Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 1554 – 1560

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

Image Authentication by Content Preserving Robust Image Hashing Using Local and Global Features

Lima S Sebastian[a,]*, Abraham Varghese[a], Manesh T[b]

[a]*Adi Shankara Institute of Engineering and Technology, Kalady,Ernakulam, 683574, India*
[b]*Computer Science and Information Department, Salman bin Abdulaziz University, P O Box.54,11991, Soudi Arabia*

Abstract

Image hashing technique constructs a short sequence from the image to represent its contents. This method proposes an image hash which is generated from Haralick and MOD-LBP features along with luminance and chrominance, which are computed from Zernike moments. Sender generates the hash from image features and attaches it with the image to be sent. The hash is analyzed at the receiver to examine the authenticity of the image. The method detects image forgery and locates the forged regions of the image. The proposed hash is robust to common content preserving modifications and sensitive to malicious manipulations.

© 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

*Keywords:*Image authentication; Image hash;Haralick features; MOD-LBP features; Zernike moments

1. Introduction

In recent years, digital images and videos have gained more popularity because of its use in social networks. Number of image editing software is also gained importance, which allows people to easily alter the content of digital multimedia. The technologies available on internet such as emails, social networks etc. are interested on the systems which ensure the authenticity of the multimedia information received in a communication. Image

* Corresponding author. Tel.: +91-999-504-9943.
E-mail address: limasramb@gmail.com

1877-0509 © 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).
Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.02.081

authentication is the technique by which one can ensure that the image has not been altered during the transmission and the image is from the legal user. Many methods have been proposed for image authentication, among which authentication by robust image hashing is the newest and widely used authentication technique. Image hashing is a technique which generates a short message or data from the image to represent image contents. Robust image hashing is slightly different from traditional cryptographic hashing techniques such as MD5 and SHA-1, which are really sensitive to very small changes in the image. There are applications that need to consider an image as non-authentic when one pixel or even one bit of data has been changed. Robust image hashing uses techniques which can tolerate content preserving modifications such as image format conversion, image enhancement, compression and quantization, etc., and is considered to be the desired authentication system for most practical cases.

At the sender side, the hash is extracted from input image and is encrypted before attaching it to the image as image header. The image which is attached with the image hash is sent to the destination. Receiver detaches the hash from the image, and generates the hash from the received image in same way as the sender did. Finally both the hashes are compared to ensure authenticity of the image and to locate the manipulated regions of the image.

M. Schneider[1], proposed first hashing technique, which develops image signature from intensity histogram of each block of the image. An image histogram is not very representative of image contents since image contents can be changed without making any change in the image histogram.

Venkatesan et al.[2] develop hash from quantized statistics of each sub-band coefficient of wavelet decomposed image. It is robust to geometrical transformations but sensitive to JPEG compression. Chang et al.[5] generate hash from weighted norm computed from weighting function together with description of weighting function. It is robust against low pass filtering, addition of white Gaussian noise and JPEG compression; but the process of feature extraction is not key dependent which reduces the security.

Ahmed et al.[6] propose a hash which is generated from LL sub-band coefficients of non-overlapping blocks of the image. This scheme uses a key dependent feature extraction. Roy et al.[7] propose a method in which hash generation technique consists of two steps; a feature extraction step followed by a bit extraction step. This technique also localizes the manipulated region of the image. V. Kitanovskiet al.[8] propose combined hashing/watermarking scheme for image authentication. Firstly the hash is generated from DC values and coded using a secret key, then watermark is obtained by bit-sensitive-like coding of the image hash. The method is robust to JPEG compression, but sensitive to spatial domain attacks. Insertion of watermark into the image distorts the contents of the image.

Tang et al.[9] propose a method that generates hash from feature-bearing coefficient matrix which is generated by applying NMF to the pixel arrays of the image. The hash is robust to additive noise, JPEG compression, image resizing, and watermark embedding, but this scheme does not consider color components to detect color related modifications. In another work, Ahmed et al.[10] use a wavelet based image hashing method, in which the hash is extracted from the sub-band wavelet coefficients from each non-overlapping block of the image. It is robust to most content preserving techniques, but if more robustness is required, the system threshold is needed to be increased which shall increase the probability of collision.

Zhao et al.[11] construct hash from Zernike moments of the inscribed circle of the pre-processed square image. The hash is robust to most of the content preserving modifications. Since the Zernike moments are calculated from inscribed circle, it leads to loss of information in the image corners, reducing the sensitivity of the hash to malicious manipulations. In another work Zhao[12] generates hash from amplitude of the Zernike moments and texture features of each non-overlapping block of the image. The hash generated is sensitive to filtering. In another work of Zhao et al.[13], Zernike moments and texture features are computed from salient regions of the image. The tampering detection is dependent on accuracy of saliency detection algorithm.

The remaining paper is organized as follows. Section 2 gives overview of the proposed hashing method. Section 3 presents the methodology in detail. Section 4 presents experimental results and studies the performance of the method. Section 5 concludes the paper.

2. Overview

The overview of proposed hashing technique is illustrated in Fig.1. The sender generates the hash from preprocessed image. Image preprocessing includes rescaling and conversion from RGB to YCbCr representation. Local features such as Haralick features[14] and MOD-LBP features[15] are extracted from non-overlapping blocks of resized image. Global features such as luminance and chrominance characteristics are extracted from Zernike

moments[16] of Y image and |Cb-Cr| image respectively. Both the local and global features are combined to form the final hash. The hash is attached with the image and sent to the destination. At the receiver, the hash is extracted from the received image. The receiver generates the hash from the image in the same way. Both the hashes are compared based on the hash distance. If the hash distance is greater than the predefined threshold, then the image is recognized as tampered image. If the image is identified as tampered then the tampered regions of the image are localized.

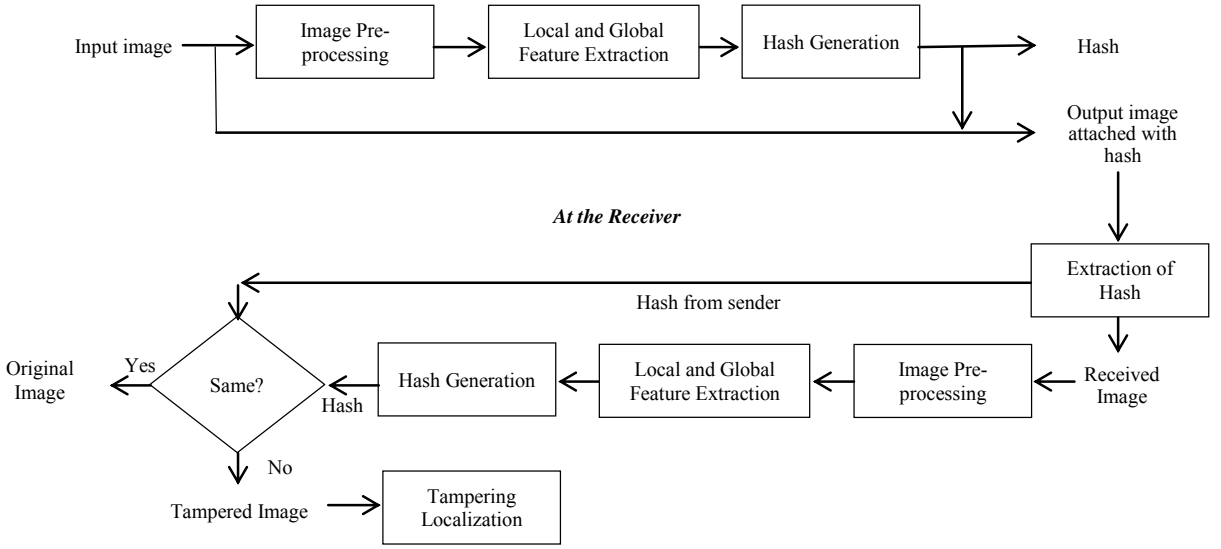


Fig. 1. Overview of the methodology

3. Methodology

In this section, we describe the proposed hashing method and the image authentication scheme. The hash is formed from two local features; MOD-LBP and Haralick features, and global features such as complex Zernike moments.

3.1. Image Hash Construction

Image hash construction includes following steps referring to Fig. 1.

- *Image Pre-processing*: Firstly, the input image is rescaled into a fixed size of K x K with bilinear interpolation, so that the generated image hash has a fixed length and same computational complexity. Large value of K leads to high computation complexity, while small value of K leads to loss of fine details. We select K=256. The image is converted from RGB to YCbCr representation to extract global features and from RGB to gray image to extract local features.
- *Local Feature Extraction:* The resized image is divided into non-overlapping blocks of size 32 x 32, and the local features are extracted from each of these blocks. There are 14 Haralick features mean of which is extracted from each block to generate hash. Mean of Histograms of MOD-LBP features from each image block is also used in hash generation. So we get Local features as L'= [H M] where H denotes Haralick features and M denotes MOD-LBP features. L' is a 1 x 128 sized vector. We randomly generate a vector Y_1 of size 1 x 128 with values in [0,255] using a secret key K_1. The encrypted Local feature vector L is obtained as $L = [(L'+Y_1) \bmod 256]$.
- *Global Feature Extraction*: The image is converted from RGB to YCbCr representation. Then complex Zernike moments from Y image and |Cb-Cr| image are computed which are luminance and chrominance characteristics of the image respectively. We choose order of the Zernike moment, n=5. We get $Z' = [Z_y Z_c]$ which is a row vector with 11x2=22 elements. We randomly generate a vector Y_2 of size 1 x 22 with values

in [0,255] using a secret key K_2.Then the encrypted global feature vector Z is obtained as $Z = [(Z'+Y_2) \bmod 256]$.

- *Final Hash Construction:* Intermediate hash is constructed by concatenating the hashes extracted from global and local image features, we get h' = [Z, L]. We randomly generate a vector Y_3 of size 1 x 150 with values with in [0,255] using a secret key K_3. Finally the hash is generated as $h = [(h'+Y_3) \bmod 256]$.

3.2. Image authentication and tampering localization

At the receiver, the hash is generated using the same methodology.The hash is called test hash, h_1. The hash from the sender is detached from the image and is called as reference hash, h_0. The reference hash is decrypted and decomposed to get intermediate hash $h_0' = [Z_0', H_0', M_0']$. At the receiver, we have $h_1' = [Z_1', H_1', M_1']$ which is compared with intermediate reference hash. We compute the differences between, Haralick and MOD-LBP features as $D_H = H_0'-H_1'$ and $D_M = M_0'-M_1'$ respectively, and calculate the total difference as $D_T = | D_H + D_M |$.

If the total difference has all the values below 1, the image is recognized as the original image. Otherwise the image blocks that have total difference greater than 1 are found as tampered blocks. Then the image is converted into Gray scale and all the pixels of the tampered blocks are made white pixels. This image is then converted into binary image, and then we find the rectangles having values 1. These rectangles are then marked in the received image as the tampered regions. The outputs of whole process are shown in Fig. 2.

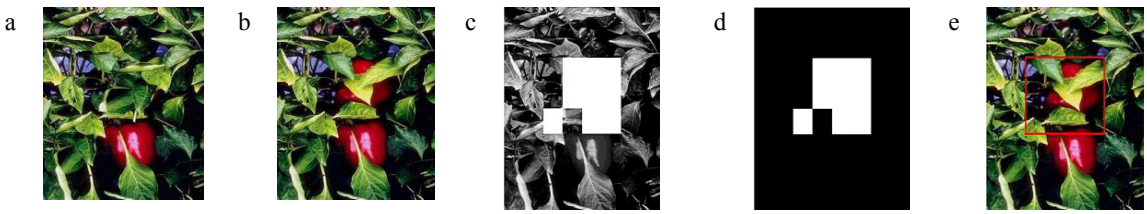


Fig. 2. (a) Sent image; (b) Received image; (c) Located blocks; (d) Binary map; (e) Localized tampered regions.

4. Results and Discussion

We have tested image pairs downloaded from internet and from dataset CASIA[4]. All the tampered images are detected and are correctly localized. The success rate of tampering detection is 100%. Robustness of the hash is checked against various content preserving modifications: JPEG coding, addition of noise, rotation, scaling, brightness and contrast adjustment, and slight cropping. Images with various contrast and brightness values are created using Photoshop, and JPEG compressed images, noise added images are created, and scaling and rotation are applied to images using MATLAB. Images are compressed at quality levels ranging from 1 to 99, Salt and Pepper noise is added with density levels ranging from 0.0001 to 0.9, and zero mean Gaussian noise is added with variance ranging from 0.0001 to 0.1. The proposed method tolerates JPEG compression above quality level of 15 which is an average value. Rotation tolerated by the proposed hash is up to 1% above which the texture features of the image changes, so that rotations above 1% can be considered as a malicious manipulation. The proposed hash can tolerate contrast adjustment and brightness adjustment up to 20 and 10 respectively.

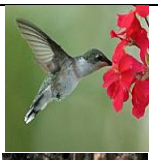
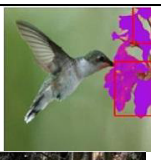
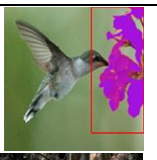
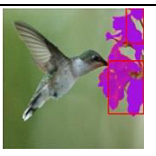
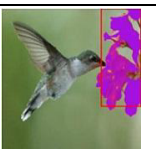
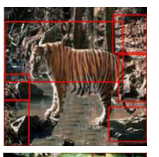
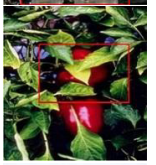
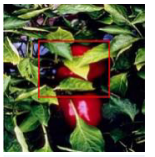
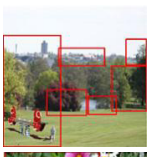
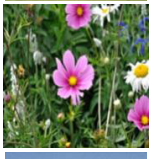
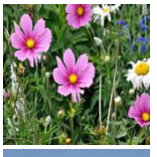
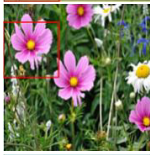
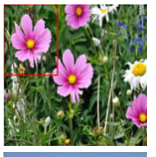
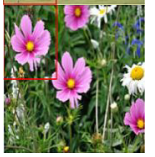
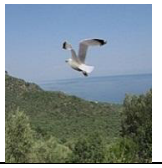
4.1. Forgery localization

Table 1 shows the tampering detection and tampering localization results of 4 hashing methods viz. method based on Haralick, MOD-LBP and Zernike moments, method based on Haralick and Zernike moments only, method based on MOD-LBP and Zernike moments only, and method proposed in "robust hashing for image authentication using Zernike moments and local features"[13], which are, for convenience, represented as follows.

Nomenclature

A	Method based on Haralick, MOD-LBP and Zernike moments (Proposed method).
B	Method based on Haralick and Zernike moments only.
C	Method based on MOD-LBP and Zernike moments only.
D	Method proposed in "Robust hashing for image authentication using Zernike moments and local features"[13]

Table 1. Tampering Localization.

Input image			Tampered Image	Tampering Localization			
Name	Size	Image		A	B	C	D
Img1.jpg	269 x 215						
Img2.jpg	384 x 256						
Img3.jpg	256 x 384						
Img4.jpg	512 x 384						
Img5.jpg	536 x 356						
Img6.jpg	2272 x 1704						

The table lists tampering localization of six '.jpg' images of different sizes. The methods A, B and C outperform the method proposed in D.

The proposed method A detects the forgery correctly and locates the forged regions accurately as compared to other three methods B, C, and D. The success rate of forgery localization of method A is obtained as 100%.

4.2. Robustness to JPEG compression

Table 2 illustrates the robustness of the hashes to JPEG Compression. The Robustness is checked for the hashes generated from A, B, C, and D. The images are compressed with quality levels ranging from 1 to 99. The values in

the table show the quality levels below which the image is identified as the manipulated one. From Table 2, it is clear that C outperforms other three methods, but combining methods of B and C, A shows better results.

Table 2. Robustness to JPEG compression

Images	A	B	C	D
Img1.jpg	22	90	20	58
Img2.jpg	19	70	14	51
Img3.jpg	13	74	12	83
Img4.jpg	15	68	14	74
Img5.jpg	10	92	8	85
Img6.jpg	9	28	7	88

4.3. Robustness to brightness/contrast adjustments

Table 3, gives the results showing robustness of the proposed method (A), to contrast/brightness adjustment which are also content preserving modifications. The table shows the values of contrast and brightness adjustments above which the image is recognized as forged image. It can be concluded from the table that, MOD-LBP features contribute to the proposed method to attain robustness to contrast and brightness adjustments.

Table 3. Robustness to contrast/brightness adjustments.

Images	Contrast adjustment				Brightness adjustment			
	A	B	C	D	A	B	C	D
Img1.jpg	24	2	24	3	18	1	18	2
Img2.jpg	12	2	12	1	6	2	6	1
Img3.jpg	20	3	20	1	6	1	6	1
Img4.jpg	22	2	22	8	12	1	12	3
Img5.jpg	18	1	18	4	8	2	8	1
Img6.jpg	26	2	26	1	12	2	12	1

4.4. Robustness to other content preserving modifications

The method A shows satisfying robustness to other content preserving modifications such as image rotation, slight cropping, and addition of noise. The proposed hash tolerates rotation by 1%, slight cropping below 1% of the image, scaling with scaling factor ranging from 0.2 to 1.5, mean Gaussian noise with σ^2 below 0.005 and salt and pepper noise with noise density below 0.05. The robustness to content preserving modifications is achieved by use of MOD-LBP features in the proposed hash.

4.5. Sensitivity to tampering

In order to make malicious modification in images, the regions of the image are selected and the pixel values of those regions are set to 255 so that the regions turn into white in colour. The percentage of the tampering is considered to study the sensitivity to tampering.

Table 4 gives the results of detecting tampering and the methods detect tampering above the specified percentages in the table. The method B is more sensitive to tampering which uses Haralick features as local features. MOD_LBP features are less sensitive to tampering as compared with Haralick features, but by combining both the local features in A, the hash can be made sensitive to forgery.

Table 4.Sensitivity to tampering

Images	A	B	C	D
Img1.jpg	1.20%	0.30%	1.50%	1.40%
Img2.jpg	0.70%	0.40%	3.50%	0.90%
Img3.jpg	0.60%	0.30%	0.80%	0.50%
Img4.jpg	0.50%	0.30%	0.80%	1%
Img5.jpg	1.20%	0.30%	1.60%	0.80%
Img6.jpg	0.70%	0.50%	1%	0.90%

5. Conclusion

In this paper, an image hash based on both global and local features is proposed. The local features are Haralick features and MOD-LBP features extracted from image blocks. The global features are luminance and chrominance characteristics of the whole image which are computed from Zernike moments. The proposed hash is applicable to image authentication. The hash generated is robust to common content preserving modifications such as JPEG compression, addition of noise, contrast and brightness adjustment, scaling, small angle rotation and slight cropping, but sensitive to forgery.

The Haralick features extracted from image blocks are highly sensitive to tampering as compared to MOD-LBP features, and MOD-LBP features are robust to content preserving modifications. Therefore the proposed hash is robust to content preserving manipulations and sensitive to malicious modifications.

References

1. M Schneider, S Fu. A robust content based digital signature for image authentication.*Proc IEEE Int Conf Image Processing* 1996; 3:227-230.
2. R Venkatesan, SM Koon, MH Jakubowski, P Moulin. Robust image hashing. *Proc IEEE Int Conf Image Processing* 2000; 3:664-666.
3. A Haouzia, R Noumeir. Methods for image authentication: A survey.*Journal Multimed tools and Appl* 2008; 39:1-46.
4. CASIA tampered image detection evaluation database. Available : http://forensics/idealtest.org.
5. EC Chang, MS Kankanhalli, X Guan,Z Huang, Y Wu.Robust image authentication using content based compression.*Journal Multimedia systems* 2003; 9:121-130.
6. F Ahmad, MY Siyal.A secure and robust hashing scheme for image authentication. *IEEE Int Conf InfComm And Signal Proc* 2005. p.705-709.
7. S Roy, Q Sun.Robust hash for detecting and localizing image tampering.*IEEE Trans Image Process* 2007; 6:IV-117 – VI-120.
8. VKitanovski, D Taskovski, S Bogdanova. Combined hashing/watermarking method for image authentication.*World Academy of Science, Engg and Tech* 6 2007; 3:223-229.
9. ZTang, SWang, X Zhang,W Wei, S Su.Robust image hashing for tamper detection using non-negative matrix factorization.*J Ubiquitous Convergence Technol* 2008; 2:18-26.
10. F Ahmed, M Y Siyal, V U Abbas.A secure and robust hash based scheme for image authentication.*Signal Process* 2010; 90:1456-1470.
11. Y Zhao, S Wang, G Feng, Z Tang. A robust image hashing method based on Zernike moments.*Journal of Computational Information Systems* 2010. p. 717-725.
12. Y Zhao.Perceptual image hash using texture and shape feature. *Journal of Computational Information Systems* 2012. p. 3519-3526.
13. Y Zhao, S Wang, X Zhang, H Yao.Robust hashing for image authentication using zernike moments and local features. *IEEE Trans Information Forensics and Security* 2013; 8:55-63.
14. RM Haralick, K Shanmugam, I Dinstein.Textual features for image classification.*IEEE Trans Systems MAN and Cybernetics*1973. p.610-621.
15. A Varghese, K Balakrishnan, RR Varghese, JS Paul.Content based image retrieval of brain MR images across different classes.*International journal of Electrical, Electronic science and Engineering* 80 2013.
16. Z Chen, SK Sun.A Zernike moment phase based descriptor for local image representation and matching.*IEEE Trans Image Process* 2009; 19:227-237.