally efficient; therefore, simple mathematical operations are preferred.

The objective of this study is to develop an image hashing algorithm to generate a unique and robust image hash with smaller hash length and high computational efficiency for the applications of authentication and copyright protection. Uniqueness of image hash shows that it can be discriminated among a large number of image hashes for identification of true image while robustness is the true identification after tampering. Mostly, an image hashing algorithm is applied to a digital image library having a huge number of images. Therefore, the hashing algorithm should not be much complex for computation and its short length provides the advantage of fast image searching. The proposed study targets to achieve a low computational cost and short hash length with high discriminative efficiency and robustness.

The algorithm of the proposed method is elaborated with detailed steps in Section 2. Experiments, results, and discussions are given in Section 3.

2. Proposed work

Image hashing is a way to recognize an image, even after contamination, while maintaining discrimination from other images. These challenging characteristics are provided in the proposed algorithm by exploiting the structural and perceptual features of an image. These features are directly related to the edges of objects present in an image. There are some conventional methods for edge detection like Laplacian or gradient-based algorithms. Canny edge detection scheme is a classical, efficient, and famous method but smoothing and thresholding are limitations for its use in image hashing. Keeping this in view, we propose a scheme similar to Laplacian point detection with some novel improvements. The scheme uses image scanning with contiguous neighbors of a focused pixel to develop a perceptual feature profile and it is named 8-neighbor distance magnitude profile (N_8DMP).

The host image is preprocessed by smoothing and resizing at a predefined standard. The proposed image

hashing method comprises two parallel paths: 1) Scanning of color image for development of perceptual profile to extract image features for hash generation. 2) Scanning of grayscale image for development of structural profile for identification of robust areas to maintain discrimination capability. The proposed image hashing is illustrated in Figure 1 and the operation of each block is further described in Section 2.1 to Section 2.6. Color image is provided to one branch for making perceptual profile while its grayscale version is forwarded to the other branch for extraction of structural features. These image features are further used to develop block features and finally formulated as binary feature profiles. Both image profiles are combined to develop a robust and discriminative image for hashing. Finally, the system applies ring partitioning and generates a state-of-the-art image hash.

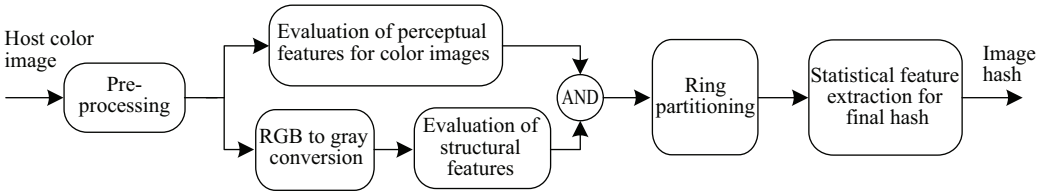


Figure 1. Block diagram of the proposed image hashing.

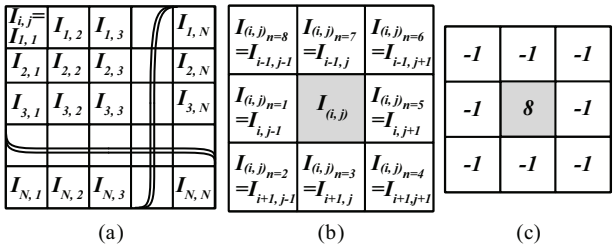


Figure 2. (a) Pixel organization in an image, (b) pixel (i, j) with eight neighbors, (c) Laplacian kernel for point detection.

2.1. Preprocessing

Preprocessing consists of image resizing and smoothing of input color image. Image resizing with bicubic interpolation is applied for images to make the standard size of $N \times N$. Gaussian filtering is an efficient tool for removal of high-frequency noise contents. Therefore, the resized image is passed through low-pass Gaussian filter. After initial processing, we scan the image for extraction of robust features. Robust features are extracted by means of image perceptual and structural binary profiles. Feature profiles are discussed in Sections 2.2 and 2.3.

2.2. Development of perceptual profile

Development of perceptual profile needs a preprocessed color host image for extraction of the desired perceptual image features. Organization of pixels in a color image is shown in Figure 2a as an example. A focused pixel (i, j) of image I and its neighbors are illustrated in Figure 2b with designated names. Edges of objects in an image are more perceptible than a smooth area for human vision. Therefore, we identify visually insignificant contents of the image for a robust image hash. Inspired by the Laplacian edge detection method [22], we have developed a scheme with enhanced features for perceptual profile of color images. The Laplacian algorithm evaluates the

average difference with neighbor pixels according to the kernel given in Figure 2c and its filtered result is shown in Figure 3a. We propose a more sensitive nonlinear approach that uses the maximum difference with the 8 neighbors of the pixel. Figure 3 compares the result of the proposed method with that of Laplacian filtering. It is evident that the proposed method has yielded stronger edges. For better understanding, the perceptual image shown in Figure 3b is binarized and shown in Figure 3c. The proposed method for development of perceptual profile consists of two steps that are elaborated in Sections 2.2.1 and 2.2.2.

(a) (b) (c)

Figure 3. (a) Resulting pepper image after Laplacian filtering, (b) filtering through the proposed N_8DMP, (c) binary output from N_8DMP after thresholding and inversion.

2.2.1. N8 distance magnitude profile (N_8DMP)

The preprocessed image of size $N \times N$ is scanned so that each pixel of the color image, excluding border pixels, is used to produce squared magnitudes of color distance vectors with its eight neighbor pixels $n = 1$ to 8 as shown in Figure 2b. The maximum squared distance out of the eight neighbor color distances is selected. This makes our algorithm more sensitive than the Laplacian edge detection. Squared magnitudes are used to enhance the deviation in statistical data for a powerful hash. Ring partitioning and statistical features for hash are elaborated in Section 2.6. The proposed procedure of N_8DMP generation is shown graphically in Figure 4. The procedure is also formulated mathematically in Eq. (1).

$$d_{i,j} = \max_{1 \le n \le 8} \; D^2(I_{i+1,j+1}, I_{(i+1,j+1)_n}), \quad (i,j) = (1,1) \; to \; (N-2, N-2) \tag{1}$$

where i and j are the indices for N_8DMP, $I_{(i+1,j+1)_n}$ is n^{th} neighbor of $I_{i+1,j+1}$ and D is their Euclidian distance.

2.2.2. Distance blocks and perceptual features

The profile $d_{i,j}$ is divided into nonoverlapping square blocks of size $L \times L$, where L controls the trade-off between discrimination and robustness. Robustness and discrimination capability are two contrasting requirements; they have direct and inverse relation with L, respectively. To develop a better trade-off between feature details for robustness and computational complexity, we configure the block size of 2×2 for better robustness fast computation. Each block is used as perceptual feature identifier. Maximum value from each block is evaluated and compiled as perceptual profile $p_{i,j}$ to make the hash features full of variety. It should be noted that the

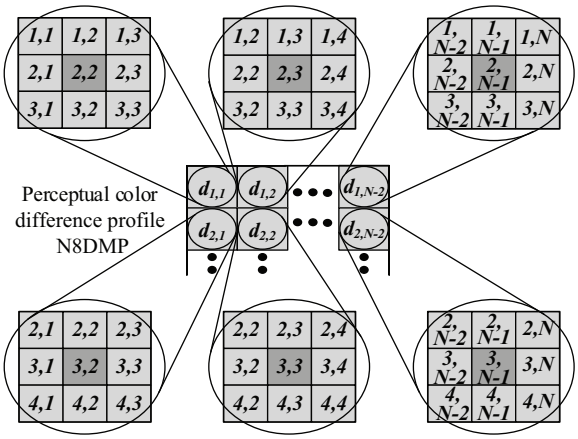


Figure 4. Graphical illustration of N_8DMP generation.

size of perceptual profile is a square image with $(N-2)/L$ rows and columns. Let $M = (N-2)/L$ then:

$$p_{i,j} = \max_{v=1}^{L} \max_{u=1}^{L} d_{(i-1)L+u,(j-1)L+v}, \quad (i,j) = (1,1)\ to\ (M,M) \tag{2}$$

where u and v are pointers to the elements of $((i-1)L, (j-1)L)$ distance blocks.

2.3. Development of structural profile

Structural profile is a set of image features that are used to explore spatial locations of image that are robust against common image processing attacks. Structural profile is further used for masking of perceptual features. It requires the grayscale copy Ig of preprocessed image. Structural profile development is described in Sections 2.3.1 and 2.3.2.

2.3.1. Robust binary structural image

Edges and structure of the image can be easily defined by using intensity plane of color image. Border pixels of intensity plane are discarded to maintain the compatibility with N_8DMP. The intensity image Ig is first converted to the binary image, using the most significant bits (bit plane 8) with the help of bit plane slicing of intensity image. Robustness of bit plane 8 against most of the signal processing attacks depends on the state of lower bit planes. We selected two lower bit planes, i.e. bit planes 6 and 7 because they have more weightage as compared to the other lower planes. As the contents of image pixels may be altered during signal processing attacks, these minor alterations may affect the pixels of composed binary image. This effect may alter the most significant bit in the case where bit 6 and 7 of the respective pixel are found at extremes, i.e. '00' or '11'. Therefore, to increase the robustness of the proposed algorithm, we clear the respective bit of binary image to mask the perceptual contents at this fragile location. This is how we integrated the state-of-the-art robustness in our algorithm. The size of the resultant binary structural image is $(N-2 \times N-2)$ and denoted by $q_{i,j}$.

$$q_{i,j} = (Ig_{i+1,j+1})_{bit8} \ \wedge \ ((Ig_{i+1,j+1})_{bit6} \oplus (Ig_{i+1,j+1})_{bit7}) \tag{3}$$

where $q_{i,j}$ is the robust binary structural image. The symbols '$\wedge$' and '$\oplus$' are used for logical AND and XOR operations, respectively.

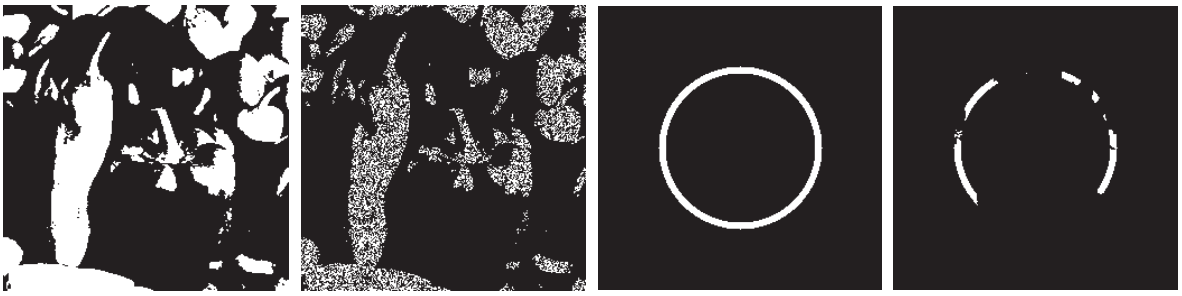
2.3.2. Binary structural profile

The robust binary structural image $q_{i,j}$ is divided into nonoverlapping blocks of size $L \times L$ (2×2 in our case) to maintain the compatibility with $p_{i,j}$. Since each block is used as a structural feature identifier, a single bit is extracted from each block. Binary structural profile is formulated by composition of extracted bits. Binary structural features are further used to mask perceptual features. Therefore, we divide $q_{i,j}$ into blocks of $L \times L$ to maintain the size compatibility. If the count of ones in the $L \times L$ block is greater than half the number of elements in the block, then the extracted bit is marked as one, otherwise as zero. It should be noted here that if the number of ones in a block is more than half of the number of elements, then the block is suitable for extracting hash features. Summation of block contents is expressed in Eq. (4) while the binary structural profile is given in Eq. (5).

$$S_{i,j} = \sum_{v=1}^{L} \sum_{u=1}^{L} q_{(i-1)L+u,(j-1)L+v}, \quad (i,j) = (1,1)\ to\ (M,M) \tag{4}$$

$$k_{i,j} = \begin{cases} 1 & if S_{i,j} \geq \frac{L \times L}{2}, \\ 0 & if S_{i,j} < \frac{L \times L}{2} \end{cases} \quad (i,j) = (1,1)\ to\ (M,M) \tag{5}$$

where $k_{i,j}$ is the binary structural profile and it is shown as binary image in Figure 5a.



(a) (b) (c) (d)

Figure 5. (a) Binary image $k_{i,j}$, (b) masked perceptual profile $R_{i,j}$, (c) binary ring image $Br_{i,j}$ for $k = 12$, (d) binarized ring partition from masked perceptual profile for $k = 12$.

2.4. Masked perceptual profile (MPP) and weighted MPP

Perceptual profile $p_{i,j}$ is filtered by $k_{i,j}$. The contents of $p_{i,j}$ are masked to zero for locations where the logic values of $k_{i,j}$ are zero by using AND operation while the remaining elements are passed to develop perceptual features only from robust spatial locations. The masking can be carried out either by using AND-operated MPP between $p_{i,j}$ and $k_{i,j}$ or by applying weights on $p_{i,j}$ proportional to $S_{i,j}$ weighted MPP, given in Eq. (6), i.e. 100% if $S_{i,j} = 3$, 50% if $S_{i,j} = 2$, 25% if $S_{i,j} = 1$, and 0% if $S_{i,j} = 0$ as the block sum $S_{i,j}$ ranges from 0 to 3. Masking by simple AND-operated MPP is more time-efficient than applying weights. Table 2 shows the comparison of similarities with computational efficiency for both options. The resulting weighted MPP $R_{w_{i,j}}$

and MPP $R_{i,j}$ are expressed in Eqs. (6) and (7), respectively, and $R_{i,j}$ is also shown in Figure 5b.

$$R_{w_{i,j}} = \begin{cases} p_{i,j} & if S_{i,j} = 3, \quad (i,j) = (1,1)\ to\ (M,M) \\ p_{i,j} \times 0.5 & if S_{i,j} = 2, \\ p_{i,j} \times 0.25 & if S_{i,j} = 1, \\ 0 & if S_{i,j} = 0 \end{cases} \tag{6}$$

$$R_{i,j} = p_{i,j} \wedge k_{i,j}, \quad (i,j) = (1,1)\ to\ (M,M) \tag{7}$$

2.5. Ring partitioning

Robust MPP $R_{i,j}$ is highly invariant against most of the image processing attacks but still rotational tampering may alter its contents. Ring partitioning is an efficient tool for improving invariance of hash against rotation because statistical norms of image features are not altered by image rotation. Therefore, the authors are motivated to use ring partitioning. Partitioning of $R_{i,j}$ into circular stripes or rings concentric at image center (i_c, j_c) is carried out by generating binary ring images $Br_{i,j}$ of ones for each individual ring. Selection of number of rings depends on the desired size and quality of image hash and has a direct relation with them. K number of rings are assumed with radii r_k. The binary image for k^{th} ring $Br_{i,j}^{(k)}$ having size of $M \times M$ (same as the size of $R_{i,j}$) can mathematically be represented as in Eq. (8) and is illustrated in Figure 5c for ring number $k = 12$ out of a total 21 rings. It should be noted here that Figure 5c shows the mask ring to extract image features laying on the ring. Image features $R_{i,j}$ masked by the ring are shown in Figure 5d.

$$Br_{i,j}^{(k)} = \begin{cases} 1 \mid |dr_{i,j} - r_k| \leq \frac{1}{2}w, \quad (i,j = 1,1\ to\ M,M \text{ and } k = 1,2,...,K) \\ 0\ otherwise \end{cases} \tag{8}$$

where w is the width of ring stripes, $dr_{i,j}$ is the distance of pixel (i,j) in $Br_{i,j}^{(k)}$ from the image center (i_c, j_c) and $M = (N-2)/L$

Rotation and cropping may distort the outer most ring; therefore, we select the radii of rings while protecting from distortion as given in Eq. (9).

$$r_k = \frac{\frac{M}{2} - \frac{1}{2}w}{K}, \quad k = 1,2,...,K) \tag{9}$$

where minimum distance from center of ring image to sides of image is $\frac{M}{2}$, so it must be divided in K radii but first we subtract half of the ring stripe width w to protect outer most ring from distortion. Therefore, $\frac{1}{2}w$ is subtracted from $\frac{M}{2}$ before division in total rings.

The binarized image of k^{th} ring partition from perceptual profile $R_{i,j}$ is shown in Figure 5d and its nonzero perceptual contents are formulated in Eq. (10) as a set of perceptual ring vectors $Rp^{(k)}$.

$$Rp^{(k)} = R_{i,j} \wedge Br_{i,j}^{(k)}, \quad Br_{i,j}^{(k)} \neq 0 \tag{10}$$

where $Rp^{(k)}$ has only those contents of $R_{i,j}$ which lie on k^{th} ring. The number of elements in k^{th} ring is M_k which is same as the number of ones in $Br_{i,j}^{(k)}$.

2.6. Statistical features and final hash composing

Finally, image hash is developed with the help of statistical contents of ring vectors $Rp^{(k)}$. Mean, variance, or other vector norms can be used for hash generation. The elements of ring vectors are real and have quite high values. Therefore, variance is a suitable statistical parameter that can provide smaller hash elements. However, normalization, scaling, and rounding off to obtain the image hash of a specific bit length is performed further. Let σ_k^2 be variance, μ_k be the mean, and M_k the number of elements of k^{th} ring, then the variance is calculated as follows.

$$\sigma_k^2 = \frac{1}{M_k}\sum_{i=1}^{M_k}\{Rp^{(k)}(i) - \mu_k\}, \quad i = 1, 2, ..., M_k \tag{11}$$

where i is pointing to the elements of k^{th} ring vector.

Normalization and scaling are performed on variance in Eq. (12) to evaluate the image hash.

$$h(k) = \frac{\sigma_k^2}{\max \sigma_k^2} \times 10000 \tag{12}$$

where $h(k)$ is the final hash having K elements each rounded off at 14 bit value. Therefore, the length of our state-of-the-art hash is $14 \times K$ bits.

3. Experiments, results, and discussions

Performance of the proposed algorithm is evaluated for color images, taken from USC-SIPI standard image database and Graphics, Imaging, and Games Lab (GIGL) [26]. Images from both databases are 24 bit true color RGB with their sizes ranging from 512×512 to 2250×2250. During preprocessing, the image size is first standardized to the constant size of 512×512 followed by Gaussian filtering with mean $\mu = 0$, standard deviation $\sigma = 1.0$, and filter size of 3×3 to remove high-frequency noise contents. The thickness or width of rings is $\pm\frac{1}{2}w = 1.5$ and total number of rings $K = 21$ is specified.

3.1. Robustness

Forty-two images from volume 2 and volume 3 of USC-SIPI image database and 20 images from GIGL NPR general Benchmark were subjected to image processing attacks using MATLAB and Photoshop to generate a tampered image library. Types and strength of signal processing attacks are shown in Table 1. A total of 66 signal processing attacks were performed on 62 host images from both databases. This provides a total of 4092 tampered images to pair with their original images for the evaluation of similarity after tampering with original ones. Nine different types of attacks were carried out and the robustness of image hash was measured by means of similarity between tampered and host images.

3.2. Similarity

The proposed algorithm was implemented using MATLAB to generate the color image hashes. A total of 4092 tampered image hashes were analyzed for similarity content with hashes of their 62 original images from USC-SIPI and GIGL NPR image databases. Similarities of hash pairs were tested for each tampering class and their mean and standard deviations with computational time for both MPP and weighted MPP options of masking were evaluated. Table 2 shows brief results of hash similarities for different tampering classes. According to

Table 1. Description of signal processing attacks.

Tool	Operation	Parameter	Parameter value	No. of images
Photoshop	Brightness adjustment	Photoshop's scale	±10, ±20	4
Photoshop	Contrast adjustment	Photoshop's scale	±10, ±20	4
MATLAB	Gamma correction	γ	0.75, 0.9, 1.1, 1.25	4
MATLAB	3 x 3 Gaussian	Standard deviation	0.3, 0.4, . . . , 1.0	8
MATLAB	JPEG compression	Quality Factor	30, 40, . . . , 100	8
MATLAB	Scaling	Ratio	0.5, 0.75, 0.9, 1.1, 1.5, 2.0	6
MATLAB	Rotation and cropping	Angle in degree	$\pm1, \pm2, \pm5, \pm10, \pm15, \pm30, \pm45, \pm60, \pm75, \pm90$	20
MATLAB	Salt and pepper noise	Density	0.01, 0.02,..., 0.06	6
MATLAB	Speckle noise	Density	0.01, 0.02,..., 0.06	6

Total signal processing attacks & **66**

the results, simple AND-operated MPP masking option has more computational efficiency than weighted MPP masking; therefore, simple MPP masking is selected for the proposed algorithm.

Table 2. Mean similarity values of the original and tampered image hash pairs with standard deviation (SD) and hash computational time using both $R_{i,j}$ and $R_{w_{i,j}}$ masked perceptual profiles.

Operation (tampering class)	U sing MPP $R_{i,j}$ by AND operation			Using weighted MPP $R_{w_{i,j}}$		
	Mean	SD	Time (s)	Mean	SD	Time (s)
Brightness adjustment	0.945	0.091	0.267	0.946	0.089	0.335
Contrast adjustment	0.991	0.014	0.264	0.996	0.008	0.329
Gamma correction	0.948	0.101	0.264	0.953	0.097	0.331
3 x 3 Gaussian	0.991	0.027	0.264	0.990	0.030	0.331
JPEG compression	0.992	0.022	0.262	0.992	0.022	0.328
Scaling	0.994	0.019	0.267	0.995	0.018	0.334
Rotation and cropping	0.930	0.116	0.274	0.931	0.128	0.349
Salt and pepper noise	0.996	0.014	0.267	0.995	0.016	0.339
Speckle noise	0.994	0.016	0.264	0.994	0.022	0.332

Table 3 shows a comparison of mean similarity and standard deviation between the proposed method and a similar approach [14] which is named Canny hashing. The same images with similar parameters of tampering are taken for true comparison with Canny hashing.

3.3. Discrimination capability

Discrimination capability is the characteristic of image hashing scheme that makes it efficient for generating true-positive results. On the other hand, we can say that it is a characteristic that protects from false-positive results. In the proposed hashing scheme, masking perceptual profile by structural image features in final image hash provides ability of discrimination. Discrimination capability of the proposed scheme can be easily analyzed

Table 3. Similarity comparison of the proposed method and a previous method.

Image processing operation	Canny hashing [14]		Proposed hashing	
	Mean	Standard deviation	Mean	Standard deviation
Brightness adjustment	0.98	0.04	0.95	0.09
Contrast adjustment	0.97	0.04	0.99	0.01
Gamma correction	0.97	0.04	0.95	0.10
3 x 3 Gaussian	0.97	0.05	0.99	0.03
JPEG compression	0.94	0.08	0.99	0.02
Scaling	0.96	0.05	0.99	0.02
Rotation and cropping	0.92	0.08	0.93	0.12
Salt and pepper noise	-	-	0.99	0.01
Speckle noise	-	-	0.99	0.02

with the help of Figure 6a where frequency of occurrence is plotted against correlation values of possible different hash pairs of 400 images, i.e. $(400 \times 399)/2 = 79,800$ from Ground Truth standard image database.

In the Canny hashing approach [14], the authors used 200 different images to analyze their discrimination capability. The frequency distribution taken from their research paper is shown in Figure 6b for performance comparison.

The statistical comparison of data is given in Table 4. It is evident that the proposed scheme has a state-of-the-art performance. Our mean similarity ratio for 79,800 dissimilar image pairs is 0.026 for $K = 21$ and $w = 6$. While only 19,800 dissimilar image pairs were considered in Canny hashing and a similarity of 0.175 was achieved.

Table 4. Similarity distribution parameters of correlation coefficients for dissimilar image pairs.

Algorithm	Max.	Min.	Mean	Standard deviation
Proposed hashing (for 79,800 pairs)	0.968	–0.927	0.026	0.365
Canny hashing (for 19,800 pairs)	0.971	–0.869	0.175	0.357

3.4. Receiver operating characteristics

Receiver operating characteristics (ROC) curve is an effective tool for analyzing the efficiency of a detection system. ROC curve is a plot of true detection rate versus false detection rate. For an efficient system, true detection rate should be maximum while false rate should be minimum. Therefore, values of an efficient system must lie at the top left corner. ROC generated by the proposed system are presented in Figure 7. Area under ROC curve (AUC) is a measure of the efficiency of ROC. Table 5 illustrates the comparison of AUC and hash length of the proposed method with some latest schemes [14, 23–25]. We provided the hash length in both binary bits and decimal digits for $K = 21$. Number of decimal digits required to save the result is $\log_{10} 2^{bits}$ where $bits = 14 \times K$.

AUR should be unity for an ideal system. AUC of Canny hashing [14] is very slightly higher than our scheme because of its larger hash size and longer computational time. Therefore, it is evident that the proposed method is an efficient image hashing method with a high true-positive rate and a very low false-positive rate.

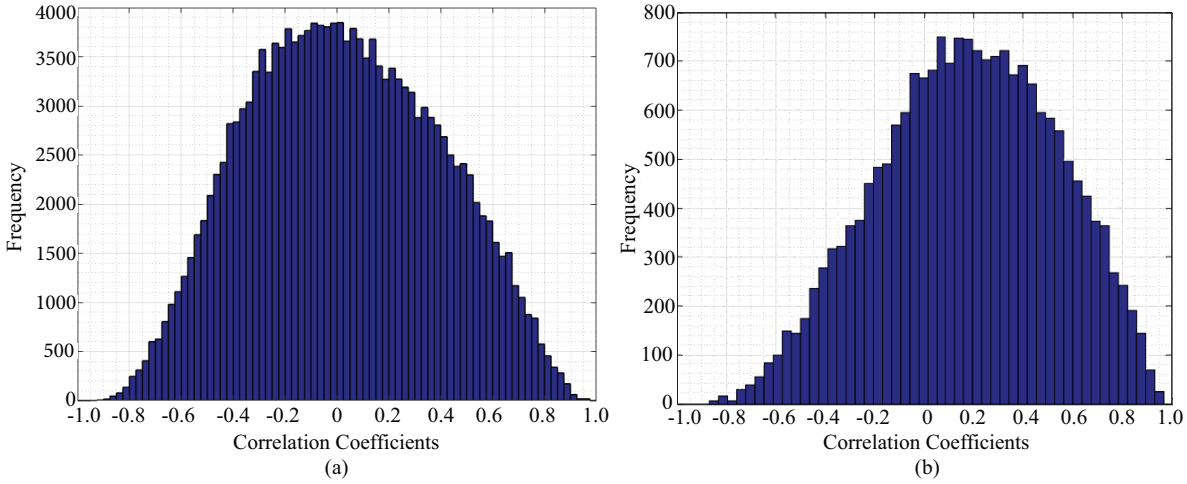


Figure 6. (a) Distribution of correlation for the proposed hashing, (b) frequency distribution taken from [14].

Table 5. Comparison of area under the ROC curves for the proposed and the previous methods.

Algorithm	Area under ROC curve	Hash length
Proposed hashing	0.9951	294 bits or 89 digits
Canny hashing [14]	0.9955	400 bits or 121 digits
Hybrid hashing [23]	0.9947	343 bits or 104 digits
Histogram hashing [24]	0.9572	448 bits or 135 digits
MDS hashing [25]	0.9905	720 bits or 217 digits

3.5. Effect of varying K on ROC curve

The proposed algorithm is tested for a range of K from 1 to 35 and ROC curves for some selected values $K = 7, 14, 21, 28, 35$ are shown in Figure 7a keeping $w = 6$. The values of area under ROC curves (AUC) are also illustrated in this figure. It can be concluded from Figure 7a that the optimum value of K is 21.

3.6. Effect of varying w on ROC curve

Ring width w is also optimized for $K = 21$ by using a range of w from 2 to 10 and ROC curves are shown in Figure 7b. Clearly, the larger values of ring thickness are improving AUC but also increasing computational time. Therefore, the optimum result can be taken for $K = 21$ and $w = 6$ without distortion of outer most ring and is illustrated in Figure 7c.

3.7. Computational cost

Computational cost of the proposed color image hashing algorithm was evaluated using MATLAB 2017 on a machine having core i3-4030U CPU at 1.9GHz. The results are compared with [14, 23–25] and found to be better among the compared methods because of the limitations discussed in Section 1. Table 6 shows a comparison of average computational time and the hash length. Average computational costs of Canny hashing [14], hybrid hashing [23], histogram hashing [24], and MDS hashing [25] are higher and have larger hash size than our scheme. Therefore, the proposed method is computationally more efficient.

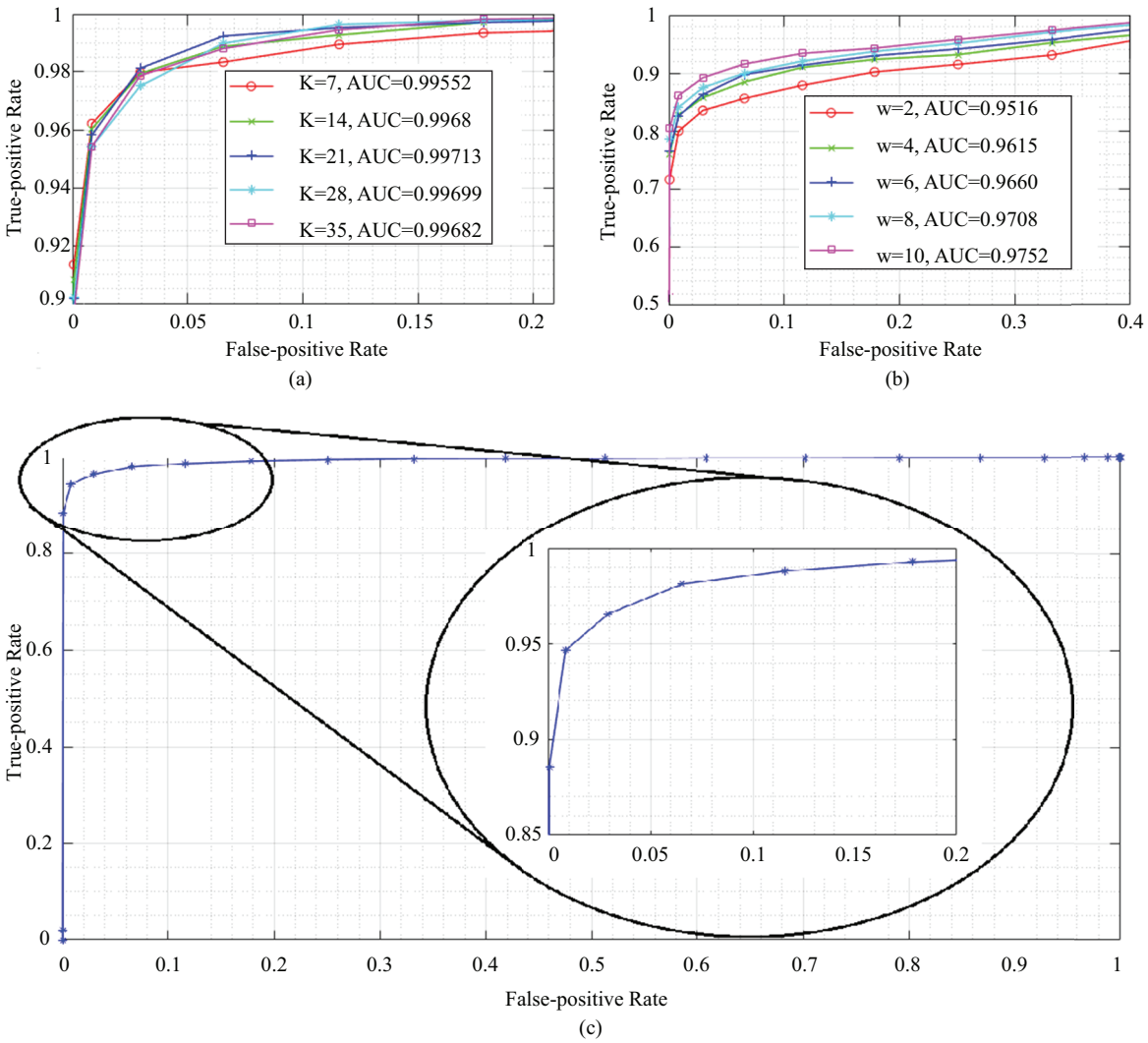


Figure 7. (a) ROC curves for different values of K, (b) ROC curves for different values of w, (c) ROC curve for $w = 6$ and number of rings $K = 21$.

Table 6. Comparison of computational costs for the proposed and the previous work.

Algorithm	Average computational time (s)	Hash length
Proposed hashing	0.27	294 bits or 89 digits
Canny hashing [14]	0.49	400 bits or 121 digits
Hybrid hashing [23]	35	343 bits or 104 digits
Histogram hashing [24]	0.413	448 bits or 135 digits
MDS hashing [25]	0.492	720 bits or 217 digits

4. Conclusion

This paper presents a robust image hashing technique for color images based on image scanning for identification of robust areas and perceptual features of image. Host image is scanned for its robust spatial locations to generate image perceptual profile. Robust image feature profile of the color image is developed for selecting those parts of image which are more suitable for robustness. The color host image is further scanned for developing its structural information. The image perceptual and structural features are further processed to generate the robust hash image. The robust hash image is finally partitioned in robust ring vectors to compose image hash by extracting the statistical features. We analyzed $162,372$ pairs of tampered and original color images to prove the robustness and discriminative capability of the proposed algorithm. The algorithm is capable of tamper localization using $L \times L$ small blocks. However, fragile hashing and tamper localization are the parts of extension work that will be presented in a separate paper. Comparative analysis of the results shows the level of robustness of the proposed scheme against normal digital image processing operations with improved discrimination.

Acknowledgment

The authors would like to appreciate their respective institutions for facilitating this research.

Contributions of authors

The authors contributed for this paper as follows: MONIR gave the idea, KHAN carried out the experiments, KHAN and MONIR interpreted the results, KHAN wrote the paper, MONIR and NASEEM reviewed the paper.

References

[1] Burrows, James H, Department of Commerce Washington DC. Secure hash standard. Washington, DC, USA: Federal Information Processing Standards Publication, 1995.

[2] Schneider M, Chang S-F. A robust content based digital signature for image authentication. In: 3rd IEEE International Conference on Image Processing; Lausanne, Switzerland; 1996. pp. 227-230.

[3] Kunhu A, Al-Ahmad H, Taher F. Medical images protection and authentication using hybrid DWT-DCT and SHA256-MD5 hash functions. In: 24th IEEE International Conference on Electronics, Circuits and Systems (ICECS); Batumi, Georgia; 2017. pp. 397-400.

[4] Lamba AK, Jindal N, Sharma S. Digital image copy-move forgery detection based on discrete fractional wavelet transform. Turkish Journal of Electrical Engineering and Computer Science 2018; 26 (3): 1261–1277.

[5] Khan MF, Monir SMG, Naseem I. A novel zero-watermarking based scheme for copyright protection of grayscale images. Mehran University Research Journal of Engineering and Technology 2019; 38 (3): 627–640.

[6] Li Y, Lu Z, Zhu C, Niu X. Robust image hashing based on random Gabor filtering and dithered lattice vector quantization. IEEE Transactions on Image Processing 2012; 21 (4): 1963–1980. doi: 10.1109/TIP.2011.2171698.

[7] Jung C, Cao L. Randomized ring-partition fingerprinting with dithered lattice vector quantization. In: 2015 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery; Xi'an, China; 2015. pp. 100–103. doi: 10.1109/CyberC.2015.96.

[8] Toan Do T, Hoang T, Le Tan D, Doan A, Cheung N. Compact hash code learning with binary deep neural network. IEEE Transactions on Multimedia 2020; 20 (4): 992-1004. doi: 10.1109/TMM.2019.2935680.

[9] Zhang Z, Chen Y, Saligrama V. Efficient training of very deep neural networks for supervised hashing. In: 2016 The IEEE Conference on Computer Vision and Pattern Recognition (CVPR); Boston; 2016. pp. 1487 – 1495.

[10] Tang Z, Dai Y, Zhang X, Huang L, Yang F. Robust image hashing via colour vector angles and discrete wavelet transform. IET Image Processing 2014; 8 (3): 142–149.

[11] Govindaraj P, Sandeep R. Ring partition and DWT based perceptual image hashing with application to indexing and retrieval of near-identical images. In: 2015 Fifth International Conference on Advances in Computing and Communications (ICACC); Kochi, India; 2015. pp. 421–425. doi: 10.1109/ICACC.2015.90.

[12] Qin C, Chang C-C, Tsou P-L. Robust image hashing using non-uniform sampling in discrete fourier domain. Digital Signal Processing 2013; 23 (2): 578–585. doi: https://doi.org/10.1016/j.dsp.2012.11.002.

[13] Tang Z, Yang F, Huang L, Zhang X. Robust image hashing with dominant DCT coefficients. Optik - International Journal for Light and Electron Optics 2014; 125 (18): 5102–5107. doi: https://doi.org/10.1016/j.ijleo.2014.05.015.

[14] Tang Z, Huang L, Zhang X, Lao H. Robust image hashing based on color vector angle and canny operator. AEU - International Journal of Electronics and Communications 2016; 70 (6): 833 – 841. doi: https://doi.org/10.1016/j.aeue.2016.03.010.

[15] Cao J, Chen L, Wang M, Tian Y. Implementing a parallel image edge detection algorithm based on the otsu-canny operator on the hadoop platform. Computational Intelligence and Neuroscience 2018; 2018.

[16] Singh S, Datar A. Improved hash based approach for secure color image steganography using canny edge detection method. International Journal of Computer Science and Network Security (IJCSNS) 2015; 15 (7): 92-98.

[17] Yang B, Shang X, Pang S. Isometric hashing for image retrieval. Signal Processing: Image Communication 2017; 59: 117–130. doi: https://doi.org/10.1016/j.image.2017.07.002.

[18] Tabatabaei SAHAE, Ruland C. The analysis of an NMF-based perceptual image hashing scheme. In: IEEE International Symposium on Signal Processing and Information Technology; Athens, Greece; 2013. pp. 000108–000112. doi: 10.1109/ISSPIT.2013.6781863.

[19] Karsh RK, Laskar RH, Richhariya BB. Robust image hashing using ring partition-PGNMF and local features. Springer Plus 2016; 5: 1-20. doi:10.1186/s40064-016-3639-6.

[20] Abbas SQ, Ahmed F, Zivic N, Ur-Rehman O. 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); Lisbon, Portugal; 2016. pp. 401–407. doi: 10.1109/ICUMT.2016.7765393.

[21] Ortiz-Jaramillo B, Kumcu A, Platisa L, Philips W. Evaluation of color differences in natural scene color images. Signal Processing: Image Communication 2019; 71: 128–137. doi: https://doi.org/10.1016/j.image.2018.11.009.

[22] Gonzalez RC, Woods RE, Eddins SL. Digital Image Processing Using MATLAB. Upper Saddle River, New Jersey: Pearson-Prentice-Hall, 2004.

[23] Qin C, Sun M, Chang C-C. Perceptual hashing for color images based on hybrid extraction of structural features. Signal Processing 2018; 142: 194–205.

[24] Vadlamudi LN, Vaddella RPV, Devara V. Robust hash generation technique for content-based image authentication using histogram. Multimedia Tools and Applications 2016; 75 (11): 6585–6604.

[25] Tang Z, Huang Z, Zhang X, Lao H. Robust image hashing with multidimensional scaling. Signal Processing 2017; 137: 240–250.

[26] Mould D, Rosin PL. A benchmark image set for evaluating stylization. In: Proceedings of the Joint Symposium on Computational Aesthetics and Sketch Based Interfaces and Modeling and Non-Photorealistic Animation and Rendering; Lisbon, Portugal; 2016. pp. 11–20. doi: 10.2312/exp.20161059.