View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Institute of Advanced Engineering and Science

International Journal of Electrical and Computer Engineering (IJECE)
Vol. 9, No. 4, August 2019, pp. 2950~2959
ISSN: 2088-8708, DOI: 10.11591/ijece.v9i4.pp2950-2959

Modified CSLBP

Varsha Patil[1], Tanuja Sarode[2]
[1]Department of Computer Engineering, Mumbai University, India
[2]Department of Computer Engineering, TSEC, Mumbai University, India

Article Info

Article history:

Received Sep 26, 2018
Revised Mar 18, 2019
Accepted Mar 21, 2019

Keywords:

Authentication
CSLBP
Hashing
Histogram
Laplacian of Gaussian
Quantization
Standard deviation

ABSTRACT

Image hashing is an efficient way to handle digital data authentication problem. Image hashing represents quality summarization of image features in compact manner. In this paper, the modified center symmetric local binary pattern (CSLBP) image hashing algorithm is proposed. Unlike CSLBP 16 bin histogram, Modified CSLBP generates 8 bin histogram without compromise on quality to generate compact hash. It has been found that, uniform quantization on a histogram with more bin results in more precision loss. To overcome quantization loss, modified CSLBP generates the two histogram of a four bin. Uniform quantization on a 4 bin histogram results in less precision loss than a 16 bin histogram. The first generated histogram represents the nearest neighbours and second one is for the diagonal neighbours. To enhance quality in terms of discrimination power, different weight factor are used during histogram generation. For the nearest and the diagonal neighbours, two local weight factors are used. One is the Standard Deviation (SD) and other is the Laplacian of Gaussian (LoG). Standard deviation represents a spread of data which captures local variation from mean. LoG is a second order derivative edge detection operator which detects edges well in presence of noise. The proposed algorithm is resilient to the various kinds of attacks. The proposed method is tested on database having malicious and non-malicious images using benchmark like NHD and ROC which confirms theoretical analysis. The experimental results shows good performance of the proposed method for various attacks despite the short hash length.

Copyright © 2019 Institute of Advanced Engineering and Science.
All rights reserved.

Corresponding Author:

Varsha Patil,
Department of Computer Engineering,
Mumbai University, India
Email: varshasp2977@gmail.com

1. INTRODUCTION

Over the last decade, there have been tremendous developments and advances in digital media such as image, audio and video. Various image editing tools are also easily available for modification of original content. Intentionally or unintentionally, these editing operations might change data maliciously. To deal with such problems, blind and non-blind approaches exist to handle authentication of the original content. Blind approaches do not need any extra information to determine change in original content. While non-blind approaches need some piece of information to determine authenticity of data. Watermarking and hashing come under category of non-blind techniques. Image hashing represents the image in an abstract form. This abstract form is obtained by extraction, compression, quantization of important features. In image hashing, unlike watermark, the generated image hash is not inserted in the image data, rather it is stored in the image header. Therefore original content of image remains intact. As hash is stored separately in an image, it must be compact in length. To identify either content-change or content-preserving operation on the original data, the hash code of original image stored in image header is compared with hash of modified image. If the difference of compared hash codes exceeds the set threshold then it indicates malicious

operation. Apart from compact size, other desirable property of the hash is discrimination power that is to distinguish between content-preservation and content-change operations [1-3].

The extracted image features are large in size due to high dimensional nature of the image. In order to restrict the hash to a small size, it is necessary to extract quality features at various levels like local, semi global and global, in various domains and stored in quantized form. Proposed hashing method 'Modified CSLBP' extracts texture details from an image. Center Symmetric Local Binary Pattern (CSLBP) is textual descriptor used for hashing [4]. The CSLBP covers entire local region in only four pairs, that results in a 16 bin histogram. In addition to advantage of small size histogram, CSLBP captures structural changes in strength and gives rotational invariance. The proposed method used CSLBP in modified form based on position of neighbours. It covers entire local region and represent in only 8 bin histogram which gives out compact and quality image hash code. It generates two 4 bin histogram. Quantization loss on 16 bin histogram (CSLBP) is more than quantization on 4 bin histogram. Proposed method overcome loss of quantization problem by performing quantization of 4 bin histogram. CSLBP uses only sign information. Proposed method improves discrimination capability by incorporating local weight factor such as Standard Deviation (SD) and Laplacian of Gaussian (LoG) with sign information.

Backbone of an image hashing is quality features extraction. Identifying structural changes are important at global and local level. Due to local and global combination, methods are capable of detecting image forgery as well as locating counterfeit area of the image. In following approaches, global features and local features are extracted and used jointly. Local feature with saliency object detection using spectral residual model and global feature with DWT-SVD (Discrete-Wavelet Transform-Singular Value Decomposition) are combined [5]. Local feature by saliency detection and global feature by ring partition on projected gradient non-negative matrix factorization (PGNMF) [6]. Shape detection by zernike moment as a global feature and position and texture are detected by salient point detection as a local feature [7]. Zernike moment represents global feature and Haralick texture extracts 14 local statistics values represents local texture feature [8]. Global zernike moments combined with local MOD-LBP feature are combined [9]. Radon transformed image has both local and global features. Invariant moments from radon coefficients represents global feature and statistical measures such as zero-order moment, variance, singular value, DC component forms local features [10]. DCT (Discrete Cosine Transform) as a global feature and local feature extraction using least-squares line (LSL) fitting of Discrete Wavelet Transform (DWT) coefficients are combined [11]. DCT global feature and Gray Level Co-occurrence Matrix (GLCM) local feature are used in combination [12].

Frequency domain methods are quite popular in hashing as transformed coefficients are invariant to various geometric attacks. DCT is applied on Radon transformed image and various statistical features extracted from AC components to generate hash [13]. Fourier-Mellin Transform (FMT) is applied on an image to get translation invariance. Fourier Transforms is applied on log-polar coordinates of FMT transformed image to obtain rotation and scale invariance. Resultant coefficients are used to obtain hash [14]. Content-change coefficients are generated by applying first DWT followed by Radon transform [15]. Sign component of DCT coefficients carry information about textures and edges which utilized in hash formation [16]. SVD is applied on contourlet HMT transformed image to select most efficient components and followed by randomization to generate final hash [17].

Methods based on matrix factorization provide efficient way of separating most important information carrying components. NMF is applied twice on pseudo random sub images of original image. This method distinguishes between malicious and non-malicious attack but fail for local region forgery [18]. NMF is performed on luminance component of pseudo-randomly re-arranged input image. Hash is constructed based on the concept that adjacent entries in the NMFs coefficient matrix is basically invariant to content-preserving image operations [19].

Other approaches uses various spatial and statistical features. SIFT and Harris detector detects local stable robust feature points. These points are embedded into shape-contexts-based descriptors [20]. Local robust SIFT feature points of the original image and its attacked version are found. These points are matched using distance vector [21].

Texture extraction is a very popular way for an image hashing. Textural changes is an efficient way to discriminate between malicious and non-malicious activities. Various approaches are available for texture detection. Specifically Local Binary Pattern is a popular texture descriptor which extracts texture details at local level and binds them at semi global level through histogram. Problem associated with the LBP is that generated histogram for a local region of size 3×3 is of 256 bin [22]. There are many variants of the LBP's such as MBP, ILBP, RLBP, DLBP etc. which capture texture strength in different ways. The LBP's are also available for color images. Main drawback of the LBP and its variants are large number of the histogram bin, which eventually affects final size of descriptor. To achieve short hash length, CSLBP is a suitable option for hashing. Davarzani had constructed CSLBP histogram for four times. Each histogram is built with weight

factor. Four weight factors are generated from magnitude difference of four cross-symmetric pairs of CLSBP. Drawback with this method is that hash size is increased by 4 times. Also weight factor contributes very little in enhancing discrimination power [23].

In our previous approaches, we found that CSLBP can be made more robust for discrimination if local weight factor is utilized during the CSLBP histogram construction. Local weight factor captures local strength and it is bind in histogram. In our AQ-CSLBP, SDQ-CSLBP, CoCQ-CSLBP, LoGQ-CSLBP approaches, average of magnitude difference, standard deviation, correlation coefficient, Laplacian of Gaussian is used as a local weight factor respectively [24-27]. All our mentioned methods has compressed a 16 bin CSLBP histogram to a 8 bin histogram by the flipped difference concept [28]. Without a weight factor, discrimination power of the Q-CSLBP is less desirable.

The proposed method covers the local region of size 3×3 by using two histogram, each histogram having size of a 4 bin, one histogram covers two pairs (opposite) and other one will covers two pairs (cross diagonal). Therefore total bins of first and second histogram are 8 bin. Other advantage is that, uniform quantization with a 4 bin incurs small loss compared to uniform quantization on a 16 bin. The rest of this paper is organized as follows: Section 2 gives detail explanation of the proposed modified CSLBP hashing method. Section 3 discusses the experimental results and analysis. We depicts our conclusions in section 4.

2. PROPOSED METHOD

The proposed method is designed for gray scale images which are mainly characterized by texture and shape. The size of an input image is set to 256×256 using bilinear interpolation. This is done for the experimental purpose and comparative result analysis. In pre-processing step, an input image is altered by Gaussian filter. Gaussian filtered input image is robust for content-preserving manipulation as well as to reduce disturbance caused by manipulations like noise, lossy compression etc. For LoG weight factor, the gradient image is generated from an input image.

After pre-processing, the modified CSLBP is applied on an entire image. For the modified CSLBP calculation, the local region size is confined to 3×3. After modified CSLBP, each image pixel is represented by two values and are in the range from 0-3. First value is generated from the nearest neighbours and second one is from the diagonal neighbours. For a center pixel g_c, eight neighbours are there as shown in Figure 1(a). Neighbours are classified as the nearest and the diagonal neighbours as shown in Figure 1(b) and 1(c) respectively.

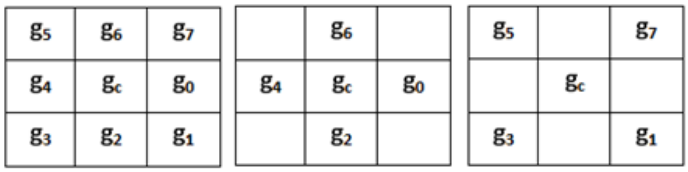


Figure 1. (a) Local region around g_c (b) Nearest neighbours (c) Diagonal neighbours

Following (1) and (2) represents the modified CSLBP for the nearest and the diagonal neighbours

$$MCSLBP-N(g_c)=s(g_0-g_4)2^1+s(g_2-g_6)2^2 \quad (1)$$

$$MCSLBP-D(g_c)=s(g_1-g_5)2^1+s(g_3-g_7)2^2 \quad (2)$$

$$s(g_p-g_{p+(P/4)})=\begin{cases}1 & (g_p-g_{p+(P/4)})>T\\ 0 & \text{otherwise}\end{cases} \quad (3)$$

where T is non-negative value to extract texture for an uneven surface; g_c is center pixel; g_p is neighbours of center pixel; P is no. of neighbours for centre pixel; $g_{p+(P/4)}$ is sign function of MCSLBP; MCLBP-N and MCLBP-D are Modified CSLBP for nearest and diagonal neighbours respectively.

The pixel value varies from 0 to 3 for each neighbour in the modified CSLBP. In the modified CSLBP, like CSLBP all four cross-symmetric pairs are covered. But unlike the CSLBP, all pairs are not combined in one histogram of 16 bin. Instead, the two different histograms are generated, each of four bin by separating neighbours. The generated histogram of modified CSLBP is of 8 bin which shows 50% saving of hash code. Two weight factors, Standard deviation (SD) and Laplacian of Gaussian (LoG) are used for the nearest and the diagonal neighbours. SD weight factor is calculated from an original image while LoG weight factor is derived the Gradient image.

Standard deviation is one of the powerful texture descriptor. It represents average distance from the mean of the data set to a center point. Standard deviation is calculated for both the neighbours by following (4) and (5) respectively. For center pixel g_c, absolute difference of four cross-symmetric pairs are taken as (g_0-g_4), (g_1-g_5), (g_2-g_6) and (g_3-g_7). The nearest neighbour pairs are (g_0-g_4), (g_2-g_6) and the diagonal neighbour pairs are (g_1-g_5), (g_3-g_7).

$$SD_N = \sqrt{\frac{\sum_{i=0}^{1}\left(gN - \overline{gN}\right)^2}{2}} \tag{4}$$

$$\overline{gN} = ((g_0 - g_4) + (g_2 - g_6))/2 \tag{5}$$

$$gN = \{(g_0 - g_4), (g_2 - g_6)\} \tag{6}$$

$$SD_D = \sqrt{\frac{\sum_{i=0}^{1}\left(gD - \overline{gD}\right)^2}{2}} \tag{7}$$

$$\overline{gD} = ((g_1 - g_5) + (g_3 - g_7))/2 \tag{8}$$

$$gD = \{(g_1 - g_5), (g_3 - g_7)\} \tag{9}$$

where SD_N and SD_D is Standard Deviation weight factor of nearest and diagonal neighbours respectively; g_i is the set of observations of particular neighbours; g bar is the mean of observations of particular neighbours

The Laplacian of an image highlights regions of rapid intensity change and is therefore often used for edge detection. If Laplacian filter is applied directly on a noisy image, the result is an edge image with many small edges which are not more useful. The Laplacian is often applied to an image that has been smoothed first with a Gaussian smoothing filter in order to reduce its sensitivity to noise. The LoG response will be zero for areas where the image has a constant intensity. However, in the vicinity of a intensity change, the LoG response will be positive on the darker side, and negative on the lighter side. This indicates reasonably sharp edge between two regions of uniform but different intensities. The Laplacian of Gaussian filter detects the horizontal and vertical boundaries as well as the boundaries other than the horizontal and vertical ones. The 2D Laplacian of Gaussian (LoG) function centered on zero and with Gaussian standard deviation sigma(σ) has the form.

$$LoG\ (x,y) = -\frac{1}{\pi\sigma^4}\left[1 - \frac{x^2+y^2}{2\sigma^2}\right]e^{-\frac{x^2+y^2}{2\sigma^2}} \tag{10}$$

where σ is standard deviation; x and y are spatial coordinates of an image.

The amount of smoothing can be controlled by varying the value of the standard deviation. In the proposed method, LoG of the input image is calculated to generate the gradient image. Weight factor is determined by taking average of LoG gradient information of the nearest and the diagonal neighbours respectively. For example for pixel G_c with 8 gradient neighbours from G_0 to G_7.

$$LoG_N = \frac{1}{4}(LoG(G_0) + LoG(G_2) + LoG(G_4) + LoG(G_6)) \tag{11}$$

$$LoG_D = \frac{1}{4}(LoG(G_1) + LoG(G_3) + LoG(G_5) + LoG(G_7)) \quad (12)$$

where LoG_N and LoG_D are LoG weight factor of the nearest and the diagonal neighbours respectively. Final weight for the nearest and the diagonal neighbours are given by (9) and (10).

$$W_N = SD_N + LoG_N \quad (13)$$

$$W_D = SD_D + LoG_D \quad (14)$$

where W_N and W_D are weight factor of the nearest and the diagonal neighbours respectively.

After calculation of the modified CSLBP, histogram is constructed at sub-block level. For every sub-block, two histogram are generated, each of a 4 bin. While constructing the modified CSLBP histogram, particular histogram bin is not incremented by one like CSLBP histogram. However, bin is incremented by weight factor. Equation of the modified CSLBP histogram for the nearest and the diagonal neighbours are given as below.

$$H_{MCSLBP-N} = \sum_{i=1}^{B} \sum_{j=1}^{B} W_N(i,j) \times f(MCSLBP - N(i,j), b) \quad (15)$$

$$H_{MCSLBP-D} = \sum_{i=1}^{B} \sum_{j=1}^{B} W_D(i,j) \times f(MCSLBP - D(i,j), b) \quad (16)$$

f is bin increment function; $H_{MCSLBP-N}$ and $H_{MCSLBP-D}$ represents histogram for nearest and diagonal neighbours respectively; B is size of sub-block; b ϵ [0; 3].

If the image is manipulated maliciously, then weight factor of an original image and its modified version will not be the same. This difference captures perceptual characteristics of hashing. For content-preserving operations, image hash of an original and content-preserving modified image is different, still difference of hash codes remains within the prescribed limits of the set threshold. If the modified CSLBP histogram is constructed without weight factor then discrimination power which contributes in success rate is low. Histogram constructed with weight factor captures perceptualness at local level and identifies change area of an image.

Uniform quantization is applied separately on each histogram to generate a binary hash. In uniform quantization, the step size between adjacent quantized levels is fixed. All the sub-blocks are processed in this manner and quantized hash code of all sub blocks are concatenated to generate the final hash of the image. On the receiver side, binary hash can be efficiently compared with hamming distance. If hamming distance is less than the set threshold, then it is content-preserving manipulation, otherwise it is treated as content-change manipulation.

3. EXPERIMENTAL RESULTS AND ANALYSIS

In image hashing authentication, robustness to content-preserving and sensitivity to content-change are important properties to be evaluated. These two properties are evaluated using two benchmarks. One is Normalized hamming distance (NHD) and other is Receiver Operating Characteristics (ROC) are used. Above mentioned benchmarks are suitable for binary classification that is either authentic or non-authentic. NHD measures how much change happen for both content-preserving and content-change operations. ROC basically checks discrimination capability of hashing methods.

3.1. Experimental setup

From original database, two database are created namely malicious and non-malicious. For analysis purpose, the total 36 images are taken from Matlab directory and the internet. To compare performance with other methods, all images are set to uniform standard size 256×256. For every image, total 61 attacks are applied as specified in Table 1. Some of the attacks are content-preserving while others are content-change. Last column of Table 1 specifics acronyms for various attacks. Table 2 specifies various comparative methods with their acronyms.

Table 1. Various attacks, parameter, and their acryonym

Operations	Descriptions	Parameters	Acryonym
Cropping	Ratio	1%, 3%, 5%, 7%, 9%	A
Salt & Pepper Noise	Noise Density	0.01, 0.02, 0.03, 0.05, 0.1	B
Gaussian Noise	Noise Variance	0.001, 0.005, 0.01, 0.02, 0.05	C
Scaling	Scaling factor	0.7, 0.8, 0.9, 1.1, 1.2, 0.01, 0.05, 0.10, 0.15, 0.20	D
Rotate	Rotation Angle	2^0, 4^0, 6^0, 8^0, 10^0	E
JPEG Compression	Quality Factor	10, 30, 50, 70, 90	F
Gamma Correction	Gamma value	0.75, 0.8, 0.9, 1.1, 1.25, 4.25, 4.50, 4.75, 5.00, 5.25	G
Increase Brightness	Range of adjustment	[0.8 1],[0.6 1],[0.4 1],[0.2 1]	H
Decrease Brightness	Range of adjustment	[0 0.6],[0 0.4],[0 0.2],[0 0.1]	I
Increase Contrast	Range of adjustment	[0 0.8], [0 0.6], [0 0.4], [0 0.2]	J
Decrease Contrast	Range of adjustment	[0.8 1], [0.6 1], [0.4 1], [0.2 1]	K

Table 2. Hashing methods with their acryonym

Hashing Method	Acryonym	Weight Factor
CSLBP	I	Only Sign
CSLBP Sep. Mag.	II	Separate Magnitude
QC-SLBP	III	Only Sign
AQ-CSLBP	IV	Magnitude Average
SDQ-CSLBP	V	Standard Deviation
CoCQ-CSLBP	VI	Correlation Coefficient
LoGQ-CSLBP	VII	Laplacian of Gaussian
Proposed Modified CSLBP	VIII	Standard Deviation + Laplacian of Gaussian

Following paragraph describes various parameter used in the modified CSLBP calculation. Input image is divided into non overlapping sub-blocks of size 3×3 i.e. R = 1 and P = 8 which represent neighbour around center pixel. T is non-negative threshold for texture extraction and it is set to 0.1. The gradient image (G) is generated by applying LoG operator on input image. For LoG operator, σ is 0.9. For the histogram generation, sub-block size is set to 32×32. This sub-block size gives good balance between hash size and discrimination capability.

3.2. Perceptual robustness test

Perceptual robustness measure indicates content preserving. It ensures that original image and its attacked version are visually similar. It categorizes such type of modification as non-malicious operations and attacked version is accepted as authentic image. To check for visual similarity, normalized hamming distance is used. Hamming distance is simple ex-or operation. Two hashes, one from original image and other from its attacked version is ex-ored to get hamming distance. Hamming distance is normalized for analysis simplicity. The threshold T_{NHD} is set for Normalized Hamming Distance (NHD). For authentic image, NHD between original image and its attacked version is less than T_{NHD} and for non-authentic images it is greater than the set threshold. T_{NHD} for every method is different. For modified CLSBP, T_{NHD} is 0.14 as shown in Figure 3.

Table 3. NHD for modified CSLBP image hashing

Attack	Modified CSLBP Image Hashing T_{NHD}=0.14	
	Auth	Non Auth
Cropping	0.07	0.16
Salt & Pepper Noise	0.06	0.16
Gaussian Noise	0.13	0.23
Scaling	0.03	0.24
Rotate	0.11	0.18
JPEG Compression	0.03	0.09
Gamma Correction	0.02	0.19
Increase Brightness	0.06	0.19
Decrease Brightness	0.04	0.31
Increase Contrast	0.05	0.23
Decrease Contrast	0.05	0.25

Observations: T_{NHD} is set to 0.14. This method almost clearly distinguishes between authentic and non-authentic images except JPEG non-authentic images. Difference between minimum NHD and maximum NHD is also large. Minimum is 0.03 and maximum is 0.31.

3.2.1. NHD results with comparative methods

The proposed method is compared with other existing methods from Method I to VII as mentioned in Table 4. Results clearly shows that Method I and Method III satisfies perceptual robustness. Method I is implemented CSLBP texture operator and generates 16 bin histogram. Method III is same as method I only histogram is compressed from 16 bin to 8 bin using the flipped difference concept. Method II is implemented by author Davarzani has poor perceptual property as it fails to distinguished between content-change and content-preserving. This method used weight factor as magnitude of difference of cross-symmetric pairs of CSLBP. For each pair, they generate separate histogram of 16 bin. This results in 64 bin histogram and subsequently increase resultant hash size. Method IV to VII represents our previous approaches in which we achieved perceptual robustness as well as discrimination capability. For Method IV to VII, all are generated 8 bin histogram using the flipped difference concept. However flipped difference concept compresses histogram but its overall discrimination power is low. To enhance this discrimination power, various weight factors are utilized during CSLBP construction. In our proposed approach, CSLBP equations are arranged according to neighbours which gives out 50% reduction in histogram bins without compromise on quality and without compression.

Table 4. NHD for method comparative methods

Attack	Method I		Method II		Method III		Method IV		Method V		Method VI		Method VII	
	A	NA	A	NA	A	NA	A	NA	A	NA	A	NA	A	NA
A	0.04	0.10	0.01	0.01	0.05	0.13	0.04	0.11	0.05	0.13	0.05	0.13	0.06	0.14
B	0.03	0.11	0.01	0.01	0.04	0.10	0.06	0.12	0.07	0.15	0.04	0.10	0.05	0.11
C	0.14	0.22	0.01	0.02	0.12	0.19	0.09	0.14	0.11	0.19	0.13	0.17	0.12	0.19
D	0.02	0.14	0.00	0.02	0.02	0.17	0.02	0.17	0.02	0.19	0.02	0.19	0.03	0.19
E	0.05	0.10	0.01	0.01	0.07	0.13	0.07	0.13	0.09	0.15	0.07	0.13	0.08	0.15
F	0.03	0.09	0.00	0.01	0.03	0.10	0.02	0.07	0.02	0.08	0.04	0.13	0.04	0.09
G	0.01	0.12	0.00	0.01	0.01	0.13	0.01	0.14	0.01	0.16	0.02	0.16	0.01	0.12
H	0.04	0.12	0.00	0.01	0.05	0.14	0.05	0.15	0.05	0.17	0.06	0.17	0.04	0.11
I	0.03	0.18	0.00	0.02	0.03	0.21	0.03	0.27	0.03	0.30	0.04	0.26	0.03	0.18
J	0.05	0.17	0.01	0.02	0.06	0.20	0.04	0.18	0.04	0.20	0.08	0.26	0.04	0.15

A represents Authentic NHD and NA represents Non-Authentic NHD

3.3. Discrimination test

Receiver Operator Characteristic (ROC) curve is used to display the performance of a binary classification algorithms at various threshold settings. TPR and FPR indicate robustness and discrimination, respectively. The area under the ROC curve is a measure of how well a parameter can distinguish between two diagnostic groups (authentic/non-authentic). Accuracy is measured by the area under the ROC curve. Table 5 shows TPR and FPR for the proposed method.

Table 5. TPR and FPR for modified CSLBP image hashing

Attack	Modified CSLBP Image Hashing	
	TPR	FPR
Cropping	0.90	0.06
Salt & Pepper Noise	0.90	0.25
Gaussian Noise	0.47	0.07
Scaling	1.00	0.07
Rotate	0.44	0.05
JPEG Compression	0.99	0.67
Gamma Correction	1.00	0.08
Increase Brightness	0.85	0.03
Decrease Brightness	1.00	0.01
Increase Contrast	0.88	0.10
Decrease Contrast	0.94	0.19
Avg. Database	0.89	0.11

Observations: For compressed image hashing, success rate is 89%. For almost all attacks, proposed method 'Modified CSLBP' shows better discrimination capability. The proposed method 'Modified CSLBP' shows average discrimination capability only for JPEG attack as JPEG non-authentic images have smooth visual appearance.

For an average database, TPR is 0.89. If weight factor is not utilized, then TPR is close to 0.82, which shows that with the help of local weight factor, the discrimination power of hashing algorithm can be

enhanced. ROC results for methods I to VIII are represented in Figure 4 to Figure 15. From Figure 2 to Figure 12, it shows that the proposed modified CSLBP is quite robust for almost all types of attack with good discrimination capability. Only for decrease contrast and JPEG quality factors, performance is average. Performance is improved for Gaussian noise and rotation attack than existing and our previous proposed image hashing methods.

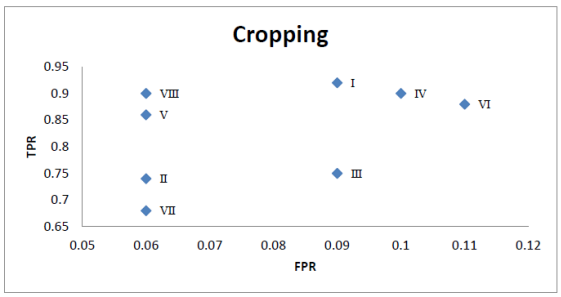


Figure 2. ROC: Cropping

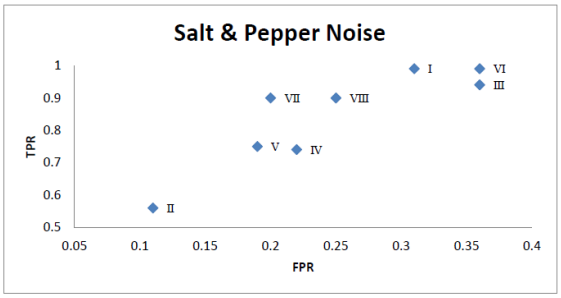


Figure 3. ROC: Salt & pepper noise

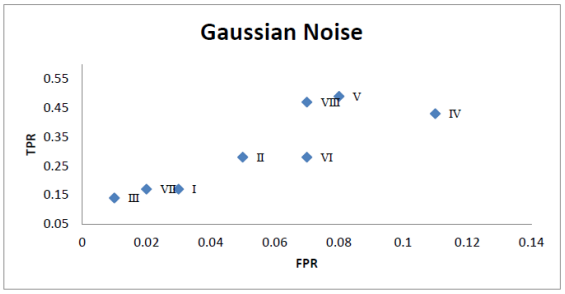


Figure 4. ROC: Gaussian noise

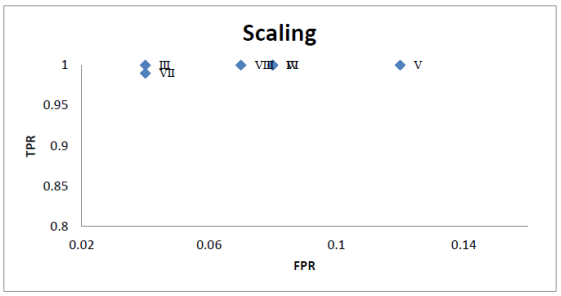


Figure 5. ROC: Scaling

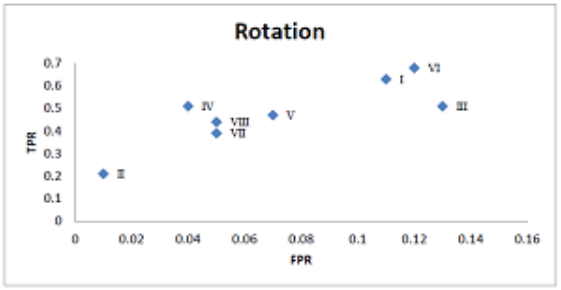


Figure 6. ROC: Rotation

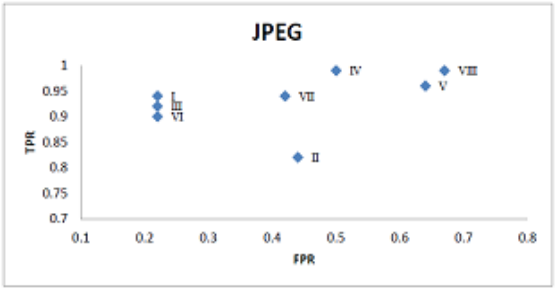


Figure 7. ROC: JPEG

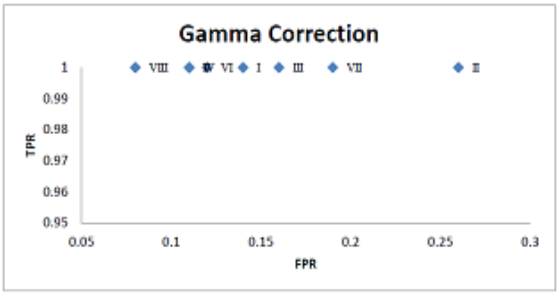


Figure 8. ROC: Gamma correction

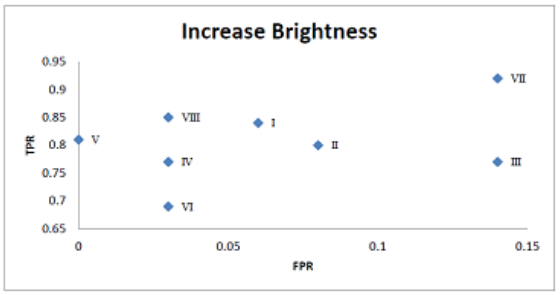
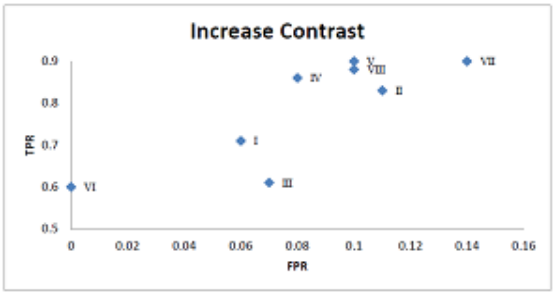


Figure 9. ROC: Increase brightness



Figuure 10. ROC: Decrease brightness

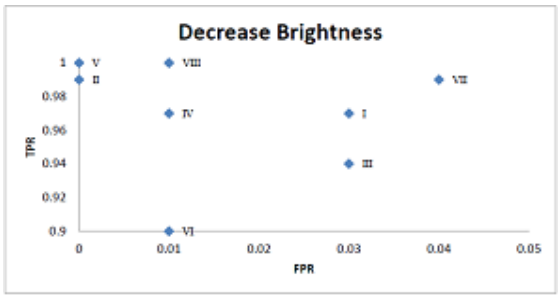


Figure 11. ROC: Increase contrast

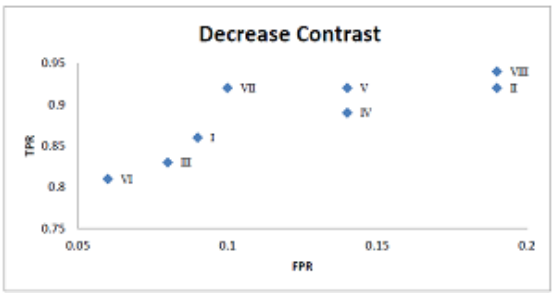


Figure 12. ROC: Decrease contrast

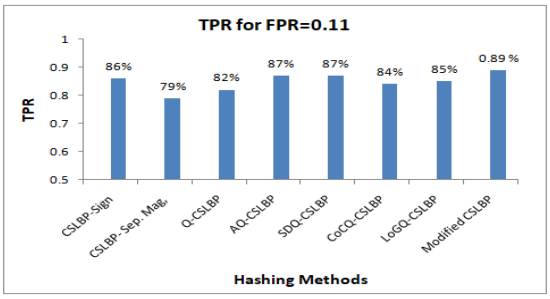


Figure 13. TPR for existing and proposed methods

4. CONCLUSION

We have proposed the modified CSLBP image hashing method with weight factor. Original CSLBP is modified depending on neighbours location. Modified CSLBP generates two 4 bin histogram for a sub-block. With Modified CSLBP, resultant hash code is 50% compact than original CSLBP. Quantization loss is decreased when it is applied on 4 bin histogram. Discrimination power is enhanced by using local weight factor namely, standard deviation and LoG. Desirable characteristics of hashing like compact length, quality features and desirable discrimination power are achieved by the proposed method. Proposed method is robust to variety types of attacks as results are proved by NHD and ROC curve.

REFERENCES

[1] V. Mall, et al., "Exposing structural tampering in digital images," *Signal Processing, Computing and Control (ISPCC), 2012. ISPCC 2012. IEEE*, pp. 1-6, 2012.
[2] K. B. Adedeji and A. A. Ponnle, "Improved image encryption for real-time application over wireless communication networks using hybrid cryptography technique," *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol/issue: 4(4), pp. 307-318, 2016.
[3] V. A. Kumar, et al., "A hybrid digital watermarking approach using wavelets and LSB," *International Journal of Electrical and Computer Engineering (IJECE)*, vol/issue: 7(5), pp. 2483-2495, 2017.
[4] J. Xiao and G. Wu, "A robust and compact descriptor based on center-symmetric LBP," *Image and Graphics, 2011, ICIG 2011, Sixth International Conference IEEE*, pp. 388-393, 2011.
[5] R. K. Karsh, et al., "Robust image hashing through DWT-SVD and spectral residual method," *EURASIP Journal on Image and Video Processing*, vol. 2017, pp. 31, 2017.
[6] R. K. Karsh, et al., "Robust image hashing using ring partition-PGNMF and local features," *SpringerPlus Journal*, vol. 5, pp. 1995, 2016.
[7] Y. Zhao, et al., "Robust hashing for image authentication using Zernike moments and local features," *IEEE Transactions on Information Forensics and Security*, vol. 8, pp. 55-63, 2013.
[8] G. Soman, et al., "Block-Based Forgery Detection Using Global and Local Features," *Soft Computing Systems, 2016. Springer 2016. International Conference Springer*, pp. 147-155, 2016.
[9] L. S. Sebastian, et al., "Image authentication by content preserving robust image hashing using local and global features," *Elsevier Journal on Procedia Computer Science*, vol. 46, pp. 1554-1560, 2015.
[10] L. I. U. Yuling, et al., "Robust image hashing using radon transform and invariant features," *Radioengineering*, vol. 25, 2016.

[11] Y. Q. Lei, et al., "DCT-domain global feature and DWT-domain least-squares line fitting based local feature for robust image hashing," *International Journal of Innovative Computing, Information and Control*, vol/issue: 6(6), pp. 450-464, 2010.
[12] A. Neelima and K. M. Singh, "A robust image hash function based on color and texture features of the image," *Advanced Computing and Communication, 2015, ISACC 2015, International Symposium IEEE*, pp. 238-243, 2015.
[13] M. Srivastava, et al., "Robust image hashing based on statistical features for copy detection," *Electrical, Computer and Electronics Engineering, 2016. UPCON 2016. International Conference IEEE*, pp. 490-495, 2016.
[14] S. Prungsinchai, et al., "Fourier-Mellin transform for robust image hashing," *Emerging Security Technologies, 2013. EST 2013. Fourth International Conference IEEE*, pp. 58-61, 2013.
[15] X. C. Guo, et al., "Content based image hashing via wavelet and radon transform," *Proceedings of Springer Pacific-Rim Conference on Multimedia, 2007. Springer*, pp. 755-764, 2007.
[16] S. Prungsinchai, et al., "A DCT sign-based robust image hashing," *Proceedings of IEEE Eights International Conference on Internet Technology and Secured Transactions, 2013. ICITST IEEE*, pp. 401-405, 2013.
[17] R. Sun, et al., "Perceptual image hashing method using contourlet hmt model," *Multimedia Information Networking and Security, 2011. MINES 2011. Third International Conference IEEE*, pp. 292-296, 2011.
[18] V. Monga, et al., "Robust and secure image hashing via non-negative matrix factorizations," *IEEE Transactions on Information Forensics and Security*, vol/issue: 2(3), pp. 376-390, 2007.
[19] Z. Tang, et al., "Robust image hashing for tamper detection using non-negative matrix factorization," *Journal of Ubiquitous Convergence Technology*, vol/issue: 2(1), pp. 18-26, 2008.
[20] X. Lu, et al., "Perceptual image hashing based on shape contexts and local feature points," *IEEE Transactions on Information Forensics and Security*, vol/issue: 7(3), pp. 1081-1093, 2012.
[21] C. P. Yan, et al., "Adaptive local feature based multi-scale image hashing for robust tampering detection," *Proceedings of 2015 Tenth IEEE Region Conference, 2015, TENCON IEEE*, pp. 238-243, 2015.
[22] T. Ojala, et al., "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE transactions on pattern analysis and machine intelligence*, vol. 24, 2002.
[23] R. Davarzani, et al., "Image authentication using LBP-based perceptual image hashing," *Journal of AI and Data Minings*, vol. 3, 2015.
[24] V. Patil and T. Sarode, "Image hashing using AQ-CSLBP with double bit quantization," *Optoelectronics and Image Processing, 2016. ICOIP 2016. International Conference IEEE*, pp. 30-34, 2016.
[25] V. Patil and T. Sarode, "Image hashing by SDQ-CSLBP," *Advances in Computing, Communications and Informatics, 2016. ICACCI 2016. International Conference IEEE*, pp. 2057-2063, 2016.
[26] V. Patil and T. Sarode, "Image hashing by CCQ-CSLBP," *Electrical and Computer Engineering, 2016. WIECON-ECE 2016. International Conference IEEE*, pp. 73-78, 2016.
[27] V. Patil and T. Sarode, "Image hashing by LoG-QCSLBP," *Communication and Information Processing, 2016. Second International Conference ACM*, pp. 124-128, 2016.
[28] J. Baber, et al., "Q-CSLBP: compression of CSLBP descriptor," *Multimedia and Information Processing, 2012. Pacific-Rim conference Springer*, pp. 513-521, 2012.

BIOGRAPHIES OF AUTHORS

Varsha Patil has received M.E. (Computer Engineering) degree from Mumbai University in 2007, pursuing Ph.D. from Mumbai University, INDIA. She has more than 12 years of experience in teaching. Currently working as Assistant Professor in Computer Engineering Department at South Indian Graduate School of Technology, Mumbai. She is Life member (ISTE). Her areas of interest are Image Processing, Signal Processing and Data Mining, Machine Learning.

Dr. Tanuja K. Sarode has received M.E. (Computer Engineering) degree from Mumbai University in 2004, Ph.D. from Mukesh Patel School of Technology, Management and Engg. SVKMs NMIMS University, Vile-Parle (W), Mumbai, INDIA in 2010. She has more than 17 years of experience in teaching. Currently working as Professor and Head in Dept. of Computer Engineering at Thadomal Shahani Engineering College, Mumbai. She is Life member (ISTE) and (IETE). Her areas of interest are Image Processing, Signal Processing and Computer Graphics. She has 170 papers in International Conferences/journal to her credit.