International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Content Based Image Authentication Using Local and Global Feature Extraction

K.Alice[1], N.Ramaraj[2]
[1]GKM College of Engineering and Technology
[2]Thangavelu Engineering College

Abstract- The entire content of the image can be represented with the help of a short sequence called Hash. It can also be represented using local and global feature. The methods used for extracting the local features are simple statistical data such as Mean and Standard deviation. The method used for extracting the global feature is Zernike moments. Sender generates the hash using the local and global features and attaches it with the image to be sent. The same process is repeated in the receiver side. Finally the hash generated from the sender and receiver side should be verified to examine the authenticity of the image. Then the tampered image is detected and localized the areas where the forgery takes place.

Keywords-Image hash, tamper detection, global features, Zernike moments, local features.

I. INTRODUCTION

In Modern universe counterfeiting identification technique is a significant outlet with the extensive application of image editing applications and software. Image hashing method can be used as an image authentication and security. Dissimilarly the hash methods in cryptography as they are utmost sensitive to trifling changes the hash method must be brawny against analogical and simple image processing. The beneficial nature of the image hash should be compact, brawny, and perceptive to forgery. It should be peculiar and not acknowledge any unsecured or unauthorized person to rend and change the hash. At this time we present a process amalgamating favourable opportunity of the one and the other of local lineaments and global lineaments. Our characterizing is to give an equitably compact image hash with beneficial accomplishment. Zernike moments of the brightness components to cogitate the image global characteristics are applied to finalize whether the image is tampered or not. Estimate relatively with few other system the tendered method has more excellent performance in tamper localisation.

II. LITERATURE SURVEY

There are lots of hashing techniques and only some of them are referred here. Khelifi et al [1] stated a robust and authenticated hashing method that relay on virtual watermark detection. Monga et al' [2] use NMF to pseudo randomly pick sub images, and they fabricate a secondary image. These processes gain a low-rank matrix gradual convergence image with NMF again. A.Swaminathan [3] stated an image hash scheme depends on rotation invariance of Fourier -mellin transformation and submit a fresh framework to learn the authentication issues of previous image hashing methods. This scheme is robust to geometric deformation. Monga [4] uses a two step framework and hash had a regular repetition in many image hashing schemes. Many old methods were compact but unsecured with local reflected area modifications. Tang et al' [5] elevate a global scheme using non-negative matrix factorization [NMF]. The initial image was translated in the form of fixed sized pixel array. A delicate image was achieved by replacing pixels and by using NMF to exhibit features bearing co-efficient matrix. In [6] xinag et al' stated a method using invariance of the image histogram to geometric distortion. Even though it was brawny it could not differentiate images with cloned histograms. In [7] lei et al' compute DFT of the invariant moments of significant radon transform coefficients and normalize the DFT coefficient to generate the image hash for the data encrypted authentication.

III. AUTHENTICATION SYSTEM

The proposed image hashing method is implemented in three stages. First, the sender generates the hash code of the pre-processed (resized into a square image of size K x K ,eliminating the noise and generating the grey scale image) image using local features like mean and standard deviation and global features like complex Zernike moments. Second, the receiver generates the hash code using the same methods as that of sender. In the final stage both the hash received from the sender and receiver should be verified. If both the hash code is same then the image is said to be authentic otherwise the image will be tampered and the region of tampering is

identified.

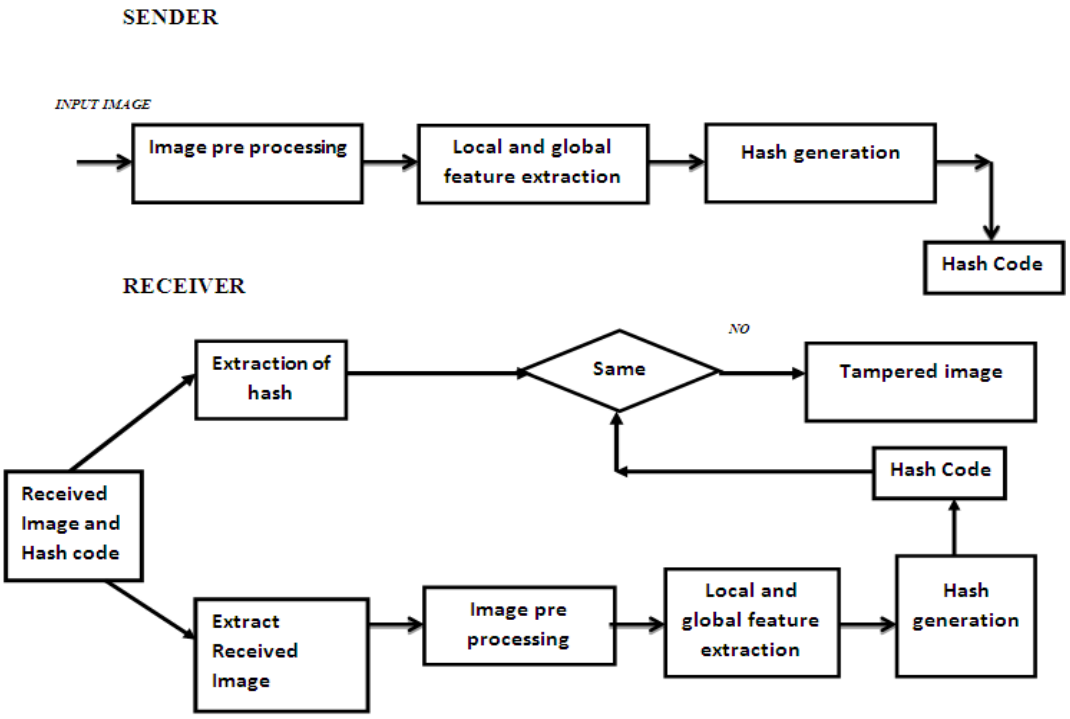


Fig: 1- Image Authentication System architecture

A. Pre-processing

In image pre-processing the input image is resized to a constant square image of size [256 x 256] using Bilinear Interpolation.A Gaussian filter is then applied to the resized image to eliminate the noise. The reason for resizing the image is when the image is too small the important features may be discarded or if it too large the hash code generated will be very lengthy. The RGB image is then converted into grey scale imageto extract the local and global features. The size of the image for this system is kept constant as a square image [256 x 256].

Fig 2 (a) Original Image of Size 215x315 (b) Interpolated to size of 256x256 (c) Grey scale image used for feature extraction

B. Local Feature Extraction

In the local feature extraction the image (256 x 256) is divided into non-overlapping 64 blocks of size 32x32 . The input for extracting the local features is in grey scale image. For each block the mean and standard deviation is calculated using the formula given below

For mean, $M=\sum^{n}_{i=1} X_i /n$

For standard deviation, $S=\sum^{n}_{i=1} (Y_i - M) /n$

Now we get the local features as L'=[M S] where M means the mean and S denotes the standard deviation. The vector of L' is 128 x 1 sizes. The size of the mean is [64x1] and standard deviation is [64x1]. After calculating the local features for each block sized

[128 x 1], the hash code is generated. We generate a secret key K1 of size [128x1] which contains values in the range 0 to 255 for generating hash using local features

C. Global Feature Extraction

In the global feature extraction, we use Complex Zernike moments. The grey scale image of size 256x256 is taken as input for extracting global features. The order of the Zernike moments we choose is 6 (i.e. n=6). For order 6 there will be totally 28 moments. These 28 moments are generated and stored as a vector of [28x1].

The Complex Zernike moments of order n with repetition m for a continuous image function f(x,y) for X Y image plane are defined as

$$A_{nm}=n+1/\pi \iint_{x^2+y^2<=1} f(x, y)\, V_{nm}^{*}(P, \theta)\, dx\, dy$$

$$A_{nm}=n+1/\pi \int_0^2 \pi \int_0^{1f} (P, \theta)\, R_{nm}^{*}(P) \exp(-jmo)\, P.dP.d\theta$$

Where n is either positive integer of 0.m takes positive and negative integer with the constants n-|m|= even and |m|<=n, P is the length of the vector from the origin to the pixel at (X, Y) and θ is the angle between vector P and the X-Axis is the counter clockwise direction.

The Zernike Polynomial is given as

$$V_{nm}(x, Y) = V_{nm}(P \sin\theta, P \cos\theta) = R_{nm}(P) \exp(jm\theta)$$

It refers complex conjugate.The features of invariance under image rotation makes Zernike function of the most important moments. We generate a secret key K2 of size [28x1] which contains values in the range 0 to 255 for generating hash using global features

D. Hash Code Generation

In hash generation, the intermediate hash is generated for both the local and global feature extracted. The hash code for local features can be constructed by adding the local features L [128x1] and key K1 [128x1] which is stored in HL of size [128x1] using

$$HL= [(L+K1) \bmod 256]$$

The hash code for global features can be constructed by adding the global features [28x1] and key K2 [28x1] which is stored in HG of size [28x1] using

$$HG= [(G+K2) \bmod 256]$$

The intermediate hash generated is then concatenating F=[HL,HG]. This size will be [156x1] vector elements. Now for generating the final hash code a secret key K3 of size [156x1] which contains values in the range 0 to 255 is randomly generated. Then the final hash is generated using

$$HF= [(F+K3) \bmod 256]$$

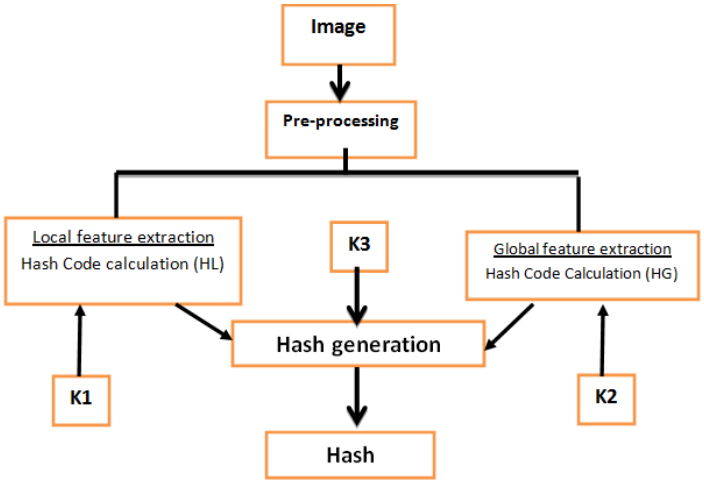


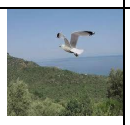
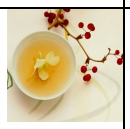
Fig.3 Hash Generation

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

E. Hash Verification

The image is transmitted along with the hash code generated using the above mentioned method to the receiver. At the receiver side the received image is extracted from hash code computed at the sender side. The same set of methods is applied to the received image to generate a hash code for the received image. At this point, there will be a hash code for both the sent and received images. They must be compared and if it is same the received image is Authentic or else received image may be a tampered one. In case of tampered image, the tampered region is detected and localized to view the regions of tampering. Tamper localization can be done by comparing the hash code of sent image and hash code of received image generated by local features. Since this hash code is generated based on image blocks, the difference in the position of hash code vector correctly identifies the location (block) of tampering.

TABLE-I

Input Image		Preprocessed Image		Received image	Result of Authentication System	Tamper Localization Image
Size	Image	Size	Image			
800 x521		256 x256			Tampered	
256 x192		256 x256			Tampered	
800 x600		256 x256			Tampered	
800 x600		256 x256			Tampered	
800 x600		256 x256			Tampered	

IV. RESULT AND DISCUSSION

Using this method, main pair of test images downloaded from internet and from dataset CASIA [10] is tested. It produces 100% result in tampering detection and also provides 100% result in identifying the tampered regions [Localization].This method is robust against salt and pepper noise and zero mean Gaussian noise as an initial Gaussian filter is applied to the image during pre-processing. The combination of both local and global features in generating hash removes the vulnerability of having same feature vector for different images which is a drawback in content based authentication system.

V. CONCLUSION

The limitation in the proposed system is that the hash code generated is not robust against content preserving modification since

simple statistical data such as mean and standard deviation is used in representing local features. The future enhancement may be focused on selecting a suitable local feature that is invariant to content preserving modification and geometric modification.

REFERENCES

[1] Khelifi and J.Jiang, "perceptual image hashing based on virtual watermark detection,"IEEEtrans. Image process. vol. 19, no. 4, pp. 981-994, Apr.2010
[2] V. Monga and M.K. Mihcak, "Robust and secure image hashing via non-negative mark factorizations,"IEEE Trans. Inf. Forensics security, vol. 2, no. 3, pp. 376-390, Sep.2007
[3] A.Swaminathan, Y. Mao, and m. Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics security, vol, 1, no. 2, pp. 215-230,Jan. 2006.
[4] V. Monga, A.Banerjee, and. L. Evans, "a clustering based approach to perceptual image hashing," IEEE Trans. Inf. Forensics security, vol. 1, no. 1, pp. 68-79, Mar. 2006
[5] 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.
[6] 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.
[7] Y. Lei, Y. Wang, and J. Huang, "Robust image hash in radon transform domain for authentication," Signal process. : Image commun.Vol 26, no. 6, pp. 28[8] A. Fouad and J. Jianmin, "Analysis of the security of perceptual image hashing based on non-negative matrix factorization, "IEEE Signal process. Lett. , vol. 17, no. 1, pp. 43-46, Jan. 2010.
[8] R Venkatesan, SM Koon, MH Jakubowski, P Moulin. Robust image hashing.Proc IEEE IntConf Image Processing 2000;3:664-666.
[9] 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. 0-288, 2011.s
[10] CASIA tampered image detection evaluation database. Available :http://forensics/idealtest.org.
[11] A Haozia, R Noumeir. Methods for image authentication: A Survey .JournalMultimed tools and appl 2008; 39:1-46.
[12] M Schneider , S Fu A robust content based digital signature for image authentication.Proc IEEE IntConf Image Processing 1996