Image Hashing based on Shape Context and Speeded Up Robust Features (SURF)

Madhumita Paul
Department of ECE
NIT Silchar
Assam, India
mita@ece.nits.ac.in

Ram Kumar Karsh
Department of ECE
NIT Silchar
Assam, India
ram@ece.nits.ac.in

Fazal Ahmed Talukdar
Department of ECE
NIT Silchar
Assam, India
fazal@ece.nits.ac.in

***Abstract*—Image Authentication is one of the key issue in today's age of multimedia technology. With the availability of many hacking techniques and picture editing tools like Photoshop, image security is a major research field. Local feature points are elaborately used in resolving many problems, i.e., object detection, robust matching etc., but its use in the field of image hashing is not explored. In this work, we propose image hashing based on shape-context via Speeded Up Robust Features (SURF). The work is motivated by SIFT-based approach. Our contributions are: 1) SURF based algorithm is several times faster than SIFT-based algorithm. 2) It is more robust against different type of image modifications than SIFT. 3) We have incorporated rotation invariance property. Rotation is a difficult content preserving operation to model. The experiments are carried out on 1000 images and have shown that the proposed image hashing technique is robust against content-preserving operations. The region of convergence shows the efficacy of the proposed method compared to many state-of-the-art methods.**

Keywords-Image hashing; SURF; image authentication; tampering detection; image security

I. INTRODUCTION

Image hashing is a process of generating a fixed short array from an arbitrary size image. Image hashing has been widely applied for different purpose such as digital watermarking [1], retrieval of images [2], image quality assessment [3], image authentication [4-7] etc. Image hash needs to fulfill the following two requirements: robust against digital operations and good discrimination. Perceptual robustness signifies that the hash must be very similar for the two visually identical images having different digital representations. In other words, we can say that if the image is undergone with any content-preserving operations like varying the brightness or contrast level, image compression, scaling, incorporating the image with salt and pepper noise etc. Discriminative capability means for the different images hashes should be sufficiently different. In other words, for two different images hash distances must be large enough. Additionally, image hash should be sensitive to the changes in visual content when it is applied to the image authentication [8]. The state-of-the-art methods [9-12] are robust to some of the digital operations but sensitive for an arbitrary rotation.

Our contributions are as follows:

a) Existing methods are not having satisfactory performance for the rotation of an image, therefore we have proposed SURF based rotation invariant method to enhance the performance of the previous methods.

b) The central orientation of the original image has been evaluated using the Radon Transform technique and has been used as one of the parameters along with the hash to make the system more robust against rotation.

II. PROPOSED METHOD

The proposed image hashing algorithm is a three-phase procedure. The input image is first pre-processed, and then the SURF features have been calculated from processed image, i.e. point of interest and their descriptors. Finally, the hash is generated using these points of interest and their descriptors.

A. Pre-processing

An arbitrary size image is first mapped to M × M image via bi-linear interpolation, so that the size of the hash remains constant with respect to the changes made in the size of images. Then, the Gaussian low pass filtering is done to mitigate the influence of noise.

B. Interest Point Detection

Interest points, key points or feature points are constantly used in the field of object recognition and their performance is excellent. So, here these interest points will be used for Image authentication. The idea is that, instead of considering the whole image, we will consider few interest points or key points for our analysis. SURF key points are more accurate as well as they are computed in very less time.

C. Interest Point Feature Descriptors

Generally, Feature descriptor describes the pixel of an image according to its local content. Feature descriptors are robust for small errors due to deformations or localizations. To find out the Feature descriptors firstly, we have convolved the neighborhood pixel with the vertical and horizontal Haar wavelet filters as Shown in Fig. 1. These yields directional directives from the intensity of an image.

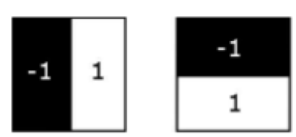


Fig. 1. Haar wavelet filters in the vertical and horizontal ways

For each equally split region, we compute the responses of Haar wavelet at 5×5 equally spaced points. Let d_x be the response in case of horizontal direction and d_y, for the vertical one. Now, the two responses are weighted with a Gaussian, centred at the point of interest. It enhances the robustness against localization error and geometric distortions.

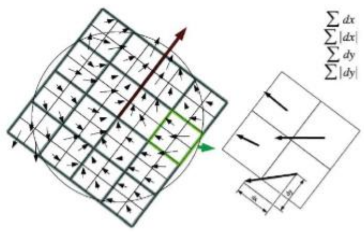


Fig. 2. The demonstration of descriptor building.

Then, the Haar wavelet responses are summed for each region yields feature vectors. In addition, absolute values of the responses (i.e., $|d_x|$ and $|d_y|$) are also used in feature set to reflect changes in intensity. Therefore, four-dimensional features is used for each regions (i.e., $v = \sum d_x, \sum d_y, \sum|d_x|, \sum|d_y|$ as shown in Fig. 2). Finally, 4×4 subregions provide a descriptor of length 64.

D. Image Hashing

An image hash has been generated using Shape context based upon the SURF features which we have previously detected. Shape context is an auspicious method in case of object recognition. The idea of generating the hash using shape context arises because the distribution of local feature points comprises the whole content structure of an image. In the following, firstly the shape context has been introduced and then the propose hashing algorithm.

E. Shape Contexts

First, we sample our points of interest from the shape context, contour of an object extracted from every point q_i by comparing to q_c is defined by S. Belongie et. al. [13] as in (1)

$$h_i(k) = \#\{q_i \neq q_c : (q_i - q_c) \in bin(k)\} \tag{1}$$

Here, $q_i \in Q$ *and* $bin(k)'s$ are undeviating in log-polar coordinates and the centre is located at q_c . So, shape context for each point signifies their respective positions by comparing a reference point. It is also detected that the descriptors of the key points or point of interests are robust toward shape deformation and yields a discriminative characterization.

F. Image hashing based upon Shape context

As we know that shape context provides an outstanding description of the object of interests in images. So, we can embed the local feature points generated using SURF and their descriptors to generate the Hash for an image. This hashing algorithm not only depended upon the content of the image but also consider the distribution of them. Upon considering the observation taken for an image authentication, in which if any visually insignificant attacks have been done over the image then it may not lead to the change in viewpoint and the centre of the image is remain preserved. So, by using this concept we can generate shape context via reference point taken at the centre yields a hash. Now, image hashing algorithm named as Angular Shape context hashing has been briefly discussed.

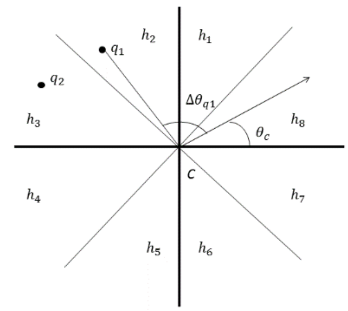


Fig. 3. Image hashing based on Radial-Shape Context

Let us consider a set of key points or points of interest as $Q = \{q_i(x, y)\}\ where\ \ 1 \leq i \leq N$ and their corresponding local descriptors are defined as $D = \{d_{p_i}(x, y)\}\ where\ \ 1 \leq i \leq N$. The steps for the generation of hash are as follows:-

1. Find out the central coordinate point $C = (x_c, y_c)$ and let L is hash length. Now construct the bins $B = \{b(k)\}\ where\ \ 1 \leq k \leq L$ of shape contexts with an increment of $a = 2\pi/L$ in a polar coordinates as depicts in Fig. 3.

$$b(k) = \{q_i \in Q : (k-1)a \leq (\theta_{q_i} - \theta_C) < ka\} \tag{2}$$

Here, $\theta_{q_i} - \theta_C = \Delta\theta_{q_i} \in [0, 2\pi]$ is orientation difference between the central point C and q_i.

2. Now, generate the pseudorandom weights by using a secret key from the normal distribution $N(u, \sigma^2)$as $\{\delta_k\}\ where\ 1 \leq k \leq L$. Each δ_k is a random vector which must be consistent with the dimension of SURF descriptor which is of 64 dimensions.

3. Now, $H = \{h_k\}\ where\ 1 \leq k \leq L$ be our hash vector and the component h_k is defined as follows given in (3):

$$h_k = \sum_{q_i \in b(k)} x\lceil \|q_i - C\|/\|C\| \rceil \langle \delta_k, d_{p_i} \rangle \tag{3}$$

G. Estimation of Central Orientation

The central orientation is estimated via the Radon transform (RT) [14]. RT is defined as an integral transform that consists an integral of a 2-D function f(x, y) over the straight lines p with the orientation of $\emptyset$ as depict in Fig. 4. Radon transform is evaluated as in (4)

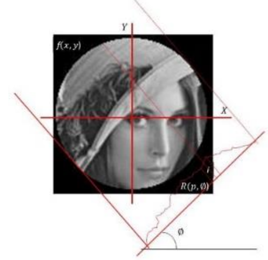


Fig. 4. Radon Transform $R(p, \emptyset)$ of *f(x,y).*

$$R_f(p,\emptyset) = \int_{-\infty}^{\infty} f(p\cos\emptyset - q\sin\emptyset\,, p\sin\emptyset + q\cos\emptyset)\,dq \quad (4)$$

where, $x = p\ cos\emptyset - q\ sin\emptyset$ & $y = psin\emptyset + qcos\emptyset$

The reference orientation is estimated using RT as follows:

1. Extract circular centre portion of radius 64 called as *f(x,y)*. Thereafter, find the RT of *f(x,y)* where $0 \leq \emptyset \leq 2\pi$.
2. Next, let us consider a reference point *i* on the *p* axis and sum with the neighborhood from [*i-t*, *i+t*] yields central orientation, as shown in Fig. 4

TABLE I CONTENT-PRESERVING OPERATIONS

Operations	Descriptions	Tool	Parameter Values	Number of images
Brightness adjustment	Photoshop's Scale	Photoshop	±10, ±20	4
Contrast Adjustment	Photoshop's Scale	Photoshop	±10, ±20	4
Gamma correction	γ	MATLAB	0.75,0.9,1.1,.25	4
Gaussian low pass filtering	Standard Deviation	MATLAB	0.3-1.0	8
Salt and Pepper Noise	Density	MATLAB	0.001-0.01	10
JPEG Compression	Quality factor	StirMark	30-100	8
Watermark Embedding	Strength	StirMark	10-100	10
Rotation	Angle in Degree	StirMark	±5, ±10, ±15,±30, ±45,±90	12
			Total :	60

As, we know that Rotation is the difficult digital operation to model, but the proposed algorithm is rotation invariant in a very simple manner by using the central orientation of the image, i.e. θ_C.

III. EXPERIMENTAL RESULTS

This section shows, various experiments are done over the images to check the efficiency of the proposed hashing approach.

A. Evaluation of Perceptual Robustness and discrimination

The value of threshold (i.e. the required Euclidean distance between hashes) for the verifications of images (i.e. whether perceptually similar to the original image, or forged, or different images) is calculated as follows: First, selected 800 different color images from the CASIA tampered database [16], and creates a database of 800x(800-1)/2=3,19,600 different image pairs. Also, opted 53 color images from USC-SIPI database [15], and creates a database of 53x60=3180 visually identical image pairs via different image editing tools presented in Table I. Then, calculates the hash distance (i.e. L2 norm) for 3,19,600 different image pairs and 3180 perceptually similar image pairs.

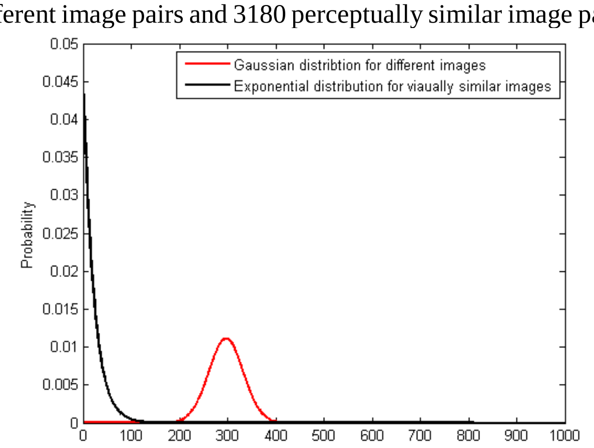


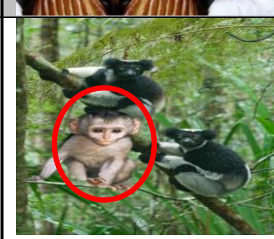
Fig. 5. Plot of Probability distribution functions

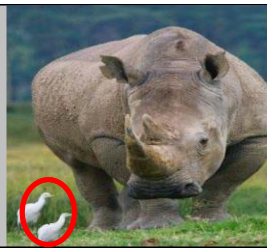
The hash distances distribution is shown in Fig. 5. The intersection point (i.e. 179) might consider as a threshold, but some different image pair might consider the similar image, that is why considered 120 a required threshold. Fig. 5 shows that the hash distances are below the threshold for perceptual similar images and larger in case of different image pairs. Hence, the proposed method provides better robustness as well as good discriminative capability.

B. Sensitivity towards forgery of images

The proposed system sensitivity against forgery in images has been discussed by CASIA 2.0 tampered image database [16]. The experiment via proposed method over 800 tampered image pairs has been performed. It has been observed that hash distances are greater than the chosen threshold. Hence, the proposed system is sensitive to image forgery. Some of tampered image pair samples from CASIA 2.0 tampered image database and hash distances are presented in Table II.

TABLE II SENSITIVITY TOWARDS FORGERY OF IMAGES

Original Image	*Forged Image*	*Hash Distance*
		185.38
		160. 69

		157.22

IV. Performance Comparison

ROC curve has been used to compare the proposed method with some existing techniques. ROC can be defined by using two probability functions: the probability of true detection $P_T(\partial)$ and the probability of false detection $P_F(\partial)$as in (5) and (6).

$$P_T(\partial) = P_r(Hash\ distance(H(A), H(A_M) < \partial) \quad (5)$$
$$P_F(\partial) = P_r(Hash\ distance(H(A), H(B_M) < \partial) \quad (6)$$

Here, ∂ is the threshold, images A are reference images, the images A_M are the digitally manipulated versions of these images A (i.e. A_M are perceptually similar to A), B_M are tampered version of A or a different one. It is expected that the hashes of A and A_M should be approximately the same, and the hashes of A and B_M should be different. So, for a good hashing technique $P_T(\partial)$ Should be higher with a lower value of $P_F(\partial)$.

The proposed hashing technique is compared with some state-of-the-art techniques (i.e. Ring partition and invariant vector distance based [17], Invariant moment based [18], SCH-SIFT based hashing [14], and RE based hashing [19]) shown in Table III. Table III shows that proposed image hashing is better than some state-of-the-art methods.

Based on $P_T(\partial)$ and $P_F(\partial)$, plotted the ROC curve of the proposed method and some existing techniques shown in Fig 6. Fig. 6 depicts that $P_T(\partial)$ of the proposed method is higher compared to the other method especially nearby zero $P_F(\partial)$

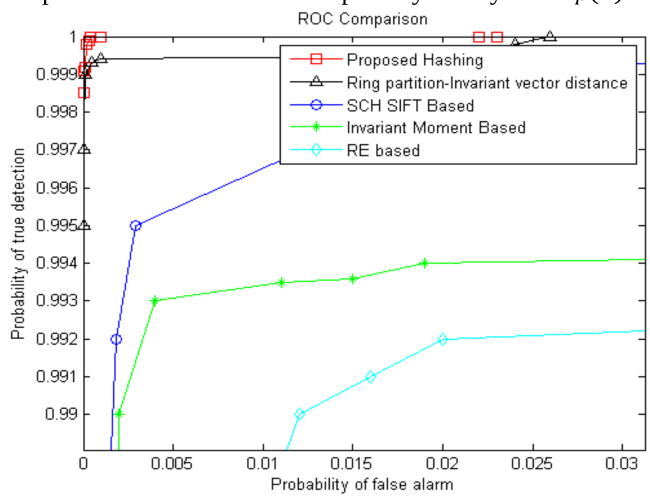


Fig. 6. ROC Curve for Comparison of Hashing Techniques.

TABLE III Comparison of proposed Hashing Technique with some State-of-the-Art Techniques.

	SCH-SIFT Based [14]	Invariant Moment Based [18]	RE based [19]	Ring partition and invariant Vector distance based [17]	Proposed method
Sensitive to changes in corner of images	No	Yes	No	No	Yes
Robust against arbitrary rotation	No	No	Yes	Yes	Yes
Length of hash	20 digit	42 digit	64 digit	40 digit	20 digit

V. Conclusion

In this paper, we have proposed the shape context-based hashing using SURF features points. The experimental results reveals the efficacy of the proposed image hashing technique such as better perceptual robustness against digital signal processing operations and good discriminative capability. ROC curve shows that the performance of the proposed image hashing approach is better than some of the existing techniques. The future work is exact localization of tampered regions.

REFERENCES

[1] S. Priya and R. Varatharajan. "Whirlpool Algorithm with Hash Function Based Watermarking Algorithm for the Secured Transmission of Digital Medical Images," Mobile Networks and Applications, pp. 1-14, 2018.

[2] X. Lu, X. Zheng, and X. Li, "Latent Semantic Minimal Hashing for Image Retrieval," IEEE Trans. Image Processing, vol. 26, pp. 355-368, Jan 2017.

[3] Z. Tang, H. Ziqing, Y. Heng, Z. Xianquan, L. Chen, and C. Yu, "Perceptual Image Hashing with Weighted DWT Features for Reduced-Reference Image Quality Assessment," The Computer Journal, vol. 61, pp. 1695-1709, May 2018.

[4] R. K. Karsh and R. H. Laskar, "Perceptual robust and secure image hashing using ring partition-PGNMF," in Proc. TENCON 2015-2015 IEEE Region 10 Conference, , pp. 1-6, Macau, China. Nov. 2015.

[5] A. Saikia, R. K. Karsh, and R. H. Laskar, "Image authentication under geometric attacks via concentric square partition based image hashing," in Proc. TENCON 2017-2017 IEEE Region 10 Conference, pp. 2214 - 2219, Penang, Malaysia, Nov. 2017.

[6] R. K. Karsh, R. H. Laskar, and B. B. Richhariya, "Robust image hashing using ring partition-PGNMF and local features," SpringerPlus, vol. 5, pp. 1995, Dec. 2016.

[7] R. K. Karsh and R. H. Laskar, "Robust image hashing through DWT-SVD and spectral residual method," EURASIP Journal on Image and Video Processing, vol. 2017, pp. 31, Dec. 2017.

[8] R. K. Karsh, A. Saikia, and R. H. Laskar, "Image Authentication Based on Robust Image Hashing with Geometric Correction," Multimedia Tools and Applications, vol. 77, pp 25409–25429, Oct. 2018.

[9] F. Ahmed, M. Y. Siyal, and V. U. Abbas, "A secure and robust hashbased scheme for image authentication," Signal Process., vol. 90, pp. 1456–1470, May 2010.

[10] Z. Tang, S. Wang, X. Zhang, W. Wei, and S. Su, "Robust image hashing for tamper detection using non-negative matrix factorization," J. Ubiquitous Converg. Technol., vol. 2, pp. 18–26, Aug. 2008.

[11] Z. Tang, S. Wang, X. Zhang, W. Wei, and Y. Zhao, "Lexicographical framework for image hashing with implementation based on DCT and NMF," Multimedia Tools Appl., vol. 52, pp. 325–345, Apr. 2011.

[12] Z. Tang, X. Zhang, and S. Zhang, "Robust perceptual image hashing based on ring partition and NMF," IEEE Trans. Knowl. Data Eng.,vol. 26, pp. 711–724, Mar. 2014.

[13] S. Belongie, J. Malik, and J. Puzicha, "Shape matching and object recognition using shape contexts. California univ san diego la jolla dept of computer science and engineering, Apr. 2002.

[14] X. Lv and Z. J. Wang, "Perceptual image hashing based on shape contexts and local feature points," IEEE Trans Inf Forensics Sec., vol. 7, pp. 1081–1093, Jun. 2012.

[15] USC-SIPI Image Database, [online] Available: http://sipi.usc.edu/database/, 2007

[16] CASIA Tampered image detection evaluation database [Online] Available: http://forensics.idealtest.org/

[17] Z. Tang, X. Zhang, X. Li, and S. Zhang, "Robust Image Hashing With Ring Partition and Invariant Vector Distance," IEEE transactions on information forensics and security, vol. 11, pp. 200-214 , Jan. 2016.

[18] Z. Tang, Y. Dai, and X. Zhang, "Perceptual hashing for color images using invariant moments," Appl. Math. Inf. Sci., vol. 6, pp. 643S–650S, Apr. 2012.

[19] Z. Tang, X. Zhang, L. Huang, and Y. Dai, "Robust image hashing using ring-based entropies," Signal Process., vol. 93, pp. 2061–2069, Jul. 2013.