

# SMART: Saliency Map, Moments and Texture Features for Robust Image Authentication

Derroll David<sup>1</sup>, Divya B<sup>2</sup>, Pournami<sup>3</sup>

<sup>1</sup>PG Scholar, Department of Computer Science and Engineering, Vimal Jyothi Engineering College, Kannur, Kerala, India

<sup>2</sup>Head of Department, Department of Computer Science and Engineering, Vimal Jyothi Engineering College, Kannur, Kerala, India

<sup>3</sup>Assistant Professor, Department of Computer Science and Engineering, NIT Calicut, Kerala, India

**Abstract:** *Image Authentication is the process of providing proof to a person or system that the images are indeed that claims to be. Image hashing is a technique used for image authentication and is very popular and ensures remarkable results. Global and Local feature extraction is enhanced for generating a hash that is sensitive to image content. Normal manipulations like JPEG coding, rotation, cropping, additive noise, gamma correction and scaling are robust enough so that the image content information can be recognized as authentic even if the image intensity is varied by these operations. The concern regarding content preserved hashing is that the salient regions need to be detected accurately so that local feature extraction can be applied in to the region of interest. A hybrid approach consisting of frequency prior, center prior and location prior along with watershed for segmentation is used for extracting the saliency regions in the image more efficiently with increasing localization capability in less hash length.*

**Keywords:** Image Authentication, Forgery, Hashing, Saliency map, Zernike moment, Texture Features

## 1. Introduction

Information had been playing a vital role since history. It is spread from battle plans to the high technologies present today. In the current era, information can travel miles through unsecure channels and are source to various communications. Forgery of these information can lead to false interpretations and can result in false military targets, false medical diagnosis etc. With the advance in technology, the image manipulation tools have skilled to efficiently alter the original image. As a result lot of forged copies are circulating widely through internet and other medias. These can lead to situations in which no digital image can be produced as an evident in court, as official document, medical reports or military etc. There are criminal cases reported and cyber cell is vigilant about these practices. The end result of such forgery can result in huge financial corruption and even thread to human lives. Recently, many digital image manipulations are identified in media outlets, scientific journals, newspapers etc. Detecting forgery in digital image is a vibrant area of research. Image authentication is the area in image processing which can identify such false images and provide wide variety of applications. Forensic image authentication is the application of image science and domain expertise to discern if a questioned image or video is an accurate representation of the original data by some defined criteria. There can be basically two types of image authentication namely, strict image authentication and selective image authentication. In hashing, signatures are generated from significant characteristics that represent the image semantic content. Since there is no exact definition of how to extract the image content, it is very much challenging to find the image semantic content. In order to determine the relevant characteristics there are some features like edge, color, histogram, textures, etc. Semantic content cannot be found if any one among these is used. Instead a combination of such features are extracted to build a hash that is sensitive

to the authenticity of the image. The hash of the suspect image is compared with the reference hash and if it is less than a predefined threshold then authentic else forged. Military target, evidence at court, research area etc are some of the applications of image authentication.

## 2. Related Work

Image authentication has obtained significance because many areas in science and literature are using images for diagnosis, proof of identity, entertainment etc. There are many image authentication techniques using hashing.

R. Venkatesan et al. [1] proposed a method that utilizes a wavelet representation for images and new randomized processing strategies for hashing. The image is submitted to Haar Wavelet decomposition and the rectangles statistics are calculated and quantized using randomized rounding. At the decoding stage, the Reed Muller error correction code is used to generate the final hash bit. It is robust to some of the attacks such as rotation (2 degree), cropping (upto 10%), scaling (upto 10%), shifting (upto 5%), JPEG compression (upto 10%), median filtering. Algorithm is not key dependent and also the Collision Probability for unrelated image is less. The disadvantages are it does not support large rotations, computationally more complex and support minor geometric distortion.

C. De Roover et al. [2] proposed a method using radial projection of image pixels for robust image hash. RASH (Radial hASH) considered moments of different order. It identifies the pair of equivalent or distinct images. The image is subjected to some operations and the Radial variance vector (RAV) is generated. It then computes the DCT of the RAV and hence the transformed RAV or TRAV. The first 40 coefficients are called RASH. The advantage of using such a system is that the computational complexity is less, robust to

filtering and geometric distortion and collision risk is very less. The disadvantages are collision avoidance property not sufficient for secure applications and RASH collision intractability is low.

In [3], Ashwin Swaminathan et al. proposed that the image hash can be generated based on Fourier transform features and controlled randomization. Three steps are included in this process namely; pre-processing, feature generation and post processing. The advantage is that the hash function is resilient to content preserved modification i.e. to moderate geometric and filtering distortion. It provides excellent security and robustness along with invariant to 2D affine transformation. The disadvantage of this approach is that some hashes are computed easily than others.

Shijun Xiang et al. [4] proposed a method in which image histogram shape invariance to geometric distortions is exploited for image hashing. The image is passed through a low pass filter. During histogram extraction, the mean of the image along with the output of the low pass filter is manipulated for generating hash. The hash is protected using a key. The approach is robust to geometric attacks and cannot distinguish images with similar histograms but different contents.

Vishal Monga and M.K. Mihcak proposed in [5] a method to compute image hash using non-negative matrix factorization. Pseudo random sub-image is selected from the image and NMF is applied and forms a secondary image. The NMF is applied to secondary image again and a NMF-NMF vector is formed. Hash bits are generated hence. It prevents intentional attacks of guessing and forgery. The drawback is that it cannot locate forged regions.

Zhenjun Tang et al. [6] used global method using non-negative matrix factorization. The pixels are rearranged and converted to fixed pixel arrays. The NMF is applied on the secondary image to obtain feature bearing coefficient matrix and then coarsely quantized. So formed binary string is scrambled to form the hash bits. The approach is robust against Gaussian filtering, moderate noise contamination, JPEG compression, re-scaling and watermark embedding. Hashes of different images have very low collision probability. It has the advantage of detect tampering to local image areas. It is not capable to resist rotation attacks is a major drawback.

Fouad Khelifi and Jianmin Jiang [7] proposed a method where robust and secure perceptual image hashing based on Virtual Watermark Detection. In order to produce the hash bit, the original image undergoes some pre-processing and the extracted coefficients along with the virtual watermark produced by passing the key through pseudo random noise generator is given to the watermark detector. Robustness is provided against normal image processing operation and geometric transformation. It also detects content changes in relatively large areas. Detection of small area forgery and localization of forged regions are not possible.

Yanqiang Lei et al. [8] produced robust image hashing using Radon Transform. Select the significant coefficients from Radon transform of image. Calculate the moment and DFT. Normalization and quantization of the result produces the hash bits. It is tolerant to image processing manipulations such as JPEG compression, geometric distortion, blur, addition of noise and enhancement. Detection of small area forgery is not possible.

Yan Zhao et al. [9] proposed a method based on rotation invariant Zernike moments. Firstly, Zernike moment transform of pre-processed image gives the extracted Zernike moment features for the hash. It is successfully secured using a key to produce the final hash. Robust features of the image is extracted and secure from content preserving attacks such as JPEG compression, additive noise, watermark embedding, scaling, brightness and color adjustments, gamma correction, gaussian filtering and rotation. It has the advantage of detecting inserted objects. Yan Zhao et al. [10] modified the work in [9] to include texture features.

Texture features that are of visual importance to humans are proposed in [11]. The four texture feature coarseness, contrast, skewness and kurtosis are selected for image authentication applications as it has more influence in determining whether an image is authentic or not.

Salient region detection is important in knowing the image semantic content. The techniques used for salient region detected are discussed.

Itti et al. [12] model follows the Feature Integration Theory [13] by first decomposing the visual input into separate low-level features maps. Then, normalized center-surround difference maps are computed for individual features and later combined by a weighting scheme to form a saliency map.

Harel et al. [14], proposed the graph-based visual saliency (GBVS) model by introducing a novel graph based normalization/combination strategy.

Klein and Frintrop [15] modeled the center-surround contrast in an information-theoretic way, in which two distributions of visual feature occurrences are determined for a center and a surround region.

Bruce and Tsotsos [16], modeled the images saliency as the maximum information that can be sampled from it. In their method, saliency is computed as Shannon's self-information.

By analyzing the log-spectrum of the input image, Hou and Zhang [17] proposed a Fourier transform based method to extract the spectral residual of an image in the spectral domain and to construct the corresponding saliency map in the spatial domain; one prominent advantage of this method is its low computational complexity.

Hou's [18], proposed the image signature to approximate the foreground of an image within the theoretical framework of sparse signal mixing.

Achanta et al. [19], proposed a conceptually simple approach by combining image's band pass filtered responses from three CIEL\*a\*b\* channels. This method can provide pleasing results in most cases and it has the advantage of computational efficiency. This was improved in [20] by considering the special effects of boundaries.

Cheng et al. [21], proposed a regional contrast based saliency extraction algorithm, which simultaneously evaluates global contrast differences and spatial coherence.

Goferman et al. [22], proposed a new type of saliency, namely context-aware saliency, which aims at detecting the image regions that represent the scene.

Salient region detection model are basically used for preprocessing in computer vision, image authentication application etc. The key features of salient region detection are salient region predicted should be highly correlated to the visual system of human beings and should be having low computational complexity.

Ling Zhang et al. [23] propose a salient region detection method called SDSP (Salient detection by combining simple prior) which have low computational complexity and high performance. Three simple priors are combined to construct the algorithm.

- Frequency Prior - Band pass filtering can be used to detect salient objects of visual importance.
- Color Prior - Warm colors are more attractive to human visual system than cold colors.
- Location Prior - The center of the image is of more visual attraction than the pixels far away.

Hence, by combining the zernike moment for global feature extraction and SDSP for determining salient region in an image, to which the texture features can be applied for local features extraction can be integrated to form a hash. The hash generated can determine whether an image is authentic or forged.

### 3. Proposed Hashing Scheme

In this section, the proposed image hashing scheme is introduced. Image authentication is achieved using the hash generated. The global properties of the image are captured using Zernike moments [24]-[26] and local properties of the image captured using texture features [27] and [28] in salient regions. In case of content aware image authentication the content or the region of interest (ROI) of the image is vital which can be obtained by SDSP [23].

#### A. Image Hash Construction

Image hash construction consists of four steps.

##### 1. Preprocessing

Different images have different dimensions and the hash generated for those should be having the same computational complexity and fixed length. That is, the time taken to generate the hash of an image should be similar to the time

taken to generate the hash of the other and also the hash length is same. Hence, the images are rescaled to a fixed size  $F \times F$  with bilinear interpolation. It is then converted from RGB to the  $YCbCr$  representation.  $Y$  and  $|C_b - C_r|$  are used as luminance and chrominance components of the image to generate the hash. Small  $F$  leads to loss of fine details, while large  $F$  results in high computation complexity. Choose  $F = 256$  as an appropriate trade-off.

##### 2. Global Feature Extraction

Global feature extraction of the image is obtained from Zernike moments. The Zernike moments of  $Y$  and  $|C_b - C_r|$  are calculated. Zernike moment of order  $n$  and repetition  $m$  of digital image  $I(\rho, \theta)$  are defined as [24] - [26].

$$Z_{n,m} = \frac{n+1}{\pi} \sum_{(\rho,\theta) \in \text{unit disk}} I(\rho, \theta) V_{n,m}^*(\rho, \theta)$$

Where,  $V_{n,m}(\rho, \theta)$  is a Zernike polynomial of order  $n$  and repetition  $m$ .

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

in which  $n - |m|$  is even,  $n = 0, 1, \dots$  and  $0 \leq |m| \leq n$ .

$$R_{n,m}(\rho) = \sum_{s=0}^{\frac{n-|m|}{2}} \frac{(-1)^s (n-s)! \rho^{n-2s}}{s! \left(\frac{n+|m|}{2} - s\right)! \left(\frac{n-|m|}{2} - s\right)!}$$

$R_{n,m}(\rho)$  are real-valued radial polynomials.

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

Where,  $\alpha$  rotation angle,  $Z_{n,m}$  and  $Z_{n,m}^{(r)}$  Zernike moment of original and rotated images respectively.

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

Magnitude of Zernike moment is rotation invariant while phase changes with angle. Shape features can be obtained from a small number of low frequency coefficients of the Zernike moment, the order is small ( $n = 5$ ). Further,  $Z_{n,-m} = Z_{n,m}^*$ , so only  $Z_{n,m} (m \geq 0)$  is needed. Exclude  $Z_{0,0}$  as it represent average intensity. Thus total number of Zernike moment is  $11 \times 2 = 22$  integers. Magnitudes of the Zernike moments are rounded and used to form a global vector  $Z = [Z_Y Z_C]$ . Each element in it is no more than 255.

##### 3. Local Feature Extraction

Salient Regions of the image are detected to extract the local features of the image. A salient region in an image is one that attracts visual attention. Salient region detection is a fundamental research area as it has wide application in content aware image authentication, neuroscience and computer vision etc. Three simple priors are combined to form the algorithm [23]. Texture properties of the salient

regions are computed along with the positions of the salient region.

### 3.1 Salient Region Detection

Saliency map is detected using the following methods. Priors are very much useful in this case.

#### 3.1.1 Frequency Prior

Achanta et al. [19] adopted the Difference of Gaussian (DoG) band-pass filtering responses from opponent color channel (such as the  $CIEL^*a^*b^*$  color channels) and integrated them for saliency detection. Lin Zhang et al. [SDSP] adopted the log-Gabor filter [29] instead of DoG. Transfer function of log-Gabor filter

$$g(x)(x = (x, y) \in R^2)$$

in frequency domain can be expressed as

$$G(u) = \exp \left( -(\log \frac{\|u\|_2}{\omega_0})^2 / 2\sigma_F^2 \right)$$

Where,  $u = (u, v) \in R^2$  is the coordinate in frequency domain and  $\omega_0$  is the filter's center frequency, and  $\sigma_F$  controls the filter's bandwidth. Image  $f(x)$  converted to opponent color space ( $CIEL^*a^*b^*$ ). The three resulting channels are denoted by  $f_L(x)$ ,  $f_a(x)$  and  $f_b(x)$ . "Frequency Saliency" defined as

$$S_F(x) = ((f_L * g)^2 + (f_a * g)^2 + (f_b * g)^2)^{\frac{1}{2}}(x)$$

Where,  $*$  denote the convolution operation.

#### 3.1.2 Color Prior

Research studies [30] show that warm colors are more attractive to human eyes than cold colors. For example, red and yellow are warm colors while green and blue are cold colors.  $CIEL^*a^*b^*$  is an opponent color system, in which  $a^*$ -channel represents green-red information while  $b^*$ -channel represents blue-yellow information. Dependence of  $a^*$  and  $b^*$  channel color appearance varies. Image  $f(x)$  converted to opponent color space ( $CIEL^*a^*b^*$ ). The three resulting channels are denoted by  $f_L(x)$ ,  $f_a(x)$  and  $f_b(x)$ . "Color Saliency" defined as

$$S_C(x) = 1 - \exp \left( -\frac{f_{an}^2(x) + f_{bn}^2(x)}{\sigma_C^2} \right)$$

Where,  $\sigma_C = 0.25$ .

Linear mapping of  $f_a(x)$  to  $f_{an}(x) \in [0, 1]$  and  $f_b(x)$  to  $f_{bn}(x) \in [0, 1]$ ,

$$f_{an}(x) = \frac{f_a(x) - \min a}{\max a - \min a}$$

$$f_{bn}(x) = \frac{f_b(x) - \min b}{\max b - \min b}$$

Where,  $\min a$  ( $\max a$ ) is the minimum (maximum) value of  $f_a(x)$  and  $\min b$  ( $\max b$ ) is the minimum (maximum) value of  $f_b(x)$ .

#### 3.1.3 Location Prior

Visual attraction of the image is largely concentrated to the center of the image. Studies have claimed it to be true as well [31]. The result can be adopted in case of saliency as the center area has more relevant information about the image than that are far away. This prior can be simply and effectively modeled as a gaussian map. Suppose  $c$  is the center of the image  $f(x)$ . "Location Saliency" defined as

$$S_D(x) = \exp \left( -\frac{\|x - c\|_2^2}{\sigma_D^2} \right)$$

Where,  $\sigma_D = 200$ .

#### 3.1.4 Saliency Detection by combining Simple Prior

Depending on the three simple prior defined. The final saliency map can be defined as.

$$SDSP(x) = S_F(x) \cdot S_D(x) \cdot S_C(x)$$

For the given image  $f(x)$ ,

$S_F(x)$  Denote frequency prior,

$S_C(x)$  Denote color prior and

$S_D(x)$  Denote location prior.

### 3.2 Texture Features

Texture features of the salient regions detected are computed. Four texture features from [27] are considered for image authentication applications for virtual perception namely coarseness  $C_1$ , contrast  $C_2$ , skewness and kurtosis to define the texture properties. The pixels in the neighborhood sized  $2^k \times 2^k$  are averaged to find the coarseness around a pixel.

$$A_k(x, y) = \frac{1}{2^{2k}} \sum_{i=x-2^k}^{x+2^k-1} \sum_{j=y-2^k}^{y+2^k-1} g(i, j) \quad k = 0, 1, \dots, 5$$

Where,  $g(i, j)$  is the gray level of pixel  $(i, j)$ .

Differences between average values of nonoverlapping neighborhoods on opposite sides of the pixel in horizontal and vertical directions are:

$$E_{k,h}(x, y) = |A_k(x + 2^{k-1}, y) - A_k(x - 2^{k-1}, y)|$$

$$E_{k,v}(x, y) = |A_k(x, y + 2^{k-1}) - A_k(x, y - 2^{k-1})|$$

For that point, find the size that leads to the highest difference value and call it  $S_{opt}(x, y)$

$$S_{opt}(x, y) = \arg \max_{k=0, \dots, 5; d=h, v} E_{k,d}(x, y)$$

Average of  $S_{opt}$  over a region is called the coarseness  $C_1$

Contrast can be defined as the brightness variation of an image. It can be defined as:



$$C_2 = \sigma^2 \mu_4^{-4}$$

Where  $\sigma^2$  represent variance and  $\mu_4$  represent fourth order moment.

### 3.3 Position of the Salient Region

Analysis of different images has shown that a particular image can have on an average of six salient regions and the rest are less important or negligible. Hence, only six salient regions are considered for generating the hash values. Each salient region is circumscribed by a rectangle. The coordinates of the top-left corner and width/height of the rectangle form a set. Six such sets are generated. If an image has less than six salient regions then the missing ones are set to zero.

$$p^{(k)} (k = 1, \dots, 6)$$

### 3.4 Local Feature Vector

The position/size and the texture features (coarseness, contrast, skewness and kurtosis) form the local feature vector.

$$S = [P \ T] = [p^{(1)} \dots p^{(6)} \ t^{(1)} \dots t^{(6)}]$$

## 4. Hash Generation

The Global vector (Z) and salient local vector (S) are concatenated to form the hash value  $H = [Z \ S]$ . The fixed length of the hash value is 560 bits long.

### A. Image Authentication

Two similar images can have different pixel intensities, it need not be same. The exact matching of pixels may not be applicable in some image authentication as it can be subjected to normal manipulations such as compression, contract variation etc. For such, image authentication application can use hashing. The procedure for image authentication is as follows and shown in Fig 3.1.

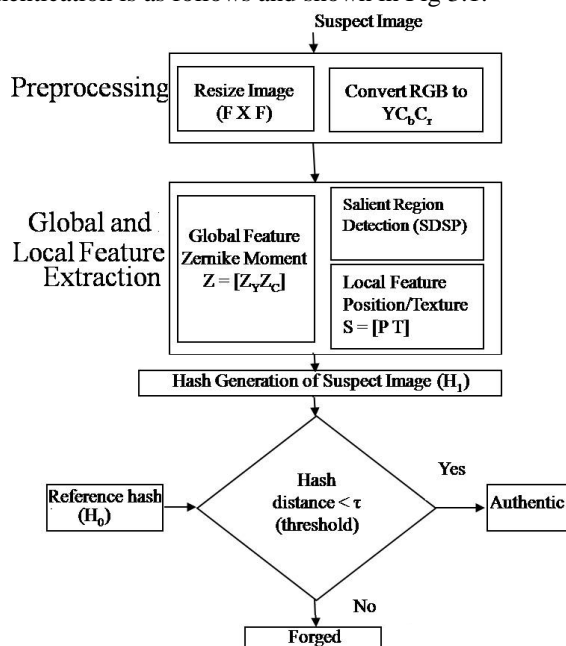


Figure 3.1: Proposed hashing scheme

Step 1: The hash of the trusted image  $H_0$  is called as reference hash.

Step 2: The hash of the suspect image  $H_1$  is computed.

Step 3: The hamming distance between the two is determined.

Step 4: If the distance is less than predefined threshold then authentic else forged.

In case of similar images the hash distance is:

$$D \approx ||Z_1 - Z_0|| \triangleq D_C$$

In case of different images the hash distance is:

$$D = ||V_1 - V_0||$$

$$V = [Z \ T]$$

T can be  $T_0$  (texture feature of reference image) and  $T_1$  (texture feature of suspect image).

$$T_0 = [t_0^{(1)} t_0^{(2)} t_0^{(3)} 0 0 0] \text{ and } T_1 = [t_1^{(1)} t_1^{(2)} 0 0 0 0]$$

The first two pairs of sub vectors in  $T_0$  and  $T_1$  may either be matched or unmatched. The vectors and are reshuffled accordingly.

### B. Forgery Classification and Localization

1. If  $N_0 > N_1 = R$

Some objects are removed and the missing objects located by comparing saliency indices Fig 3.3.

2. If  $N_1 > N_0 = R$

Some objects are inserted and the inserted objects located by comparing saliency indices shown in Fig 3.2.

3. If  $N_1 = N_0 = R$

Check the luminance and chrominance in Zernike moments.

$$\delta Z_C = ||Z_{C1} - Z_{C0}||$$

$$\delta Z_Y = ||Z_{Y1} - Z_{Y0}||$$

If  $\delta Z_C$  is greater than  $\delta Z_Y$  by a threshold  $\tau_C$  then there is color modification shown in Fig 3.5.

4. If  $N_1 = N_0 = R$

Check the luminance and chrominance in Zernike moments.

$$\delta Z_C = ||Z_{C1} - Z_{C0}||$$

$$\delta Z_Y = ||Z_{Y1} - Z_{Y0}||$$

If  $\delta Z_C$  is less than  $\delta Z_Y$  by a threshold  $\tau_C$ , then there is replaced object shown in Fig 3.4.

$$\delta t^{(k)} = ||t_1^{(k)} - t_0^{(k)}|| \quad k = 1, \dots, 6$$

$k^{\text{th}}$  salient region having maximal  $\delta t^{(k)}$  recognized as the replaced object.

5. If  $N_0 > R$  and  $N_1 > R$

Some of the salient regions are not matching. Hence the image is tampered.

## 4. Experimental Results

### A. Robustness and Anti-Collision

Fig 4.1 shows hash distances between similar images. The similar images are generated by applying the normal manipulations on the image. Some of the normal manipulations include gamma correction with  $\gamma = 2$ , JPEG coding with  $Q = 20$ , zero mean Gaussian noise addition with  $\sigma^2 = 0.01$ , rotation by 10 degree, scaling with factors 0.3, and slight cropping with more than 2 percent of the image width/height removed. It is observed that more than 99% of all distances are less than  $\tau = 2$ . If the values have exceeded the overall general hash distance, then the image intensity changes may have affected the saliency map.

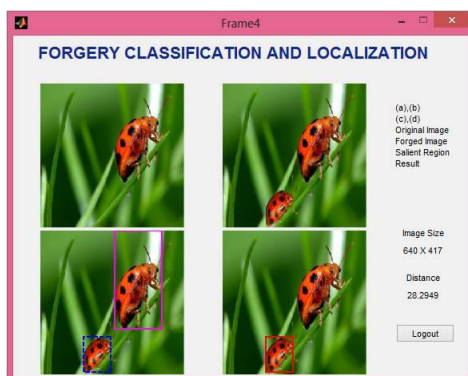


Figure 3.2: Insertion of Object

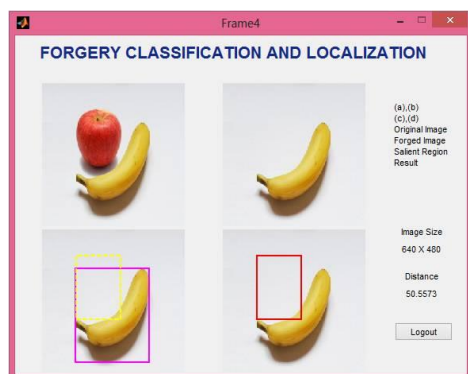


Figure 3.3: Removal of Object

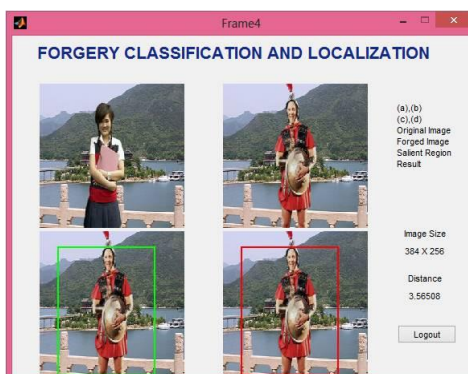


Figure 3.54: Replacement of Object



Figure 3.5: Color Modification

If two different images have a hash distance less than  $\tau$  the computed hash distance then there is a collision. In the best hash technique, the collision probability should be always very less. That is, the anti-collision performance is very important. It is observed that in the proposed system the collision probability is very low so that the different images having less hash distance than  $\tau$  is minimal.

### B. Capability to Detect Forgery

It is observed that the hash has good ability in distinguishing normal manipulations from regional forgery. Note that, in calculating ROC, the false negative (FN) and false positive (FP) errors are errors in differentiating between similar and forged images rather than between similar and different images shown in Fig 4.2.

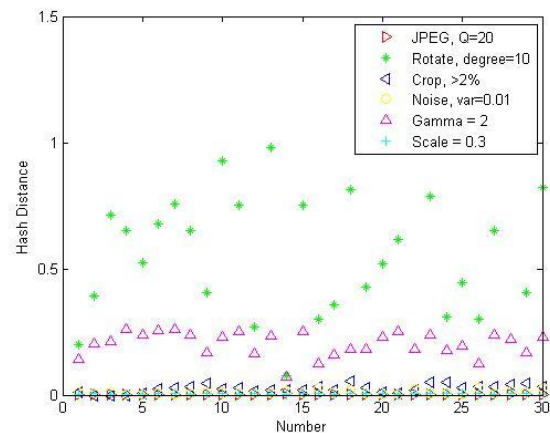


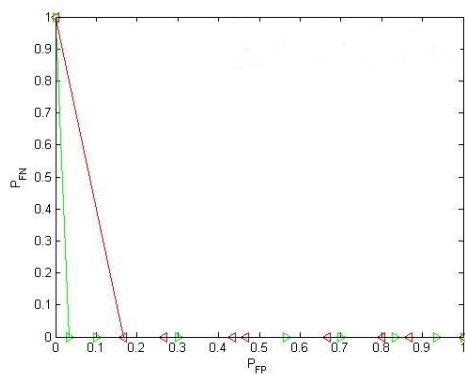
Figure 4.1: Hash Distance of similar images

The error probabilities are defined as:

$$P_{FN} = \frac{\text{Number of natural images judged as forged images}}{\text{Total number of natural images}}$$

$$P_{FP} = \frac{\text{Number of forged images judged as natural images}}{\text{Total number of forged images}}$$

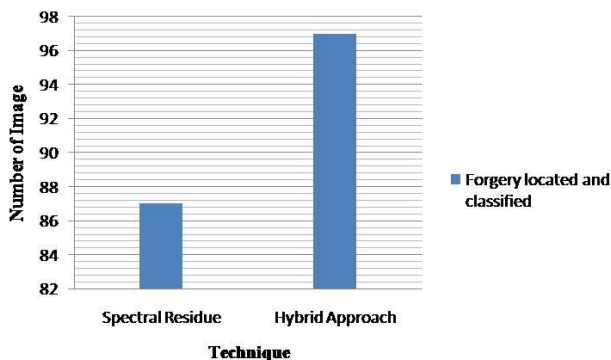
The red curve shows the performance to provide robustness for normal manipulations by Yan Zhao et. al [10] and the green curve shows the proposed work result. The more the curve is close to the axis the more the system is efficient to normal manipulations like JPEG coding, cropping, rotation, scaling, gamma correction and additive noise.



**Figure 4.2: ROC Curve**

### C. Forgery Localization

Around 100 image pairs, with the original and forged images collected from the CASIA dataset and color modification manually edited using photoshop are tested. The forged images are all correctly detected. Without considering forgery classification, the success rate of forgery localization is 98%. The success rate while considering localization and classification is substantially increased from 87% in [10] to an accuracy of more than 97%. Hence the issues of saliency detection in the previous work [17] lowering the accuracy of localization and classification is improved. The performance is shown in 4.3.



**Figure 4.3: Location and classification comparison**

## 5. Conclusion

Image authentication is achieved using the image hashing technique. The hash for the original and forged image is computed and compared to check if the images are authentic or forged. The proposed hash scheme is developed using two types of feature extraction namely global feature extraction and local feature extraction. The luminance and chrominance characteristics of the image as a whole is computed and the zernike moment is applied on it. Global feature is extracted by using zernike moments. The position and texture features of the salient region detected are concatenated to form the local feature extraction. High performance is achieved as both global and local feature extraction is considered. Localization and classification of image forgery is achieved by saliency detection simple prior. Further study is desired to find features that better represent the image contents so as to enhance the hashes sensitivity to small area tampering.

## References

- [1] R. Venkatesan, S. M. Koon, M.H. Jakubowski and P. Moulin, "Robust Image Hashing", In: Proceeding of International conference on Image processing, 2000, Vol. 3, pp. 664 – 666.
- [2] C. De Roover, C. De Vleeschouwer, F. Lefebvre and B. Macq, "Robust Image hashing based on Radial variance of pixels", International Conference on Image Processing, 2005, pp. III-77-80.
- [3] Ashwin Swaminathan, Yinian Mao and Min Wu, "Robust and Secure Image hashing", IEEE Transaction on Information Forensics and Security, 2006, Vol. 1, Issue 2, pp. 215-230.
- [4] S. Xiang, H. J. Kim, and J. Huang, "Histogram-based image hashing scheme robust against geometric deformations", In Proc. ACM Multimedia and Security Workshop, 2007, pp. 121–128.
- [5] 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.
- [6] 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.
- [7] F. Khelifi and J. Jiang, "Perceptual image hashing based on virtual watermark detection", IEEE Transaction on Image Processing, vol. 19, no. 4, pp. 981–994, Apr. 2010.
- [8] Y. Lei, Y.Wang, and J. Huang, "Robust image hash inRadon transform domain for authentication", Signal Processing: Image Commun., vol. 26, no. 6, pp. 280–288, 2011.
- [9] Yan Zhao, Shuozhong Wang, Guorui Feng and Zhenjun Tang, "A Robust Image Hashing Method Based on Zernike Moments", Journal of Computational Information Systems, pp. 717-725, 2010.
- [10] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao "Robust Hashing for Image Authentication Using Zernike Moments and Local Features", IEEE transactions of information forensics and security, vol. 8, no. 1, January 2013.
- [11] T. Deselaers, D. Keysers, and H. Ney, "Features for image retrieval: A quantitative comparison," in Lecture Notes in Computer Science, 2004, vol. 3175, pp. 228–236, Springer.
- [12] L. Itti, C. Koch, and E. Niebur, "A model of saliency based visual attention for rapid scene analysis," IEEE Trans. PAMI, vol. 20, pp. 1254-1259, 1998.
- [13] A.M. Treisman and G. Gelade, "A feature-integration theory of attention," Cognitive Psychology, vol. 12, pp. 97-136, 1980.
- [14] J. Harel, C. Koch, and P. Perona, "Graph-based visual saliency," Adv. Neural Information Process. Syst., vol 19, pp. 545-552, 2007.
- [15] D.A. Klein and S. Frintrop, "Center-surround divergence of feature statistics for salient object detection," ICCV'11, pp. 2214-2219, 2011.

- [16] N. Bruce and J. Tsotsos, "Saliency based on information maximization," *Adv. Neural Information Process. Syst.*, vol. 18, pp. 155-162, 2006.
- [17] X. Hou and L. Zhang, "Saliency detection: a spectral residual approach," *CVPR'07*, pp. 1-8, 2007.
- [18] X. Hou, J. Harel, and C. Koch, "Image signature: highlighting sparse salient regions," *IEEE Trans. PAMI*, vol. 34, pp. 194-201, 2012.
- [19] R. Achanta, S. Hemami, F. Estrada, and S. Susstrunk, "Frequency-tuned salient region detection," *CVPR'09*, pp. 1597-1604, 2009.
- [20] R. Achanta and S. Susstrunk, "Saliency detection using maximum symmetric surround," *ICIP'10*, pp. 2653-2656, 2010.
- [21] M. Cheng, G. Zhang, N.J. Mitra, X. Huang, and S. Hu, "Global contrast based salient region detection," *CVPR'11*, pp. 409-416, 2011.
- [22] S. Goferman, L. Zelnik-Manor, and A. Tal, "Context aware saliency detection," *CVPR'10*, pp. 2376-2383, 2010.
- [23] Lin Zhang, Zhongyi Gu, and Hongyu Li, "SDSP: A Novel Saliency Detection method by combining Simple Priors", *ICIP 2013*.
- [24] H. Lin, J. Si, and G. P. Abousleman, "Orthogonal rotation-invariant moments for digital image processing," *IEEE Trans. Image Process.*, vol. 17, no. 3, pp. 272-282, Jan. 2008.
- [25] 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.
- [26] 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.
- [27] T. Deselaers, D. Keysers, and H. Ney, "Features for image retrieval: A quantitative comparison," in *Lecture Notes in Computer Science*, 2004, vol. 3175, pp. 228-236, Springer.
- [28] H. Tamura, S. Mori, and T. Yamawaki, "Textural features corresponding to visual perception," *IEEE Trans. Syst., Man, Cybern.*, vol. 8, no. 6, pp. 460-472, Jun. 1978.
- [29] D. J. Field, "Relations between the statistics of natural images and the response properties of cortical cells," *J. Opt. Soc. Am. A*, vol. 4, pp. 2379-2394, 1987.
- [30] X. Chen and Y. Wu, "A unified approach to salient object detection via low rank matrix recovery," *CVPR'12*, pp. 853-860, 2012.
- [31] T. Judd, K. Ehinger, F. Durand, and A. Torralba, "Learning to predict where humans look," *ICCV'09*, pp. 2106-2113, 2009.