How to cite this article:

Srivastava, M. Siddiqui, J., & Ali, M. A. (2018). Hough transform generated strong image hashing scheme for copy detection. *Journal of Information and Communication Technology*, *17*(4), 653-678.

HOUGH TRANSFORM GENERATED STRONG IMAGE HASHING SCHEME FOR COPY DETECTION

[1]Mayank Srivastava, [2]Jamshed Siddiqui & [3]Mohammad Athar Ali

[1] Institute of Engineering and Technology, Ganeshi Lal Agrawal University, India

[2] Department of Computer Science, Aligarh Muslim University, India

[3]Department of Applied Computing, University of Buckingham, United Kingdom

mayank.srivastava@gla.ac.in; jamshed_faiza@rediffmail.com; athar.ali@buckingham.ac.uk

ABSTRACT

The rapid development of image editing software has resulted in widespread unauthorized duplication of original images. This has given rise to the need to develop robust image hashing technique which can easily identify duplicate copies of the original images apart from differentiating it from different images. In this paper, we have proposed an image hashing technique based on discrete wavelet transform and Hough transform, which is robust to large number of image processing attacks including shifting and shearing. The input image is initially pre-processed to remove any kind of minor effects. Discrete wavelet transform is then applied to the pre-processed image to produce different wavelet coefficients from which different edges are detected by using a canny edge detector. Hough transform is finally applied to the edge-detected image to generate an image hash which is used for image identification. Different experiments were conducted to show that the proposed hashing technique has better robustness and discrimination performance as compared to the state-of-the-art techniques. Normalized average mean value difference is also calculated to show the performance of the proposed technique

Received: 7 April 2018 Accepted: 30 August 2018 Published: 1 October 2018

towards various image processing attacks. The proposed copy detection scheme can perform copy detection over large databases and can be considered to be a prototype for developing online real-time copy detection system.

Keywords: Content-based copy detection, digital watermarking, discrete wavelet transform, hough transform, image forensics, image hashing.

INTRODUCTION

The use of digital media is increasing in our day to day life due to the adaptability of a large number of smart devices like smartphones. These devices allow us to do a lot of application-oriented tasks very easily, including capturing and editing of images. We know it very well that the use of editing software does not require any special technical expertise and they can easily manipulate images (Liu, Wang, Lian, & Wang, 2011). Massive creation and widespread dispersion of data, arising from easy to copy nature, poses new challenges for the protection of intellectual property of multimedia data (Kang & Wei, 2009). Protecting the copyright of an image is a matter of great concern (Qazi, Hayat, Khan, Madani, Khan, Kolodziej, Lin & Wu, 2013). To ensure that the given image is original and is not a modified version, image authentication techniques are required (Battiato, Farinella, Messina, & Puglisi, 2012). Traditionally, authentication issues are addressed by cryptographic hashes, which are sensitive to each bit of the input message. As a result, change in even a single bit of the input data leads to a significant change in the hash value (Qureshi & Deriche, 2015). However, due to the high sensitivity of the input data these hash functions are not suitable for image authentication.

In this context, we need to explore the area of image forensics (Redi, Tatak, & Dugelay, 2011) which involves a combination of techniques used not only to verify the authenticity of an image but also to verify ownership and detect unauthorized copies. Currently, two approaches named as watermarking and content-based copy detection are used to detect unauthorized copies. In watermarking, an authenticator is generated and added to the media content which is used to identify the authenticity of an original content (Rey & Dugelay, 2002). Content-based copy detection (CBCD) is an alternative to digital watermarking, in which multimedia content itself is used to establish its ownership. (Hsiao, Chen, Chien, & Chen, 2007). In image-based copy detection, unique features are extracted from an image which can be used for identification.

Over the last few years, a number of significant works have been proposed in the area of image hashing which is an extension of the content

based copy detection techniques (Tang, Yang, Huang, & Zhang, 2014b). In image hashing, the generated unique feature is represented as small, preferably bit level data to form the image hash, which is used for image identification (Tang, Zhang, Dai, Yang, & Wu, 2013a). Ideally, image hashing should be able to discriminate between similar and dissimilar images, i.e. the mechanism should depict robustness and discrimination among the images. Apart from that, it should be robust to various kinds of image processing attacks besides fulfilling the properties related to specific applications.

LITERATURE REVIEW

In the past, researchers have implemented many algorithms related to various aspects of image hashing. Some of the notable algorithms categorized on the basis of transformation/functionalities used are as follows:

Tang, Yang, Huang, and Zhang (2014b) proposed image hashing based on dominant discrete cosine transform (DCT) coefficients which have been proven to perform well in classification and in detecting image copies. Tang, Wang, and Zhang (2010) used a mechanism based on a dictionary, which represents the characteristics of various image blocks. The proposed mechanism depicted a low collision probability. DCT-based techniques fail against geometric transformations (Al-Qershi & Kho, 2013). Lei, Wang, and Huang (2011) proposed a novel robust hashing method based on the use of radon transform and discrete Fourier transform (DFT). The algorithm performs well in detecting copies with a small hash size. Wu, Zhou, and Niu (2009) proposed a hashing algorithm based on radon and wavelet transform, which can identify content changes. Unfortunately, radon transform is not resistant to all the geometric transformations such as shifting & shearing. (Wu, Zhou, & Niu, 2009).

Ahmed, Siyal, and Abbas (2010) proposed a robust hash-based scheme, where pixels of each block are randomly modulated to produce the hash. Such algorithms have proven to exhibit good time-frequency localization property. Karsh, Laskar, and Aditi (2017) proposed an image hashing, where four- level 2D-DWT is applied along with SVD to produce the image hash. Chen and Hsieh (2015) proposed an algorithm, where 128-dimensional SIFT features are extracted from a normalized image. The proposed scheme significantly reduces the retrieval time with a minor loss of accuracy. Ling, Yan, Zou, Liu, and Feng (2013) proposed a fast image copy detection approach based on local fingerprint defined visual words. The mechanism outperforms similar state-of-the-art methods in terms of precision and efficiency. Lv and Wang (2012) proposed a technique similar to Ling et al. (2013), wherein the Harris detector is used to select the most stable key-points which are less vulnerable to image processing attacks after the application of SIFT.

Tang, Dai, Zhang, Huang, and Yang (2014) proposed a block-based robust image hashing based on color-vector angles and discrete wavelet transform (DWT). The proposed mechanism is robust to normal digital operations including rotation up to 5°. Tang, Huang, Dai, and Yang (2012b) proposed the use of multiple histograms in which normalized image is divided into different rings with equal area and then ring-based histogram features are extracted. The proposed mechanism is claimed to be resilient against rotation of any arbitrary angle. Tang, Zhang, Huang, and Dai (2013) proposed another hashing on the basis of ring-based entropies which outperforms similar techniques in terms of time complexity. Tang, Zhang, Li and Zhang (2016) proposed a robust image hashing method based on ring partition and four statistical features, i.e. mean, variance, skewness and kurtosis. Tang, Zhang, and Zhang (2014) proposed image hashing based on ring partition and non-negative matrix factorization (NMF). Here, NMF is applied to the secondary image produced on the basis of ring partition. The algorithms show good robustness against rotation and have good discriminative capability.

Tang, Wang, Zhang, Wei, and Su (2008) proposed a robust hashing in which NMF is applied to produce a coefficient matrix, which is coarsely quantized to produce the final hash. The algorithm exhibits a low collision probability. Karsh, Laskar, and Richhariya (2016) proposed image hashing on the basis of ring-based projected gradient non-negative matrix factorization (PG-NMF) features and local features. PGNMF generated features are combined with salient region-based features to produce the final hash. The method is robust to content preserving operations and is capable of localizing the counterfeit area. Tang, Dai, and Zhang (2012a) proposed perceptual hashing for color images using seven invariant moments. These moments are invariant to translation, scaling and rotation and have been widely used in image classification and image matching.

Although many hashing algorithms have been reported, there are still some practical problems in hashing design. More efforts are needed for developing high-performance algorithms having a desirable balance between robustness and discrimination particularly considering shifting and shearing attacks. Few of the algorithms have claimed varying degrees of success against shearing (Lei, Wang, & Huang, 2011; Zou et al., 2013; Lv & Wang, 2012). However, for shifting only one author reported its use (Wu, Zhou, & Niu, 2009).

In this work, we have proposed an image hashing based on a Hough transform and DWT which is robust to shifting & shearing apart from giving comparable performance against different image processing attacks. The key advantage of using Hough transform is that it is tolerant of gaps in the edges and

relatively unaffected by the noise & occlusion in the image. DWT can be used to convert a signal to its approximation based short representation. As shifting & shearing attacks change the orientation of the image, keeping rest of the image contents unchanged, Hough transform is applied to get its unique edge based feature for better identification. Many experiments have been conducted to validate the efficacy of our technique. receiver operating characteristics (ROC) curve comparisons with some of the representative hashing algorithms are also done, and the results indicate that proposed hashing outperforms the compared algorithms in terms of classification performance. The rest of the paper is arranged as follows: The next section describes the proposed image hashing followed with the section that gives experimental results.

PROPOSED IMAGE HASHING

In this section, we analyze the basic properties of the DWT followed with a brief description of canny edge detector. Hough transform, which is used to generate the image hash on the basis of canny edge detection is then explained in detail. Finally, the proposed approach is given which is based on the features given above.

Discrete Wavelet Transformation

In image processing, 2D wavelet is of great importance where the transformation is first applied along the rows of the image followed by transformation along the columns of the image. Such a process generates four sub-band regions LL, LH, HL and HH where LL represents blur and LH, HL & HH represents horizontal, vertical and diagonal differences respectively (Lu & Hsu, 2005; Thanki, Dwivedi, & Borisagar, 2017). DWT decomposes a signal into a set of mutually orthogonal wavelet basis functions and it is invertible, which means that the original signal can be completely recovered from its DWT representation. The main advantage of using wavelet transformation is its efficiency in converting a signal to its short representation (Tang, Dai, Zhang, Huang, & Yang, 2014a).

Let A is N x N matrix; W_N is a wavelet transformation matrix; W_N^T is the transposed values of W_N. The product $A*W_N^T$ processes the rows of A into weighted averages and differences. Similarly, the product W_N*A simply transforms the column of A into weighted averages and differences. Thus, two-dimensional DWT can be easily represented as $W_NAW_N^T$. In our implementation, we have used Daubechies wavelet transform where four-term orthogonal filter is constructed by using low-pass filter $h=(h_0,h_1,h_2,h_3)$ and the

high-pass filter g=(g_0,g_1,g_2,g_3). Mathematically, such a wavelet transform built from given h and g that is applied to vectors of length N=8 can be written in block format as follows:

$$W_8 = \begin{bmatrix} H \\ G \end{bmatrix} \tag{1}$$

Next, we compute $W_8 W_8^T$ and show that if W_8 orthogonal then it gives:

$$W_8 W_8^T = \begin{bmatrix} H \\ G \end{bmatrix} \begin{bmatrix} H^T / G^T \end{bmatrix} = \begin{bmatrix} HH^T / HG^T \\ GH^T / GG^T \end{bmatrix} = \begin{bmatrix} I_4 / 0_4 \\ 0_4 / I_4 \end{bmatrix} \tag{2}$$

where I_4 is the 4x4 identity matrix and 0_4 is the 4x4 zero matrix. After computation we get the following value for I_4 :

$$I_4 = \begin{bmatrix} a & b & 0 & b \\ b & a & b & 0 \\ 0 & b & a & b \\ b & 0 & b & a \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{3}$$

where a = h_0^2+ h_1^2+h_2^2+ h_3^2 and b = h_0h_2+h_1h_3. In this way, the following nonlinear equations are generated and are used to produce the Daubechies filter components.

$$h_0^2 + h_1^2 + h_2^2 + h_3^2 = 1 \tag{4}$$

$$h_0 h_2 + h_1 h_3 = 0 \tag{5}$$

$$h_0 - h_1 + h_2 - h_3 = 0 \tag{6}$$

$$h_0 - h_1 + h_2 - h_3 = 0 \tag{7}$$

The above generated filter components are used to produce the different sub-bands of the input image. In our proposed algorithm, we only use the approximation values (LL) of the transformed image for further steps of hash generation.

Hough Transform

Hough transform is used to identify specific shapes in an image. It converts all the points in the curve to a single location in another parameter space by

coordinate transformation (Fig. 1). Hough transform is applied to the image that is obtained after applying one of the edge detection algorithms like canny edge detection, which returns a binary image containing 1's where it finds edges in the input image and 0's elsewhere (Shih, 2010).

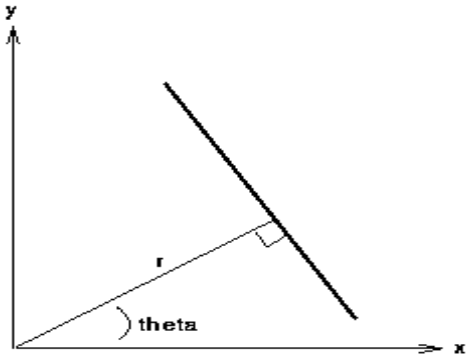

Figure 1. Parametric description of a straight line.

The Hough transform is used to detect straight lines uses the following parametric representation of the line (Aminuddin et al., 2017).

$$r = x * \cos(theta) + y * \sin(theta) \quad (8)$$

Here r is the distance from the origin to the line, along a vector perpendicular to the line and theta is the angle between the x-axis and the line (Shih, 2010). The calculation of the Hough transform is a parameter space matrix whose rows and columns correspond to the values of r and theta, respectively. For every point of interest in the image, r is calculated for every theta and it is rounded off to the nearest value. The value of that accumulator cell is incremented by one. At the end of this procedure, any value T in the matrix means that T points in the XY plane lie on the line specified by distance r and angle theta. Peak values in the matrix represent the potential lines in the input image. The algorithm for Hough transform can be given as follows:

1. Identify the maximum and minimum values of r and theta.
2. Subdivide the parametric space into accumulator cells.
3. Initialize the accumulator cells to be all zeros.
4. For all edge points (x,y) in the image

a. Use gradient direction for theta.
b. Compute r from the equation.
c. Increment A(r, theta) by one.

5. In the end, any value Q in A(r,theta) means Q points in the XY plane lie on the line specified by angle theta and r.
6. Peak values in the accumulator matrix A(r,theta) represents potential lines in the input image.

Hough transform maps each of the points in the input image into sinusoids. As given above, the Hough transform is tolerant of gaps in the edges and therefore it is relatively unaffected by the noise in the image.

Implementation Approach

The hash generation algorithm consists of various steps of preprocessing, transformation and hash generation. The process for feature extraction is shown in Fig. 2.

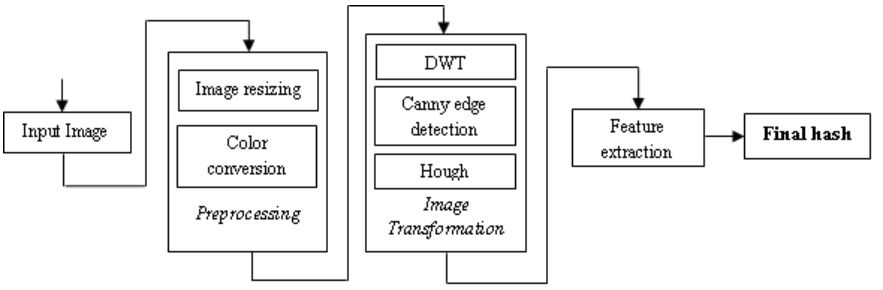

Figure 2 Basic block diagram of the proposed hashing.

Preprocessing

The first step is normalization in which the input image is normalized by employing image resizing and color space conversion. Image resizing is used to resize the original image to a standard size of 512´512. The image thus produced is converted to a grayscale image for further processing and hash generation.

Transformation and Hash Generation

In the next step, the processed image is filtered through 2D DWT by using Daubechies wavelet filter. After applying the wavelet transform, the four different sub-bands are generated where we use approximation coefficients of size 256x256 for further processing. The Canny edge detection is then

applied to the approximation matrix to produce a binary image (BW). It is important here to specify that BW is logical and having a size of 256x256. Hough transform is then applied to the generated BW matrix to produce a matrix of size 1445x360, where the rows correspond to the distance bins and the columns correspond to the angle in theta. Row-wise mean is calculated to produce a column vector of size 1445x1. Such integer column vector is used as an image hash for image identification.

Similarity Metric

To measure the similarity between a pair of hashes, L1 norm is used, which is one of the standard methods used for measuring the hash distance (Lei, Wang, & Huang, 2011). Let h1 and h2 be two image hashes, then hash distance can be calculated as follows:

$$Hash\ distance\left(HD\right)=\sum_{i=1}^{n}\left|h_1\left(i\right)-h_2\left(i\right)\right| \tag{9}$$

If the hash distance (HD) is less than a predefined threshold T, the images are considered to be visually identical. Otherwise, they are classified as different images.

EXPERIMENTAL RESULTS

To demonstrate the efficacy of the proposed mechanism, we conduct a series of experiments to verify the proposed approach's accuracy, efficiency and sensitivity against a number of image processing attacks.

Robustness Analysis

The proposed technique is applied to test images from the USC-SIPI image database (USC-SIPI, 2007). A sample of some of the standard images is shown in Fig. 3. Each of the original images is used to create 88 modified versions by employing a number of image processing operations such as rescaling, brightness adjustment, contrast adjustment, gamma correction, Gaussian low-pass filtering, rotation as these are used in most of the research papers of the area of image hashing (Tang et al., 2014b), (Tang et al., 2013a), (Tang et al., 2008), (Tang et al., 2014c). The modified versions were created using MATLAB with the attack parameters as shown in Table 1. For example,

we take an input image like 'Airplane' and create its brightness adjustment based attacked copies by changing its intensity values as mentioned in Table 1. Similarly, duplicate copies based on different attacks of the original image 'Airplane' is created by using attacks given in Table 1. This process of duplicate image creation will be over, only when we create the duplicate copies of all the original images which are to be used in the experiment. After generating the "duplicates", hashes are extracted from all the images including the original one and the Hash distance is calculated between the original image and its duplicate copies. Definitely, the hash distance in such a scenario represents the distance between hash of each of the original image and its different attacked copies. The hash distance value, which is categorized on the basis of different attacks for all the considered images, is given in Table 2.

Figure 3. Standard benchmark images used.

Table 1

Generation of Duplicate Copies of Original Images

Attack	Details	Parameter variation	No. of images
Brightness adjustment	Intensity values	0.05, 0 .10, 0.15, 0.20	4
Contrast adjustment	Intensity values	0.75, 0.80, 0.85, 0.90	4
Cropping	Xmin, Ymin	(2,2), (4,4), (6,6), (9,9), (11,11)	5

(continued)

Attack	Details	Parameter variation	No. of images
Gamma correction	Gamma	1.25, 1.5, 1.75, 2.0	4
3x3 Gaussian low-pass filtering	Standard deviation	0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9, 1.0	8
Gaussian Noise	Variance	0.01, 0.02, 0.03, 0.04, 0.05	5
JPEG Compression	Quality	30, 40, 50, 60, 70, 80, 90, 100	8
Median Filter	Neighborhood	(3,3), (5,5), (7,7), (9,9), (11,11)	5
Rescaling	Ratio	0.5, 0.75, 0.9, 1.1, 1.5, 1.75, 2.0	7
Rotation	Angle	-1, -0.75, -0.5, -0.25, 0.25, 0.5, 0.75, 1	8
Salt & Pepper	Noise density	0.01, 0.03, 0.05, 0.07, 0.09	5
Speckle	Variance	0.02, 0.04, 0.06, 0.08, 1.0	5
Shift-H	Positions	10, 20, 30, 40, 50	5
Shift-V	Positions	10, 20, 30, 40, 50	5
Shift-HV	Positions	(10 10), (20 20), (30 30), (40 40), (50 50)	5
Shearing	Transformation values	0.1, 0.2, 0.3, 0.4, 0.5	5
Total			**88**

Table 2 presents the maximum, minimum and mean of hash distance under different attacks. It is observed that all the mean values are less than 0.7, while the maximum distance, taking into account all attacks, is less than 2.6. It is justifiable to choose a distance value of 0.78 as the threshold on which the proposed technique is resistant to most image processing operations. In this case, 96.59% visually similar images are correctly identified as copies of original images. In this experiment, we have used 10 original images and created 88 copies of each of the original images to produce 880 copies. Out of the total number of 880 duplicate copies, our system can correctly identify 850 as copied ones, i.e. 96.59% as copied ones. Ideally, we are looking for that threshold value where the percentage of visually similar images identified as copied is higher and the percentage for different images identified as similar images is low. It is inferred that the threshold value of 0.78 gives good experimental results.

Table 2

Maximum, Minimum, Mean and Standard Deviation of Hash Distances for Different Attacks

Attack	Max	Min	Mean	Std Dev
Brightness Adjustment	0.39	0.046	0.169	0.093
Contrast Adjustment	0.443	0.082	0.195	0.088
Cropping	0.548	0.092	0.222	0.102
Gamma Correction	0.779	0.107	0.266	0.165
Gaussian Low-pass filtering	0.523	0.064	0.213	0.13
Gaussian Noise	2.25	0.142	0.675	0.482
JPEG	0.292	0.007	0.065	0.051
Median filter	1.919	0.077	0.658	0.42
Rescaling	0.639	0.035	0.196	0.12
Rotation	0.397	0.143	0.243	0.06
Salt & Pepper	2.551	0.108	0.399	0.416
Speckle	0.935	0.123	0.34	0.205
Shift-H	0.481	0.171	0.278	0.072
Shift-HV	0.73	0.204	0.414	0.122
Shearing	1.141	0.15	0.508	0.236
Shift-V	0.745	0.154	0.344	0.114

Discrimination Analysis

To demonstrate discriminability, 36 different images of sizes ranging from 225´225 to 2144´1424 are collected from USC-SIPI database (USC-SIPI, 2007). The Hash distance is calculated between each pair of 36 images to generate 630 different hash distances. The distribution of such Hash distances is shown in Fig. 4. The maximum, minimum, mean and standard deviation calculated on the basis of 630 hash distances are 5.93, 0.417, 1.8 and 0.99 respectively. If the threshold is 0.78, then 4.45% different images are falsely identified as similar images, which is because out of 630 calculated hash distances 28 is having values less than a threshold of 0.78. In general, a small threshold will improve the discrimination but simultaneously decreases robustness. Keeping in view this important point, threshold must be chosen depending upon the requirements of the specific application.

The mean value of discrimination is 1.8, which is more than four times larger than the highest mean of robustness except for Gaussian noise and median filter. For Gaussian noise and median filter, the mean of discrimination value is almost three times larger than the highest mean of robustness. Also,

the maximum value of discrimination is 5.93 which is more than six times larger than the maximum value of robustness, except for Gaussian noise and salt & pepper. For Gaussian noise and salt & pepper, this value is almost more than twice the maximum value of robustness. Ideally, a copy detection technique should exhibit very low values corresponding to robustness and high values corresponding to discrimination. This would imply that the technique is capable of correctly identifying duplicated copies while at the same time rejecting different images. Keeping in view this definition of robustness and discrimination, the proposed hashing exhibits promising results as evidenced by the graph shown above.

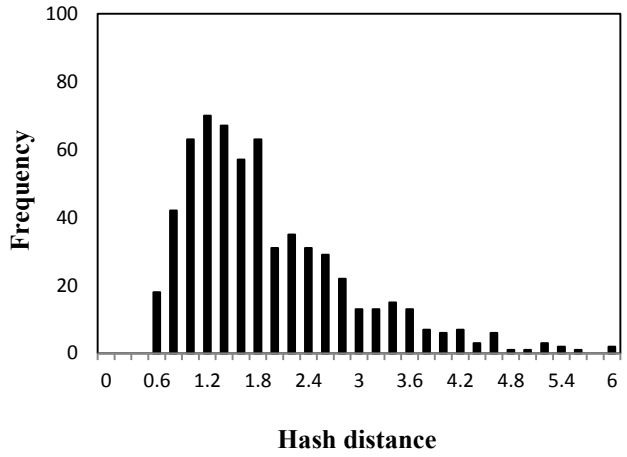

Figure 4. Distribution of hash distance for discrimination.

Normalized Average Mean Value Difference

The observations based on the Hash distance presented in the previous section were categorized on the basis of different attacks. In this section, the analysis is performed image-wise and the maximum, minimum, mean and standard deviation of the Hash distance is calculated by considering all but one of the attacks. Since, 16 different kinds of attacks have been considered, such an analysis results in 16 different maximum, minimum, mean and standard deviation values. Further, a set of values is obtained when all the attacks are considered together. The difference between the mean values is obtained by considering all the attacks and all but one of the attacks. Finally, the averaging of the difference values is done in order to reach to some conclusion. One of the important reasons to consider such an analysis is to analyze the effect of

different attacks on the proposed approach. However, in this article for the sake of brevity & without sacrificing any understandability, only the mean values of the proposed technique are included for calculation.

Acronym used in the Table 3 indicates the mean values that are obtained by considering all the attacks *except* the attack represented by the acronym. For instance, column 3 depicts the mean values obtained for the image by considering all attacks *except* brightness adjustment (BA). Other acronyms are: contrast adjustment (CA), Cropping (Crop), Gamma correction (GC), Gaussian low-pass filtering (GLPF), Gamma correction (GN), JPEG compression (JPEG), Median filter (MF), Rescaling (RE), Rotation (RO), Salt and pepper noise (S&P), Speckle noise (SPK), Shifting-H(S-H), Shifting-V(S-V), Shifting-HV(S-HV) and Shearing (Shea). To make a fair comparison of the obtained mean values, four state-of-the-art techniques are referenced.

Table 3 represents the mean values obtained by the proposed approach. Similarly, we obtained the mean values by using the techniques reported by (Tang et al., 2014b), (Tang et al., 2013a), (Tang et al., 2008) and (Ou et al., 2009) respectively. It is important here to emphasize that there may be slight difference between the values reported by (Tang et al., 2014b), (Tang et al., 2013a), (Tang et al., 2008), (Ou et al., 2009) and the values obtained by us. This is because the dataset used by us is different as compared to the dataset used by the reported techniques. Also approach adopted to generate duplicate copies of original ones also differs. However, in our experiment in order to make a fair comparison among all the reported techniques and the proposed technique, they are evaluated on the same dataset. Therefore, the comparison here can be correctly used to draw any findings from the calculated results.

The difference is calculated one by one between the mean values given in the first column and the remaining 16 columns. Finally, the averaging of different values is done to produce the row vector, which corresponds to the values related to different attacks. This calculation is done for all the techniques and is given in Table 4. It was found that the calculated values have varying ranges for each of the referenced techniques. Therefore, to perform a fair comparison between them, the values are normalized within the range of 0 to 1. The normalized average values of the proposed technique along with the techniques reported in (Tang et al., 2014b), (Tang et al., 2013a), (Tang et al., 2008) and (Ou et al., 2009) are given in Table 5 and Fig. 5 plots these normalized values. The normalized values of Shifting horizontally (SF-H), Shifting horizontally-vertically (SF-HV), Shearing (Shea) and Shifting vertically (SF-V) corresponding to the proposed technique are 0.484, 0.661, 0.784, and 0.570 respectively. It is quite evident from the values given in Table 5 that the proposed technique exhibits lowest average values for all the shifting and shearing attacks.

Table 3

Mean values of hash distances under different attacks for the proposed technique

Image	All Attacks	BA	CA	Crop	GC	GLPF	GN	JPEG	MF	RE	RO	S&P	SPK	SF-H	SF-HV	Shea	SF-V
Airplane	0.24	0.25	0.24	0.25	0.24	0.25	0.24	0.26	0.21	0.25	0.25	0.24	0.24	0.24	0.22	0.22	0.23
Barbara	0.24	0.25	0.24	0.24	0.24	0.25	0.22	0.26	0.22	0.25	0.24	0.24	0.24	0.24	0.23	0.23	0.24
Boat	0.34	0.35	0.35	0.35	0.35	0.36	0.30	0.37	0.30	0.36	0.35	0.35	0.33	0.34	0.33	0.33	0.34
Couple	0.36	0.36	0.37	0.36	0.36	0.36	0.34	0.39	0.33	0.37	0.37	0.36	0.36	0.36	0.36	0.33	0;.36
Goldhill	0.37	0.38	0.38	0.38	0.38	0.38	0.33	0.39	0.35	0.38	0.38	0.36	0.37	0.38	0.37	0.35	0.37
Lena	0.25	0.26	0.26	0.26	0.26	0.26	0.24	0.27	0.24	0.26	0.25	0.26	0.25	0.25	0.24	0.24	0.25
Peppers	0.25	0.26	0.26	0.26	0.25	0.26	0.23	0.27	0.24	0.26	0.25	0.25	0.24	0.25	0.25	0.24	0.25
Sailboat	0.27	0.28	0.27	0.27	0.27	0.28	0.27	0.29	0.24	0.28	0.27	0.27	0.27	0.27	0.26	0.26	0.27
Splash	0.37	0.37	0.37	0.38	0.37	0.37	0.32	0.39	0.36	0.37	0.37	0.32	0.36	0.37	0.37	0.37	0.37
Zelda	0.41	0.41	0.41	0.41	0.40	0.41	0.37	0.44	0.39	0.41	0.41	0.40	0.42	0.42	0.41	0.40	0.41

Journal of ICT, 17, No. 4 (October) 2018, pp: 653–678

Table 4

Average mean values difference of compared techniques for different attacks

Technique	BA	CA	CROP	GC	GLPF	GN	JPEG	MF	RE	RO	SP	SPK	SF-H	SF-HV	SHEA	SF-V
[Tang et al., 2014b]	-0.10	-0.15	0.02	-0.09	-0.02	-0.03	-1.41	0.09	-0.25	0.78	-0.06	-0.05	0.07	0.36	0.53	0.30
[Tang et al., 2013a]	-0.12	-0.04	-0.15	-0.07	-0.29	0.06	-0.39	0.00	-0.11	0.22	0.00	-0.08	0.19	0.31	0.33	0.13
[Tang et al., 2008]	0.03	-0.20	0.07	-0.25	-0.87	0.14	-1.15	-0.21	-0.66	0.17	-0.57	-0.24	0.83	0.91	1.00	0.91
[Ou et al., 2009]	1.12	2.01	0.24	0.81	-1.80	0.27	-10.55	-0.12	-1.48	0.04	0.06	-0.29	2.11	2.62	3.18	1.24
Proposed	-0.01	-0.01	-0.01	0.00	-0.01	0.02	-0.02	0.02	-0.01	-0.01	0.01	0.00	0.00	0.01	0.01	0.00

Table 5

Normalized average mean values difference of compared techniques for different attacks

Technique	BA	CA	CROP	GC	GLPF	GN	JPEG	MF	RE	RO	SP	SPK	SF-H	SF-HV	SHEA	SF-V
[Tang et. al, 2014b]	0.599	0.575	0.654	0.601	0.635	0.631	0.000	0.682	0.527	1.000	0.614	0.619	0.675	0.807	0.884	0.778
[Tang et. al , 2013a]	0.376	0.482	0.329	0.439	0.138	0.625	0.000	0.541	0.393	0.849	0.543	0.433	0.804	0.966	1.000	0.719
[Tang et al., 2008]	0.549	0.440	0.567	0.417	0.127	0.598	0.000	0.436	0.227	0.610	0.266	0.420	0.919	0.959	1.000	0.955
[Ou et al., 2009]	0.850	0.914	0.786	0.827	0.637	0.788	0.000	0.760	0.661	0.771	0.773	0.747	0.922	0.959	1.000	0.858
Proposed	0.382	0.408	0.412	0.481	0.319	1.000	0.000	0.977	0.314	0.382	0.642	0.565	0.484	0.661	0.784	0.570

Journal of ICT, 17, No. 4 (October) 2018, pp: 653–678

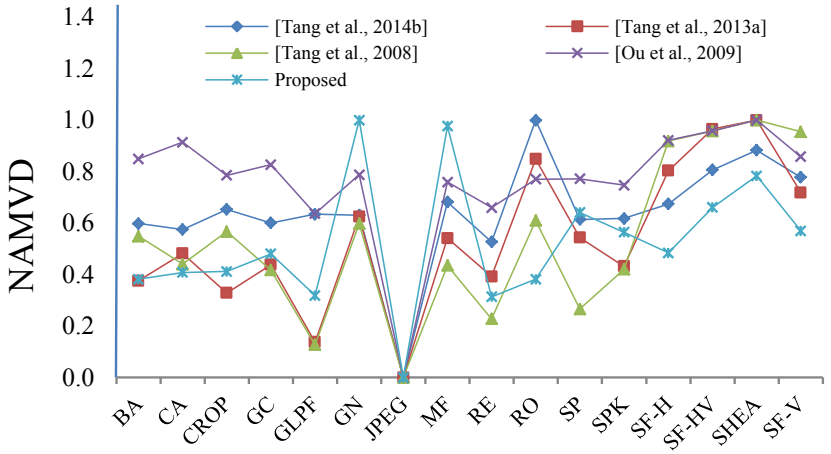

Figure 5. Normalized average mean difference values for different techniques.

Performance Comparison with State-of-the-art Techniques

Performance comparison of the proposed technique with the state-of-the-art techniques is also done in terms of robustness and discriminability by using ROC curve. The techniques compared with include (Tang et al., 2014b), (Tang et al., 2013a), (Tang et al., 2008) and (Ou et al., 2009). In (Tang et al., 2014b), the images were pre-processed by converting to a dimension of 512´512 image, application of Gaussian filtering and then converted to YCbCr for hash generation. In (Tang et al., 2013a) the image is resized to 512´512, followed by color conversion to YCbCr and HSI color models. In (Tang et al., 2008), the image is resized to 512´512 followed by gray-scale conversion for hash generation. In (Ou et al., 2009), the images are resized to 512´512 followed by conversion to YCbCr and application of 5´5 Gaussian filtering to generate the final image which is used for hash generation. To represent the performance in terms of robustness and discriminability, the receiver operating characteristics (ROC) curve is employed which is usually plotted between the true positive rate (TPR) and the false positive rate (FPR). These parameters are defined as:

$$TPR = \frac{n_1}{N_1} \quad FPR = \frac{n_2}{N_2} \tag{10}$$

where n1 is the number of visually identical images correctly identified as copies and N1 is the total number of identical images. Similarly, n2 is the number of different images incorrectly identified as a copy and N2 is the total

number of different images. TPR and FPR can be used to evaluate the robustness and the discriminability respectively. If two algorithms exhibit the same TPR, then the algorithm with the lower FPR is considered as better performing. Similarly, if two algorithms exhibit the same FPR, then the algorithm with the higher TPR is considered to be better performing. In order to draw the ROC curve, it is important to calculate the above parameters for varying thresholds. In general, a small threshold will improve the discrimination but simultaneously decreases the robustness.

The ROC curve for different algorithms including the proposed is given in Fig. 6. The various thresholds used for producing the ROC for all the algorithms are given in Table 6. From Fig. 6, it is evident that the ROC curve of the proposed technique is closer to zero as compared to the techniques reported in Tang et al. (2014b), Tang et al. (2013a), Tang et al. (2008) and Ou et al. (2009). The value of TPR when FPR = 0 in case of Tang et al. (2014b), Tang et al. (2013a), Tang et al. (2008) and Ou et al. (2009) is 0.61, 0.85, 0.38, 0.30 respectively while for the proposed technique the value is 0.93. Similarly, the value of the FPR when TPR = 1 in case of (Tang et al., 2014b), (Tang et al., 2013a), (Tang et al., 2008) and (Ou et al., 2009) is 0.91, 0.21, 1.0, 0.98 respectively while for the proposed technique the value is 0.13. Taking into account the values of the robustness and the discriminability from the previous subsection, along with the TPR and FPR values obtained in this subsection, it is quite clear that the proposed hashing technique outperforms some of the notable hashing techniques.

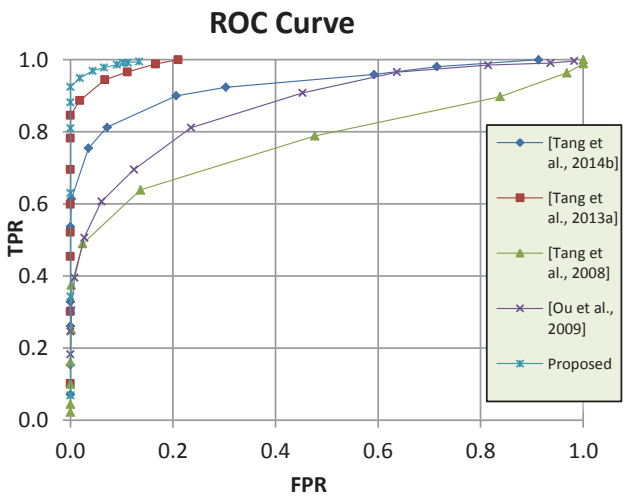

Figure 6. ROC curve comparison between proposed and other hashing algorithms.

Table 6

Thresholds used for generating ROC curves of different algorithms

Algorithm	Threshold												
[Tang et al., 2014b]	38	35	32	29	26	23	20	17	14	11	8	5	2
[Tang et al., 2013a]	13	12	11	10	9	8	7	6	5	4	3	2	1
[Tang et.al., 2008]	196	186	176	166	156	146	136	126	116	106	96	86	76
[Ou et.al., 2009]	225	214	203	192	181	170	159	148	137	126	115	104	93
Proposed	1.5	1.38	1.26	1.14	1.02	0.9	0.8	0.66	0.5	0.42	0.3	0.18	0.06

Running Time

The running time of the proposed algorithm is analyzed by generating an image hash of 200 different images. The image hashes are generated by using a computer having an Intel Pentium Core-2-Duo processor with a clock frequency of 1.8 GHz and 4GB of RAM. The MATLAB version used was R2014b. The average time for hash generation as reported in Tang et al. (2014b), Tang et al. (2013a), Tang et al. (2008) and Ou et al. (2009) is 0.24, 0.28, 1.14, 0.5 seconds respectively while for the proposed algorithm it is 0.22 seconds. It is evident from the Table 7 that the execution time of the proposed technique is smallest as compared to few of the notable algorithms.

Table 7

Summary of execution time for different algorithms

Mechanism	Total Time (in sec)	No. of Images	Time per Image (in sec)
[Tang et al., 2014b]	48.348	200	0.2417
[Tang et al., 2013a]	57.469	200	0.2873
[Tang et al., 2008]	228.458	200	1.1422
[Ou et al., 2009]	100	200	0.5
Proposed	45.647	200	0.2282

Distribution of Hash Distance

To evaluate the distribution of the Hash distance, two sets of image datasets were employed. One for the similar images and the other for dissimilar images. To produce the dataset of similar images, 225 unique images are taken like

Airplane, Baboon, Lena in addition to images from the 17 Category Flower dataset (17 Category). For each of these images, 6 copies are generated using different image processing attacks to produce a set of 1350 similar images. The attacks applied include rotation, rescaling, Gaussian noise, brightness adjustment etc. Similarly, for the dataset of dissimilar images, 1350 different images are taken from the 17 Category Flower dataset (17 Category). After arranging the images in the dataset, Hash distance is calculated by using the proposed algorithm.

The distribution of the Hash distance for both similar and dissimilar images is given in Fig. 7 and Fig. 8 respectively. Here, the threshold value used is 0.78, as it is identified during the robustness and the discrimination analysis. It is evident from these figures that the Hash distance between similar images is below threshold of 0.78, with a few exceptions. More specifically, out of 1350 similar images 1305 images return a Hash distance less than the threshold i.e. 96.66% of the total images within the dataset return a Hash distance below the threshold. Correspondingly, most of the dissimilar images return a Hash distance well above the threshold i.e. out of 1350 different images, 58 images return hash distances below the threshold. Therefore, we can say that 4.29% different images are identified as similar ones. This analysis proves the efficacy of the proposed approach. Also, the number of outliers in both the categories of (similar and dissimilar) images conforms to the true positive and false negative analysis performed for evaluating robustness and discrimination.

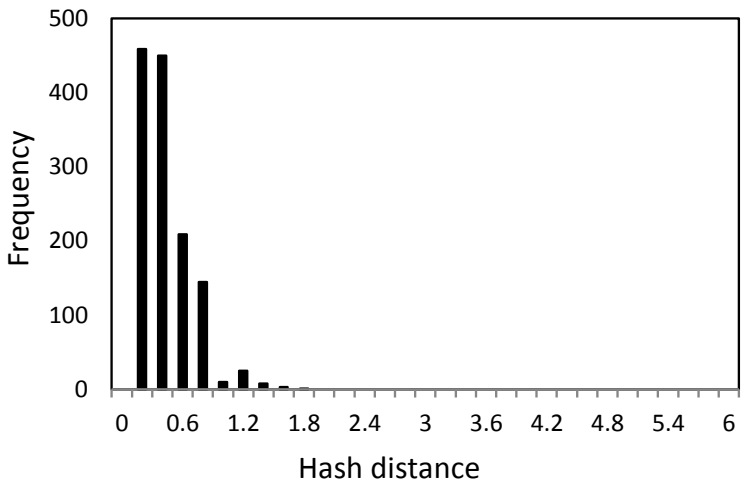

Figure 7. Distribution of hash distance for similar images.

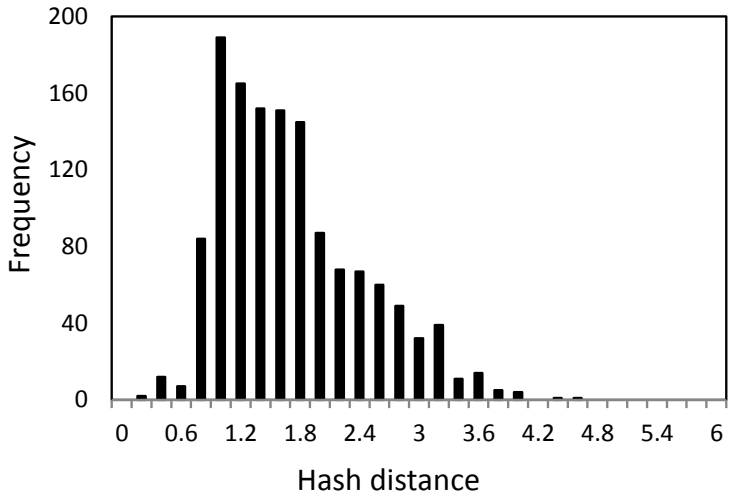

Figure 8. Distribution of hash distance for different images.

Comparison between Different Variants of Wavelet Transform

Implementing a hashing technique based on the DWT requires the calculation of wavelet coefficients at different levels. Any change in the level of DWT would change the corresponding coefficients. This section verifies the effect of DWT by calculating the hash for different levels of DWT, whereas keeping the rest of the parameters constant. It is important here to specify that the proposed technique makes use of single level of 2D DWT. To demonstrate the effect of this variation, a set of 300 images were taken from *17 Category Flower* dataset (17 Category). A further 88 "copies" were produced from a single image after applying various image processing operation (Table 1) leading to a total dataset size of 388 images. Initially, single level 2D DWT is applied in the proposed algorithm for finding duplicate copies of the original image. In the next iteration, two level 2D DWT is used for finding the duplicate copies. This procedure is repeated until we reach the level six of 2D DWT.

To effectively represent results of this analysis, ranking of the results based on the Hash distance is done. Ranking is basically used to represent the order in which multiple copies of the single image are found in the large dataset of images. For copy detection, ideally we require that the rank at which all the copies are found must be equal to the number of copies, i.e. the copied images should be represented at top with low rank and the non-copied images should have higher rank as compared to copied one. The rank of the first 83 copies of the original image at one, two, three, four, five and six levels of DWT

are 83, 90, 105, 100, 196 and 193 respectively. We can easily draw conclusion from the given values that at lower level of DWT lower rank is generated and at the higher level it generates higher rank. Specifically, at level one we obtained the lowest rank of 83 among all the compared levels. Therefore, the best performance of the proposed technique can be obtained when one level 2D DWT is used for hash generation and comparison. It is important here to clarify that result of 88 copies is not considered in this analysis as due to some outliers we are getting higher ranks for all the levels of DWT. However, such result conforms to the results obtained for 83 copies. The representation of ranks is shown in Fig. 9.

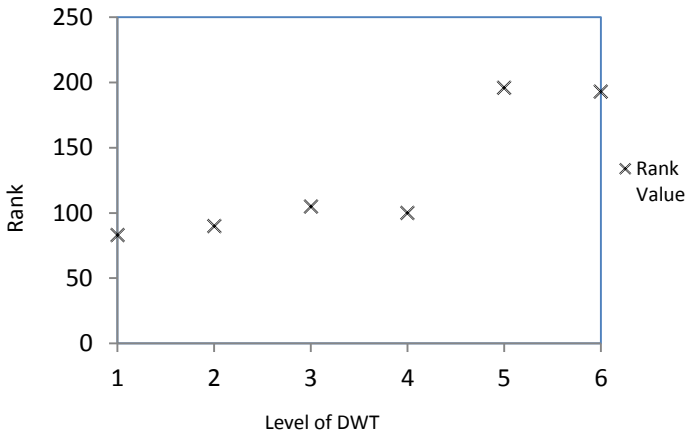

Figure 9. Ranking of results based upon hash distance for different level.

CONCLUSION

In this paper, we have presented a robust image hashing technique that employs Discrete Wavelet Transform and Hough transform to generate an image hash, which is used to differentiate the duplicate copies of images from their original ones. Many experiments have been conducted to validate the performances of the proposed hashing. Normalized average mean value difference (NAMVD) is calculated to show that the proposed technique shows remarkable robustness to various shifting operations apart from performing well for other content preserving operations like rotation, contrast adjustment. Compared with four standard algorithms, the proposed technique achieves better performance in terms of ROC curves, which clearly shows that proposed technique is having better classification in terms of robustness and

discrimination. The proposed technique is also evaluated to know the effect of different levels of DWT in its performance. The result shows that level one gives best results as compared to different levels. Lastly, the execution time of the proposed approach is measured which is the smallest as compared to other referenced techniques. Therefore, proposed method can be used for content-based image authentication in large-scale image databases.

ACKNOWLEDGEMENT

The authors gratefully acknowledge the use of services and facilities provided by Aligarh Muslim University, Aligarh to conduct this research work.

REFERENCES

Ahmed, F., Siyal, M. Y., & Abbas, V. U. (2010). A secure and robust hash-based scheme for image authentication. *Signal Processing, 90*(5), 1456-1470. https://doi.org/10.1016/j.sigpro.2009.05.024.

Al-Qershi, O. M., & Khoo, B. E. (2013). Passive detection of copy-move forgery in digital images: State-of-the-art. *Forensic Science International, 231*(1-3), 284-295. https://doi.org/10.1016/j.forsciint.2013.05.027.

Aminuddin, N. S., Ibrahim, M. M., Ali, N. M., Radzi, S. A., Saad, W. H. M., & Darsono, A. M. (2017). A new approach to highway lane detection by using Hough transform technique. *Journal of Information Communication and Technology, 16*(2), 244-260.

Battiato, S., Farinella, G. M., Messina, E., & Puglisi, G. (2012). Robust image alignment for tampering detection. *IEEE Transactions on Information Technology Forensics and Security, 7*(4), 1105-1117. https://doi.org/10.1109/TIFS.2012.2194285.

Chen, C. C., & Hsieh, S. L. (2015). Using binarization and hashing for efficient SIFT matching. *Journal of Visual Communication & Image Representation, 30*, 86-93. https://doi.org/10.1016/j.jvcir.2015.02.014.

Fleet, P. J. V. (2007). *Discrete Wavelet Transformation: Elementary Approach with Applications*. Wiley-Interscience. https://doi.org/10.1002/9781118032404.

Hsiao, J. H., Chen, C. S., Chien, L. F., & Chen, M. S. (2007). A new approach to image copy detection based on extended feature sets. *IEEE Transactions on Image Processing, 16*(8), 2069-2079. https://doi.org/10.1109/TIP.2007.900099.

Kang, X. & Wei, S. (2009). An efficient approach to still image copy detection based on SVD and block partition for digital forensics. *IEEE International Conference on Intelligent Computing and Intelligent Systems (ICIS),* 457-461. https://doi.org/10.1109/ICICISYS.2009.5358149.

Karsh, R. K., Laskar, R. H., & Aditi (2017). Robust image hashing through DWT-SVD and spectral residual method. *EURASIP Journal on Image and Video Processing, 2017:31*, 1-17. https://doi.org/10.1186/s13640-017-0179-0.

Karsh, R. K., Laskar, R. H., & Richhariya, B. B. (2016). Robust image hashing using ring partition-PGNMF and local features. *SpringerPlus, 5*(1), 1-20. https://doi.org/10.1186/s40064-016-3639-6.

Lei, Y., Wang, Y., & Huang, J. (2011). Robust image hash in radon transform domain for authentication. *Signal Processing: Image Communication, 26*(6), 280-288. https://doi.org/10.1016/j.image.2011.04.007.

Ling, H., Yan, L., Zou, F., Liu, C., & Feng, H. (2013). Fast image copy detection approach based on local fingerprint defined visual words. *Signal Processing, 93*(8), 2328-2338. https://doi.org/10.1016/j.sigpro.2012.08.011.

Liu, G., Wang, J., Lian, S. & Wang, Z (2011). A passive image authentication scheme for detecting region-duplication forgery with rotation. *Journal of Network and Computer Applications, 34*(5), 1557-1565. https://doi.org/10.1016/j.jnca.2010.09.001.

Lu, C. S., & Hsu, C. Y. (2005). Geometric distortion resilient image hashing scheme and its applications on copy detection and authentication. *Multimedia systems, 11*(2), 159-173. https://doi.org/10.1007/s00530-005-0199-y.

Lv, X., & Wang, Z. J. (2012). Perceptual image hashing based on shape contexts and local feature points. *IEEE Transactions on Information Forensics and Security, 7*(3), 1081-1093. https://doi.org/10.1109/TIFS.2012.2190594.

Ou, Y., & Rhee, K. H. (2009). A key-dependent secure image hashing scheme by using radon transform. *2009 International Symposium on Intelligent Signal Processing and Communications Systems (ISPACS)*, 595-598. https://doi.org/10.1109/ISPACS.2009.5383770.

Qazi, T., Hayat, K., Khan, S. U., Madani, S. A., Khan, I. A., Kolodziej, J., Li, H., Lin, W., Yow, K C. & Xu, C. Z. (2013). Survey on blind image forgery detection. *IET Image Processing, 7*(7), 660-670. https://doi.org/10.1049/iet-ipr.2012.0388.

Qureshi, M. A., & Deriche, M. (2015). A bibliography of pixel-based blind image forgery detection. *Signal Processing: Image Communication, 39*(A), 46-74. https://doi.org/10.1016/j.image.2015.08.008.

Redi, J. A., Taktak, W., & Dugelay, J. A. (2011). Digital image forensics: a booklet for beginners. *Multimedia Tools and Applications, 51*(1), 133-162. https://doi.org/10.1007/s11042-010-0620-1

Rey, C., & Dugelay, J. L. (2002). A survey of watermarking algorithms for image authentication. *EURASIP Journal on Applied Signal Processing, 2002*(1), 613-621. https://doi.org/10.1155/S1110865702204047.

Seo, J. S., Haitsma, J., Kalker, T., & Yoo, C. D. (2006). A Robust image fingerprinting system using the Radon transform. *Signal processing: Image Communication, 19*(4), 325-339. https://doi.org/10.1016/j.image.2003.12.001.

Shih, F. Y. (2010). *Image Processing and Pattern Recognition (Fundamental and Techniques). Wiley Press*. https://doi.org/10.1002/9780470590416.

Tang, Z., Dai, Y., & Zhang, X. (2012a). Perceptual hashing for color images using invariant moments. *Applied Mathematics and Information Sciences, 6*(2S), 643S-650S.

Tang, Z., Dai, Y., Zhang, X., Huang, L., & Yang, F. (2014a). Robust image hashing via color vector angles and discrete wavelet transform. *IET Image Processing, 8*(3), 142-149. https://doi.org/10.1049/iet-ipr.2013.0332.

Tang, Z., Huang, L., Dai, Y., & Yang, F. (2012b). Robust image hashing based on multiple histograms. *International Journal of Digital Content Technology and its Applications (JDCTA), 6*(23), 39-47. https://doi.org/10.4156/jdcta.vol6.issue23.5.

Tang, Z., Wang, S., & Zhang, X. (2010). Lexicographical framework for image hashing with implementation based on DCT and NMF. *Multimedia Tools and Applications, 52*(2-3), 325-345. https://doi.org/10.1007/s11042-009-0437-y.

Tang, Z., Wang, S., Zhang, X., Wei, W., & Su, S. (2008). Robust image hashing for tamper detection using non-negative matrix factorization. *Journal of Ubiquitous Convergence and Technology, 2*(1), 18-26. https://doi.org/10.1109/INFOP.2015.7489395.

Tang, Z., Yang, F., Huang, L., & Zhang, X. (2014b), Robust image hashing with dominant DCT coefficients. *Optik, 125*(18), 5102-5107. https://doi.org/10.1016/j.ijleo.2014.05.015.

Tang, Z., Zhang, X., Dai, X., Yang, J., & Wu, T. (2013a). Robust image hash function using local color features. *International Journal of Electronics and Communications (AEU), 67*(8), 717-722. https://doi.org/10.1016/j.aeue.2013.02.009.

Tang, Z., Zhang, X., Huang, L., & Dai, Y. (2013b). Robust image hashing using ring-based entropies. *Signal Processing, 93*(7), 2061-2069. https://doi.org/10.1016/j.sigpro.2013.01.008.

Tang, Z., Zhang, X., Li, X., & Zhang, S. (2016). Robust image hashing with ring partition and invariant vector distance. *IEEE Transactions on Information Forensics and Security, 11*(1), 200-214. https://doi.org/10.1109/TIFS.2015.2485163.

Tang, Z., Zhang, X., & Zhang, S. (2014c). Robust perceptual image hashing based on ring partition and NMF. *IEEE Transactions on Knowledge and Data Engineering, 26*(3), 711-724. https://doi.org/10.1109/TKDE.2013.45.

Thanki, R., Dwivedi, V. V., & Borisagar, K. (2017). Robust watermarking technique using different wavelet decomposition levels for signature image protection. *Journal of Information Communication and Technology, 16*(1), 157-174.

USC-SIPI Image Database, 2007. *http://sipi.usc.edu/database*

Wu, D., Zhou, X., & Niu, X. (2009). A novel image hash algorithm resistant to print-scan. *Signal Processing, 89*(12), 2415-2424. https://doi.org/10.1016/j.sigpro.2009.05.016.

Zou, F., Feng, H., Ling, H., Liu, C., Yan, L., Li, P., & Li, D. (2013). Nonnegative sparse coding induced hashing for image copy detection. *Neurocomputing, 105*, 81-89. https://doi.org/10.1016/j.neucom.2012.06.042.17 Category Flower Dataset. *http://www.robots.ox.ac.uk/~vgg/data/flowers/17/*