



A SECURE HASHING SCHEME FOR IMAGE AUTHENTICATION USING ZERNIKE MOMENTS AND LOCAL FEATURES WITH HISTOGRAM FEATURES

Deepa.S¹, Nagajothi.A²

Department Of Computer Science Engineering
Karpagam University
Coimbatore
INDIA

Abstract: A secure hashing scheme is developed for image authentication and finding the forgery regions. The hash can be used to find similar, forged, and different images. It can also identify the type of forgery and locate fake regions containing salient contents. The global, local and histogram features are used in forming the hash sequence. The global features are based on Zernike moments representing luminance and chrominance characteristics of the image. The local features contain position and texture information of salient regions in the image. The histogram features includes the no pixels in the same intensity. Secret keys are used in feature extraction and hash construction. The hash is very sensitive to malicious tampering. The hash of a test image is compared with the reference image. The received image is judged as a fake when the hash distance is greater than a threshold T_1 and less than T_2 . By decomposing the hashes, the type of image forgery and location of forged areas can be determined. Probability of collision between hashes of different images is zero.

Keywords — Forgery detection; Image hash; Saliency; Zernike moments; Gaussian Filter; Geometric Deformation.

I. Introduction

With the widespread use of image editing software, more and more digital media products are easily to distribute illegal copy. Image hashing is a technique that extracts a short sequence from the image to represent its contents, and therefore can be used for image authentication. If the image is maliciously modified, the hash must be changed significantly. The hash functions in cryptography such as MD5 and SHA-1 that are extremely sensitive to every single bit of input, the image hash should be robust against normal image processing. Different images have significantly different hash values, and secure so that any unauthorized party cannot break the key and coin the hash. To meet all the requirements simultaneously, especially robustness and sensitivity to tampering, is a challenging task. In general an ideal image hash should have the following desirable properties [3]:

- Perceptual robustness: The image hash function should be insensitive to those common geometric deformations, image compression and filtering operations, which do alter the image but protect its visual quality. Visually similar images without major differences may have hashes with a small distance.
- Uniqueness: Probability of two different images having the same hash value should tend to zero.
- Sensitivity: Perceptually significant changes to an image should lead to a totally different hash. This significant feature is very useful in both image authentication and digital forensics.
- Secret Key: Secret keys are used for hash construction.

In [6] the hash method produces a satisfactory robustness performance. All of the geometric attacks respect the rule that some or all of the pixels are displaced at a random amount under the constraint of visual coherence. Based on the rule, we propose a robust hash solution by using the invariance of the histogram shape to geometric attacks. The histogram shape as the exploited robust feature it not only is mathematically invariant to scaling, rotation and translation, but also is insensitive to those challenging geometric attacks. In [7] the NMF construct a secondary image, and obtain low-rank matrix approximation of the secondary image with NMF again. The matrix entries are concatenated to form an NMF-NMF vector. The inner products of the NMF-NMF vector and a set of weight vectors are calculated. Because the final hash comes from the

secondary image with NMF, their method cannot locate forged regions.

A new framework FASHION [4], standing for Forensic Hash for Information assurance. The FASHION framework is designed to answer a much broader range of questions regarding the processing of multimedia data than simple binary decision from robust image hashing. It also offers more efficient and exact forensic analysis than multimedia forensic techniques. In clustering based approach [5], the first step extracts a feature vector from the image, whereas the second stage compresses this feature vector to a final hash value. In the feature extraction step, the two-dimensional image is mapped to a one-dimensional feature vector. This feature vector must capture the perceptual qualities of the image. Most of the pervious schemes are based on global or local or histogram features. In this paper we proposed global, local and histogram features. Global features are insensitive to changes of small areas in the image, local features can reflect regional modifications but it usually generates longer hashes and histogram features are sensitive to small area tampering but produces longer hashes

II. Image Hashing Concepts

A. Detecting forged images

On the rise of powerful graphical editors and sophisticated image manipulation techniques make it extremely easy to modify original images in such a way that any alterations are impossible to catch by an untrained eye, and can even escape the scrutiny of experienced editors of reputable news media. Image hashing algorithm is used to analyze an image on pixel level in order to detect whether significant changes were made to the actual pixels, altering the content of the image rather than its appearance on the screen.

B. visual saliency

A salient region in an image is one that attracts visual attention. The human visual perception allows humans to focus on the most important parts when observing visual scenes. In [2] Log spectrum of an image $L(i)$ is used to represent the common information of the image. Let $A(i)$ denote the redundant information in the $L(i)$, defined as convolution between $L(i)$ and an low pass kernel h_i :

$$A(i) = h_i * L(i) \quad \dots\dots\dots(1)$$

According to the Feature- Integration theory [13], observers focus on the areas where objects with significant low-level features (such as color, intensity, orientation and so on) to pop out.

C. Zernike moments

The Zernike moments are defined over the unit circle, two steps were required to convert a rectangular region of each image to a unit circle for calculation of Zernike moments. First, the 'center of fluorescence' (analogous to the center of mass) for each image was calculated and used to define the center of the pixel coordinate system. Second, the x and y coordinates were divided by 150 (this corresponds to the size of an average cell at the magnification used in these experiments). Only pixels within the unit circle of the resulting normalized image, $f(x,y)$, were used for subsequent calculations. The Zernike moments, Z_{nl} , for an image were then calculated using,

$$Z_{nl} = \frac{n+1}{\pi} \sum_x \sum_y V_{nl}^*(x, y) f(x, y) \quad \dots\dots\dots(2)$$

$Y = 0.2126 R + 0.7152 G + 0.0722 B$, where Y store the result of Luminance.

D. Gaussian Low-Pass Filters

The input images are filtered with the low pass Gaussian filter. Low-pass filter is used for enhancing robustness of the hash values to image processing operations, such as common compression and filtering. The low-pass filtering operation can be represented as the convolution of the Gaussian function $G(x, y)$ and an image $I(x, y)$:

$$F(x, y, \sigma) = G(x, y) * I(x, y) \quad \dots\dots\dots(3)$$

Where σ is the standard deviation represent the image distribution. The resultant of the Gaussian low pass filter is stored in $F(x, y, \sigma)$.

III. Image Hashing Algorithm Generation

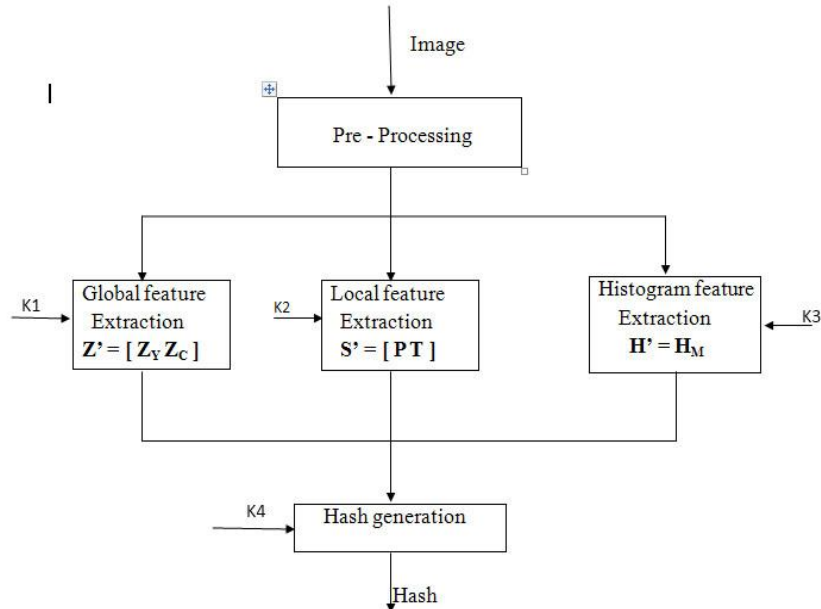
The hash function is created from Zernike moments to represent luminance / chrominance properties of the image, the texture features in salient regions to reflect local properties and the histogram properties. As illustrated in Figure 1, the image hashing method consists of the following steps,

- **Image Size :** The image is first convert to a fixed size, and converted from RGB to the YCbCr representation
- **Luminance and Chrominance Extraction:** The global features are based on Zernike moments representing luminance(Y) and chrominance(C) characteristics of the image. Zernike moments of Y and |CbCr| are calculated.

$$Z' = [Z_Y Z_C] \quad \dots\dots\dots(4)$$

A secret Key K_1 is used for hashing.

Figure 1 Block diagram of the image hashing method



- **Salient region Extraction:** Salient regions are detected from the luminance image Y. The local features include position (P) and texture information (T) of salient regions in the image. Texture is an important feature to human visual perception. There are six texture features relating to visual perception: coarseness, contrast, directionality, line-likeness, regularity and roughness. A secret key K_2 is used for image authentication

$$S' = [P T] \quad \dots\dots\dots(5)$$

- **Histogram Extraction:** The histogram (H_m) is extracted from the preprocessed image by referring to the mean value of the image. A rotationally invariant Gaussian filtering is designed to improve the hash robustness. A secret key K_3 is used to randomly generate a row vector X_3 containing 48 random integers in [0, 255]. Figure 2 shows the histogram value for the given image. The horizontal axis of the graph represents the tonal variations, while the vertical axis represents the number of pixels in that particular tone.

- **Hash Construction:** The Zernike features (Z) represent the global vectors, salient local vectors (S) and histogram vectors (H_m) are concatenated and produce an intermediate hash, namely H' . Secret key K_4 used to generate the final hash sequence H.

$$H' = [Z S H_m] \\ H' = H \quad \dots\dots\dots(6)$$

A. Image Authentication

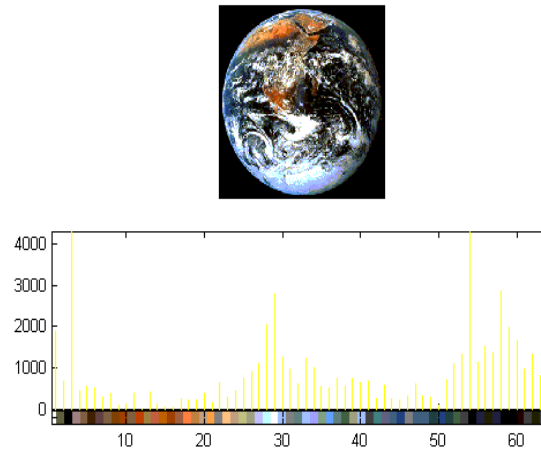
The images authentication is used to product the images from the forgery attacks. The image authentication process is performed in the following way.

- **Image Extraction:** The test image is transfer to global, local, and histogram vectors and the test image is extracted to obtain the intermediate hash without encryption ,

$$H_1' = [\text{Global vector}(Z) * \text{Salient vector}(S)] \quad \dots\dots\dots(7)$$

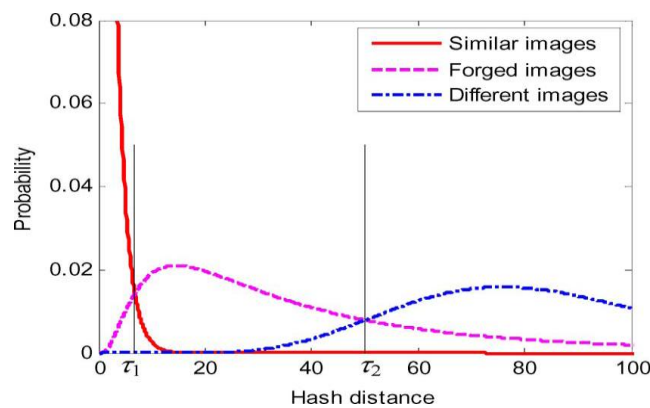
- **Decomposition of Global, Local and Histogram features:** The intermediate hash with secret keys K_1 , K_2 , and K_3 are concatenated to obtain the sequence of the trusted image. Decomposes the images into global, local and histogram features.

Figure 2: Example of Histogram Color Image



- **Salient Region comparison:** Check if the salient region in the test image is matching those in the trusted image.
- **Hash Distance Computation:** Find the distance between hashes of an image pair and check whether the images are similar, dissimilar and forged images. Figure 3, shows the hash distance of an image.
- **Localized the forgery areas:** The test images is a fake image, then locate the forged region and find the nature of the forgery. Four types of image forgery can be identified: removal, insertion, replacement of objects and unusual color changes.

Figure 3: Distribution of Hash Distance



The hash value H_0 , H_1 and H_2 representing global, local and histogram features and R denote the number of matched salient regions in the trusted image (N_0) and test image (N_1).

- If $N_0 > N_1 = R$, Object removal
- If $N_1 > N_0 = R$, Object insertion
- If $N_1 = N_0 = R$ and Calculation of hash distance $\delta Z_C - \delta Z_Y > T_C$, Unusual color changes.
- If $N_1 = N_0 = R$ and Calculation of hash distance $\delta Z_C - \delta Z_Y < T_C$, Replaced objects.
- If $N_0 > R$ and $N_1 > R$, Tampered salient region.

IV. Performance Evaluation

We have tested 350 image pairs hence the forgery images are correctly detected. The success rate of forgery localization is 96%. When the hash distance is greater than the threshold T_1 but less than T_2 , the received image is judged as a fake. Consider the threshold $T_1=7$ and $T_2=50$ used for finding the original and fake images. If the two different images have the similar hash distance, collision occurs. Figure 4 shows curves of Receiver Operating Characteristics (ROC). The ROC represent six types of content preserving processing: gamma

correction, JPEG coding, Gaussian noise addition, rotation, scaling, and slight cropping. Figure 5 shows the comparison of ROC and JPEG coding. The method ROC differentiates the original and forged image.

A. Forgery Detection

Today's powerful graphical editors and sophisticated image manipulation techniques make it extremely easy to modify original images. The image hashing algorithm is used to detect the forgery image efficiently. If the image is found as fake then analyze the hash distance in order to detect whether significant changes were made to the actual pixels, altering the content of the image rather than its appearance on the screen. Previous schemes are used either global or local features. The proposed method base on global, local and histogram features. It can easily identify the small area tampering and it is very sensitive to small area changes. It produces the short hash length. Forgery locations are schematically illustrated in Figure 6. The hash distance for the first example is 29.77, indicating the image is fake.

B. Forgery Region Findings

The forged images are produced by using graphical editing tools. The forged images are correctly detected by using the image hashing algorithm. Figure 7 shows the example of abnormal color changes. The rectangle in the image indicate salient region, hash distance $D=13.7$ indicating the image is tampered.

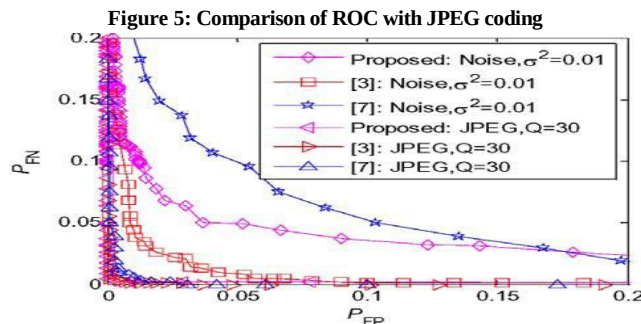
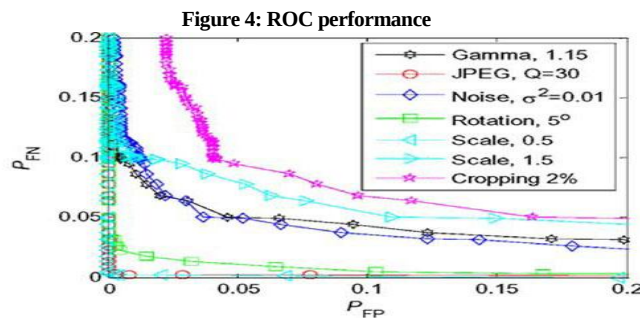


Figure 6: Hash Distance between the original and forged image a. Original image b. forged image

c. salient region and detection result

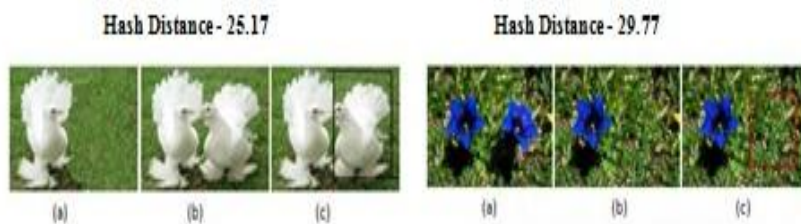
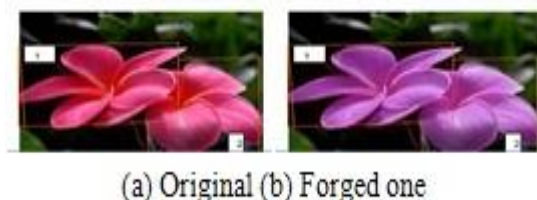


Figure 7: Example of abnormal color changes



V. Conclusion

In this paper, an image hashing method is mainly developed for image authentication and finding the forgery regions. The global features based on Zernike moments representing luminance / chrominance of the image, salient local features and histogram features include Gaussian filter are used to find the forgery region effectively. It reduces the collision between hashes of different images. The hash can be used to find similar, forged and other images. This method enhances the hash sensitivity to small area tampering at the same time it produce the short hash length and robustness.

VI. Reference

- [1] S.Xiang, H.J.Kim, and J.Huang, "Histogram-based image hashing scheme robust against geometric deformations," in Proc. ACM Multimedia and Security Workshop, New York, 2007, pp. 121-128.
- [2] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, "Robust Hashing for Image Authentication Using Zernike Moments and Local Features," IEEE Trans. Inf. Forensics Security, vol. 8, no. 1, pp. 18-26, May 2008.
- [3] Z.Tang, S.Wang, X.Zhang, W.Wei, and S.Su, "Robust image hashing for tamper detection using non-negative matrix factorization," J. Ubiquitous Convergence Technol., vol. 2, no. 1, pp. 18-26, May 2008.
- [4] W. Lu, A. L. Varna, and M. Wu, "Forensic hash for multimedia information," in Proc. SPIE, Media Forensics and Security II, San Jose, CA, Jan. 2010, 7541.
- [5] V.Monga, A.Banerjee, and B.L.Evans, "A clustering based approach to perceptual image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 68-79, Mar. 2006.
- [6] A.Swaminathan, Y.Mao, and M.Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215-230, Jun. 2006.
- [7] V.Monga and M.K.Mihcak, "Robust and secure image hashing via non-negative matrix factorizations," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 376-390, Sep. 2007.
- [8] F.Ahmed, M.Y.Siyal, and V.U.Abbas, "A secure and robust hash based scheme for image authentication," Signal Process., vol. 90, no. 5, pp. 1456-1470, 2010.
- [9] X.v and Z.J.Wang, "Perceptual image hashing based on shape contexts and local feature points," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1081-1093, Jun. 2012.
- [10] W.Lu, A.L.Varna, and M.Wu, "Forensic hash for multimedia information," in Proc. SPIE, Media Forensics and Security II, San Jose, CA, Jan. 2010, 7541.
- [11] S.Li, M.C.Lee, and C.M.Pun, "Complex Zernike moments features for shape-based image retrieval," IEEE Trans. Syst., Man, Cybern. A, Syst. Humans, vol. 39, no. 1, pp. 227-237, Jan. 2009.
- [12] Z.Chen and S.K.Sun, "A Zernike moment phase based descriptor for local image representation and matching," IEEE Trans. Image Process., vol. 19, no. 1, pp. 205-219, Jan. 2010.
- [13] X. Hou and L. Zhang, "Saliency detection: A spectral residual approach," in Proc. IEEE Int. Conf. Computer Vision and Pattern Recognition, Minneapolis, MN, 2007, pp. 1-8.
- [14] R.Venkatesan, S.M.Koon, M.H.Jakubowski, and P.Moulin, "Robust image hashing", Proceedings of IEEE International Conference on Image Processing, vol. 3, pp. 664-666, 2000.
- [15] A.Olmos and F.A.A.Kingdom. (2004) McGill Calibrated Colour Image Database. Available at: [http://tabby.vision.mcgill.ca]
- [16] Standard test image - Wikipedia, the free encyclopedia. Available at: [http://en.wikipedia.org/Standardtest image]