ISSN:0975-9646

Image Authentication by Features Extraction and Biomeric key

S.Saravanan
ECE, Maamallan Institute of technology, Sriperumbudur,Chennai,India.

***Abstract*— A robust authentication method is developed for detecting image forgery including removal, insertion, and replacement of objects, and abnormal color modification, and for locating the forged area. Both global and local features are used in forming the hash sequence. The global features are based on Zernike moments representing luminance and chrominance characteristics of the image as a whole. The local features include position and texture information of salient regions in the image. Secret keys are introduced in feature extraction and hash construction. While being robust against content-preserving image processing, the hash is sensitive to malicious tampering and, therefore, applicable to image authentication. Global features are generally short but insensitive to changes of small areas in the image, while local features can reflect regional modifications but usually produce longer hashes. So we here concatenate those important features and produce a hash. The hash of a test image is compared with that of a reference image. When the hash distance is greater than a threshold and less than the received image is judged as a fake. 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 approaches zero. In order to eaves-droppers to hack the calculated features we protect the sequence for high security. So the biometric keys produced are protected using chaotic neural network. So the time for computing whether the image is forged or same image is less and the produced sequence is less.**

***Keywords*—Imagecoding,Featureextraction, hashing, Forgery, Zernike moments,Robustness**

I. INTRODUCTION

A digital image is an array of real or complex numbers represented by a finite number of bits. An image given in the form of a transparency, slide, photograph or an X-ray is first digitized and stored as a matrix of binary digits in computer memory. This digitized image can then be processed and/or displayed on a high-resolution television monitor.In image authentication, the hash of a trusted image is available and called the reference hash. The hash of a received image to be tested is extracted using the above method.[1] These two hashes are compared to determine whether the test image has the same contents as the trusted one or has been maliciously tampered, or is simply a different image. Here, two images having the same contents (visual appearance) do not need to have identical pixel values. One of them, or both, may have been modified in normal image processing such as contrast enhancement and lossy compression.[2] In this case, we say the two images are perceptually the same, or similar. The image authentication process is performed in the following way.

Feature Extraction: Pass the test image through the steps as described in Section A to obtain the intermediate hash without encryption.

Hash Decomposition: With the secret keys and, restore the intermediate hash from the reference hash to obtain, which is a concatenated feature sequence of the trusted image. Decompose it into global and local features.[3]

Salient Region Matching: Check if the salient regions found in of the test image match those in of the trusted image. If the matched areas of a pair of regions are large enough, the two regions are considered as being matched. Reshuffle the texture vectors by moving the matched components in each of the texture vector pair to the left-most and, for notational simplicity, still call them and . For example, if there are three salient regions in the reference image and two in the test image, The first two pairs of subvectors in and may either be matched or unmatched. The vectors and are reshuffled accordingly.

Hash Distance Calculation: We use a distance between hashes of an image pair as a metric to judge similarity/ dissimilarity of the two images. To define the hash distance,a feature vector is formed by concatenating the global feature vector and the reshuffled texture feature vector .The vector does not contribute to the distance calculation but will be used to locate forged regions[4,5,6]

$$D=\|Z1 - Z0\|$$

The hash distance between the test image and the reference image is the Euclidean distance between them and for a pair of a similar images, the texture features in the corresponding salient regions are close to each other. However, since no currently available method of saliency detection is perfect, the salient regions obtained from an image after content-preserving processing may not always precisely match that of the original.[7]

If this happens, difference between the test image and the original will be exaggerated. In practice, the global structure of an image represented by Zernike moments is sufficient to distinguish similar from dissimilar. To minimize the adverse influence of saliency detection inaccuracy, we omit in calculating the hash distance for similar images:

$$D=\|Z1 - Z0\| \triangleq D_G$$

The issue of saliency detection will be discussed later. Having defined the hash distance, we can use it first to distinguish similar and dissimilar images according to a threshold. If the two images are said to be similar, otherwise the images are dissimilar. We then need to further determine whether the test image is a tampered version of the reference image, or simply a different one. To do so, compare the distance with second thresholds. The

test image is judged as tampered if. Otherwise it is a completely different image.[8,9]

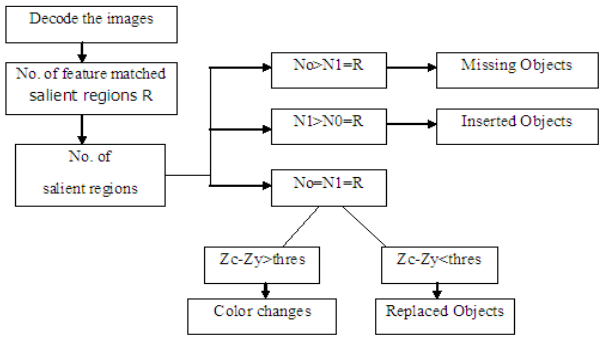

Fig.1 Image Authentication

No ⟶ no of salient regions of the reference image
N1 ⟶ *no of salient regions of the test image*
N0=4, N1=3 So No>N1 in the image the object is missing. This removal forgery is happen.N0=4,N1=5So No<N1 in the image the object is insert. This insertion forgery is happen.In this case N0=N1=4,We use a threshold value to find what type of forgery happen.
Zc-Zy> threshold.The color change is happen.
Zc-Zy<threshold.The object replacement is happen.[10,11,12]

II. EXISTING SYSTEM

The Yan Zhao, Shuozhang Wang, Xinpeng Zhang and Heng Yao, Member, IEEE developed a robust hashing scheme for image authentication using Zernike moments and local features.Both the global and local features are used in forming the hash sequence. When the hash distance is greater than a threshold t1 and less than t2,the received image is judged as fake. By decomposing the hashes, the type of image forgery and location of forged areas can be determined.[13,14]
The XudongLv and Z.Jane Wang, Member, IEEE, proposed a novel shape contexts based image hashing using local feature points. SIFT Harris detector is used for selecting the most stable SIFT keypoints under various content preserving distortions. It yields better identification performances under geometric attacks such as rotation attacks and brightness changes and the FouadKhelifi and Jianmin Jiang, Member, IEEE, analysed the security of perceptual image hashing based on NMF. Hashing technique uses three independent keys in different stages.[15,16] This use of a secret key combined with image dependent keys could enhance security, so that the information leakage about the final key will be smaller due to its dependence on the image content.
The FouadKhelifi and Jianmin Jiang, Member, IEEE, proposed a robust and secure perceptual image hashing technique based on virtual watermark detection using an optimum multiplicative watermark detector. The security of the hashing system is enhanced by decreasing the information leakage about the key.The HuibaoLin,Jennie Si, Fellow, IEEE and Glen.P.Abousleman, Member, IEEE, proposed a paper based on orthogonal rotation invariant moments for Digital Image Processing.[17] ORIM.s such as Zernike moments are introduced and defined in a continuous unit disk and have been proven powerful tool in optics application. To improve orthogonality a different approach of using numerical optimization technique is used. With the improved orthogonality image reconstruction becomes more accurate.
The Vishal Monga and M.KivancMihcak, Member, IEEE, proposed the use of NMF for image hashing.The hash algorithm is builded with lowest misclassification enhancing necessary robustness to attacks.[18]The AshwinSwaminathan, Yinian Mao, Student Member, IEEE and Min Wu, Member, IEEE proposed a novel algorithm for generating an image hash based on Fourier transform features and controlled randomization.[19,20]This hashing scheme could identify malicious manipulations such as a cut and paste type of editing, which preserves the content of the image.[21]The Vishal Monga, student member, IEEE, Arindam Banerjee and Brian. L. Evans, senior member IEEE, proposed a clustering based approach to perceptual image hashing. For the purpose of security image hashing, randomized clustering algorithm is developed.
In the existing system,secret keys are generated using probability values. Probability key values can be easily identified by random implementation.[11,12]
So we introduce a biometric technique for generating this secret keys. Therefore,unauthorized person cannot coin the hash. Hence image can be authenticated.

III. PROPOSED SYSTEM

In our proposed technique we are going to calculate some related important features of an image and then comparing it with the test image to identify the image is „Similar or Forged. There are many techniques for authenticating an image. Our aim is to authenticate an image efficiently with high reliability and less complexity. So, we extract these feature characteristics of local, i.e. Position and texture Features and global Features i.e. Zernike Moments.
We propose a method combining advantages of both global and local features. The objective is to provide a reasonably short image hash with good performance, i.e., being perceptually robust while capable of detecting and locating content forgery.We use Zernike moments of the luminance or chrominance components to reflect the image's global characteristics, and extract local texture features from salient regions in the image to represent contents in the corresponding areas. Distance metrics indicating the degree of similarity between two hashes are defined to measure the hash performance. Two thresholds are used to decide whether a given image is an original/normally-processed or maliciously doctored version of a reference image, or is simply a different image. The method can be used to locate tampered areas and tell the nature of tampering, e.g., replacement of objects or abnormal modification of colors. Compared with some other methods using global features or local features alone, the proposed method has better overall performance in major specifications, especially the ability of distinguishing regional tampering from content-preserving processing.
The second one using the human face as a key to security, biometric face recognition technology has received significant attention in the past several years due

to its potential for a wide variety of applications in both law enforcement and non-law enforcement.As compared with other biometrics systems using fingerprint/palm print and iris, face recognition has distinct advantages because of its non-contact process. Face images can be captured from a distance without touching the person being identified, and the identification does not require interacting with the person. In addition, face recognition serves the crime deterrent purpose because face images that have been recorded and archived can later help identify a person.

The Block Diagram explains the flow the Hash Key generation. Using the preprocessing techniques images are scaled, resized, formats conversions and removal of noise. The Next Step is the image is given to two blocks namely Global Feature Extraction and Salient feature Extraction. The Global Features of an images calculated here are Zernike Moments which has 22 features and the Salient Features of an images calculated here are salient region detection of Position Vectors [10]and Texture vectors which consists of 48 features.

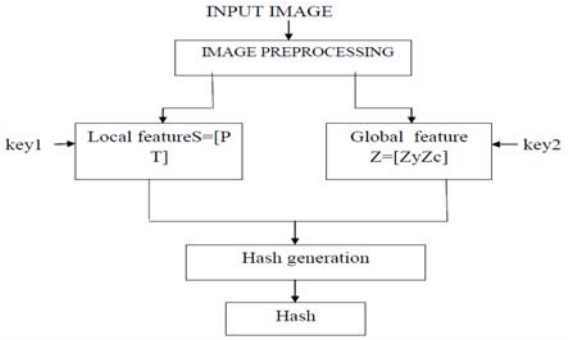

Fig. 2 Block diagram of proposed system

The image is first rescaled to a fixed size F×F with bilinear interpolation, and converted from RGB to the YCbCr representation. Y and |Cb-Cr| are used as luminance and chrominance components of the image to generate the hash. The aim of rescaling is to ensure that the generated image hash has a fixed length and the same computational complexity. Small F leads to loss of fine details, while large F results in high computational complexity. We choose F=256 as an appropriate trade-off.

In Local feature extraction, K largest salient regions are detected from the luminance image Y .The coordinates of top left corner and width/height of each circumscribed rectangle are used to form a K- element vector p(k)(k=1,2…..K), representing the position and size of each salient region. For those having more than 6 salient regions, the total area of the 7^{th} and smaller salient regions are less than 1.5% of the image areas. With larger K, fewer salient regions are missing but will lead to a longer image hash. For example, the percentage of images with no more than 7 salient regions is 99.5%. We choose K=6 as a reasonable trade-off.

Local texture features of each salient region including coarseness C1 and contrast C2,skewness and kurtosis are computed and rounded to give a 6 element vector t(k) (k = 1,2,…6).If an image has less than 6 salient regions, the positions and texture features of the missing ones are set to zero. The position/size and texture vectors of all salient regions together form a local feature vector S=[P T]=[p(1)…..p(6)t(1) ……t(6)],which contains 48 integers. A secret key K2 is used to randomly generate a row vector X2 containing 48 random integers in [0,255].An encrypted local vector S is then obtained by S=[(S+X2)mod 256].

Salient region in an image is one that attracts visual attention. It has two parts, Innovation and Prior knowledge. Innovation is the necessary region in an image and prior knowledge is the redundant or unwanted parts in an image. The information of saliency is obtained when the redundant part is removed. [9]Log spectrum of an image(f) , is used to represent general information of the image. Because log spectra of different images are similar, there exists redundant information in L (f). Let A(f) denote the redundant information defined as convolution between L(f) and l*l low-pass kernel h1.Spectral residual representing novelty of the image B(f) can be obtained by subtracting A(f) from L(f), which is then inversely Fourier transformed to give a saliency map S.

Saliency is a concept which states that there are regions in a scene that are more “attractive” than their neighboursand hence draw attention. Attention can be due to bottom-up cues or top-down influences.A saliency map of an image is a representation of the salient regions of the image. These are the regionsthat are most likely to draw attention. The conspicuity of a location in the visual scene determines the level ofactivity of the corresponding units in different feature maps. The saliency map combines the information of allthe feature maps into one global measure of conspicuity. Saliency at a given location is determined primarily byhow different thislocation is from its surroundings in terms of colour, intensity, orientation, motion, depth etc.From the many locations that are salient the most salient region stands out.

The procedure for calculating the saliency map of a frame can be summarized in the following steps:

1. Linear filtering of the image at 8 spatial scales is done to extract features corresponding to luminance andedge properties.
2. For each individual feature, the spatial contrast map is calculated by taking the difference of the featuremaps across several scales.
3. The feature maps are subjected to iterative convolutions with a Difference of Gaussian filter which suppressesisolated noisy regions.

In Global feature extraction, Zernike moments of Y and |Cb-Cr| are calculated. Because shape features can be obtained from a small number of low frequency coefficients, theordern does not need to be large. We choosen =5.Further, since Zn-m=Zn,m only $Z_{n,m}(m \geq 0)$ is needed.We do not use Z0,0 as it represents the average intensity. Table I lists the Zernike moment features from order 1 to order 5.Thus we have 11× 2=22 Zernike moments in total. Magnitudes of the Zernike moments are rounded and used to form a global vector,Z=[ZyZc] .Each element in Z is no more than 255.A secret key k1 is used to randomly generate a row vector X1 with 22 random integers in [0,255].The encrypted global vector Z is obtained as Z=[(Z+X1) mod 256]. In general, moments describe numeric quantities at some distance from a reference point or axis.

TABLE I
ZERNIKE MOMENTS OF DIFFERENT ORDERS

ORDER n	ZERNIKE MOMENTS	NO.OF. MOMENTS
1	Z1,1	1
2	Z2,0 , Z2,2	2
3	Z3,1 ,Z3,3	2
4	Z4,0 ,Z4,2 ,Z4,4	3
5	Z5,1 ,Z5,3 ,Z5,5	3

Fig. 3 Zernike Moments

The above figures shows the images of character A and five rotated versions of it. From left to right rotation angles are : 0,30,60,150,180,300.

Global features are calculated based on the Zernike moments of the image. Zernike moment of order n and repetition m of a digital image I(ρ,θ) is defined by

$$Z_{n,m} = \frac{n+1}{\pi} \sum_{(\rho,\theta)\text{unitdisk}} \sum I(\rho,\theta) V^{*}_{n,m}(\rho,\theta)$$

where $V_{n,m}$ (ρ,θ) is a zernike polynomial of order n and repetition m.

$V_{n,m}(\rho,\theta) = R_{n,m}(\rho) e^{jm\theta}$

in which n = 0,1….,0 ≤ |m| ≤ n, n-|m| is even and $R_{n,m}(\rho)$ are real valued radial polynomials. Suppose α is a rotation angle and $Z_{n,m}$ and $Z_{n,m}^{®}$ the ZM of the original and and rotated images respectively, then

$$Z^{(r)}_{n,m} = Z_{n,m} e^{-jm\alpha}$$

The magnitude of ZM is rotation invariant, while the phase changes with angle.

$\arg(Z^{(r)}_{n,m}) = \arg(Z_{n,m})^{-m\alpha}$

In Hash construction, The global and salient local vectors are concatenated to form an intermediate hash, namely H=[Z S] which is then pseudo randomly scrambled based on a secret key K3 to produce the final hash sequence H.The following table gives the constitution of an image hash of 70 integers.

TABLE II
CONSTITUTION OF IMAGE HASH

GLOBAL VECTOR (Z)		SALIENT VECTOR (S)	
Z(Zernike moments)	P(x,y,width,height)	T(texture features)	Total length
11*2=22 integers	4*6=24 integers	4*6=24 integers	70 integers

SIMULATION OUTPUT

Fig. 4 RGB to GRAY Conversion

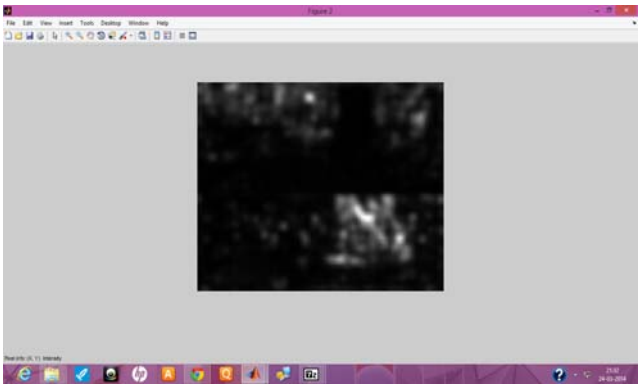

Fig. 5 RGB to YCbCr Conversion

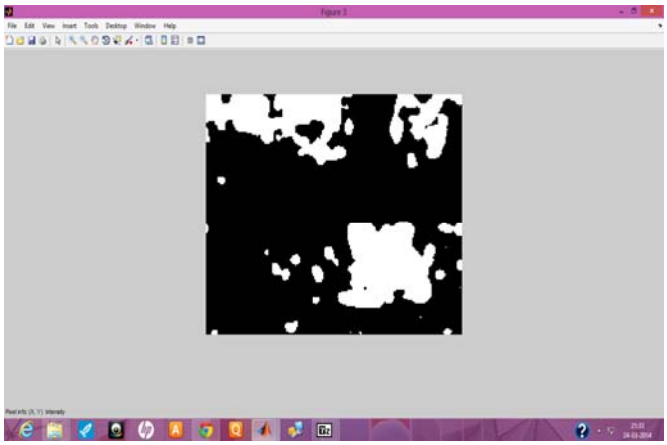

Fig. 6 Saliency Map

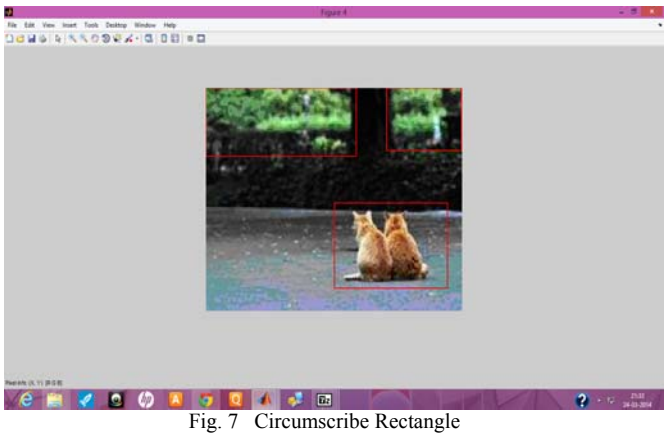

Fig. 7 Circumscribe Rectangle

PHOTOSHOOT OF HARDWARE

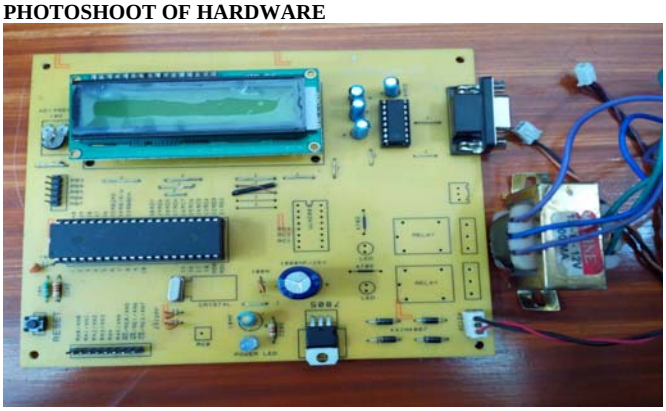

Fig.8 Processor On Board

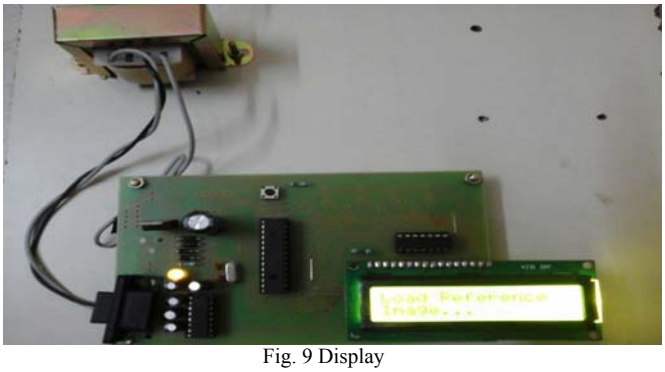

Fig. 9 Display

IV. CONCLUSIONS AND FUTURE ENHANCEMENT

In this paper, an image hashing method is developed using both global and local features.The global features are based onZernike moments representing the luminance and chrominancecharacteristics of the image as a whole. The local features includeposition and texture information of salient regions in theimage. Collision probability between hashesof different images is very low. The proposed scheme has areasonably short hash length and good ROC performance.The method described in this paper is aimed at image authentication.The hash can be used to differentiate similar, forgedand different images. At the same time, it can also identify thetype of forgery and locate fake regions containing salient contents.By decomposing the hashes, the nature of image forgeryand locations of forged areas can be determined.It should be stressed that the success of image authenticationusing the proposed scheme depends to a large extent on theaccuracy of saliency detection. The method proposed is used due to its acceptable accuracy and computation complexity.One can always incorporate a better saliency detection scheme, whenever it is available, into the algorithm for improved performance.

Further study is desired to find features that better represent the image contents so as to enhance the hash's sensitivity to small area tampering while maintaining short hash length and good robustness against normal image processing .Zernike algorithm can be efficiently enhanced for all the images.Salient feature values can be efficiently calculated.

ACKNOWLEDGMENT

I wishes to acknowledge our friends and students for developing the research idea which have been used in the preparation of this template.

REFERENCES

[1] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, Member, IEEE"Robust Hashing For Image Authentication Using Zernike Moments And Local Features" IEEE Transactions On Information Forensics And Security, Vol.8, No. 1, January 2013.

[2] Zhenjun Tang, Xianquan Zhang, Shichao Zhang, "Robust Perceptual Image Hashing Based on Ring Partition and NMF", *IEEE Transactions on Knowledge & Data Engineering*, vol.26, no. 3, pp. 711-724, March 2014.

[3] 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 and Applications*, vol. 52, no. 2/3, pp. 325-345, 2011

[4] Y. Lei, Y.Wang, and J. Huang, "Robust image hash in Radom transform domain for authentication," IEEE Signal Process.Image Communication.vol.26, no.6, pp.280288, 2011.

[5] Z. Chen and S.K. Sun, "A zernike moment phase-based descriptor for local image representation and matching", *IEEE Transaction on image processing.*, vol 19. no.1, pp. 205-219, Jan. 2010.

[6] F. Khelifi and J. Jiang, "Perceptual Image Hashing Based on Virtual Watermark Detection," *IEEE Trans. Image Processing*, vol. 19, no. 4, pp. 981-994, Apr. 2010.

[7] K. 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] F. Ahmed, M.Y. Siyal, and V.U. Abbas, "A Secure and Robust Hash-Based Scheme for Image Authentication," *Signal Processing*, vol. 90, no. 5, pp. 1456-1470, 2010.

[9] W. Lu and M. Wu, "Multimedia Forensic Hash Based on Visual Words," *Proc. IEEE Int'l Conf. Image Processing*, pp. 989-992, Hongkong,2010.

[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, C. M. Pun, "Complex Zernike Moments Features for Shape Based Image Retrieval", IEEE Transactions on System Man and Cybernetics, Vol. 39,pp. 227-237, JAN2009.

[12] 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 and Technology*, vol. 2, no. 1, pp. 18-26, may 2008.

[13] H. Lin, J. Si, G.P. Abousleman. Orthogonal rotation-invariant moments for digital image, processing.Image Processing, IEEE Transactions on, 17(3), 272 – 282, JAN 2008.

[14] X. Hou and L. Zhang, "Saliency detection: A spectral residual approach," in Proc. IEEE Int. Conf. Computer Vision and Pattern Recognition,pp 1-7, Minneapolis, MN,JUN 2007.

[15] V.Monga, 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.

[16] 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.

[17] 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.

[18] A. Swaminathan, Y. Mao, and M. Wu, "Robust and Secure Image Hashing," *IEEE Trans. Information Forensics and Security*, vol. 1, no. 2, pp. 215-230, June 2006.

[19] T. Deselaers, D. Keysers, and H. Ney, "Features for image retrieval: A quantitative comparison," in Lecture Notes in Computer Science, Volume 3175, pp 228-236,2004, Springer.

[20] E. Lehmann, J. Romano: *Testing Statistical Hypotheses*, 3rd edition, Newyork,Springer, 2005.

[21] Zhao, Shuozhong Wang, Guorui Feng, Zhenjun Tang, "A Robust Image Hashing Method Based on Zernike Moments",IEEE Journal of Computational Information Systems6:3 717-725,2011.