Feature based Image Authentication using Symmetric Surround Saliency Mapping in Image Forensics

Meenakshi Sundaram A.
Research Scholar
Visvesvaraya Technological University
Belgaum, India

C. Nandini
Dept. of Computer Science
Dayananda Sagar Academy of Technology and Management, Bangalore, India

ABSTRACT
For an efficient image security, image hashing is one of the solutions for image authentication. A robust image hashing mechanism must be robust to image processing operations as well as geometric distortions. A better hashing technique must ensure an efficient detection of image forgery like insertion, deletion, replacement of objects, malicious color tampering, and for locating the exact forged areas. This paper describes a novel image hash function, which is generated by using both global and local features of an image. The global features are the representation of Zernike moments on behalf of luminance and chrominance components of the image as a whole. The local features include texture information as well as position of significant regions of the image. The secret keys can be introduced into the system, in places like feature extraction and hash formulation to encrypt the hash. The hash incorporation into the system is found very sensitive to abnormal image modifications and hence robust to splicing and copy-move type of image tampering and, therefore, can be applicable to image authentication. As in the generic system, the hashes of the reference and test images are compared by finding the hamming or hash distance. By setting the thresholds with the distance, the received image can be stated as authentic or non-authentic. And finally location of forged regions and type of forgery are found by decomposing the hashes. Compared to most recent work done in this area, our algorithm is simple and cost effective with better scope of security.

Keywords
Zernike moments, Forgery detection, SHA-1, MD5 Image hash, Salient detection

1. INTRODUCTION
Due to the popularity of multimedia technology and internet, everyday more and more digital images are being created and uploaded over the internet. Managing the image database is a difficult task and moreover one cannot determine if the image already exists in a database without thoroughly searching through all the entries. There is a possibility of various computational complexity for identifying the two images of same type from the human vision e.g. an image and its watermarked version, a watermarked image and a copy attacked by software to remove watermarks, an image and its enhanced version using commercial software, an image stored using distinct transforms and an image and its compressed version. Increasing availability of digital data also led to growth in the methods to manipulate the digital multimedia. Hence many image hashing authentication techniques have been emerged to verify the trustworthiness of videos and images. Hashing is a function useful for indexing, searching. It is used to uniquely identify an entity easily by translating a big group of features into a number preferably unique. It also used to sort elements by features. In many cryptographic techniques, the data integrity is addressed by hash functions, which are depending on the encrypted key and are highly sensitive to even small alterations in the image data. As a result data or message can be easily validated. But in case of multimedia, it can allow lossy representation with small degradation. Even when the multimedia undergone moderate levels of geometric distortion, noise interruptions or filtering, media content will be retained. Hence pixel by pixel verification is not much suitable and also time consuming. Various techniques have been introduced for media specific image authentication [1][2][9-11]. The usual method of image authentication by hashes is shown in the Fig.1.

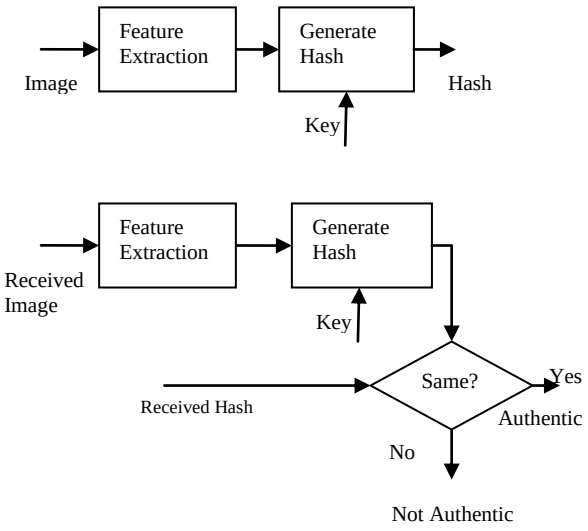


Fig 1: Normal Hashing Mechanism

According the media content uses a specific key for generating a hash from the certain features of an image. This hash is transmitted along with the image to the receiver either by appending with the data or separately. At the receiver end, the same key is used to generate the hash and which is compared with the received hash to check the validity. Given a suitable keyed image hash function hash (K, I) that authenticates using a secret key K of an image I, one can proceed as in standard cryptographic methods [6] by appending a tag of the form Encrypt (h (K; I)). In water marking, hash functions help to secure against some known attacks that use many images watermarked with the same random secret key: for an image I, use the watermarking key KI derived from a master key K by computing

$$K = message\ Digest5(MK,\ hash(K, I)).$$

In this paper, we describe a new method to develop a secure, fragile and robust image hash function the proposed method shows better performance than the methods those consider only global or local features alone. Section 2 discusses about the significant studies conducted in the past from literature viewpoint. Section 3 discusses about the essentials of moment function followed by method used for local feature extraction in Section 4. Section 5 discusses about the proposed method followed by implementation & results in Section 6. Finally section 8 concludes the paper by summarizing it.

2. PRIOR STUDIES

Usage of randomly signal processing techniques for non-reversible compression of images can be seen in the work done by Venkatesan et al. [20]. The approach was quite robust against image compression and geometric distortions. A controlled blocking strategy was introduced by Xiang et al [2], proposed by taking into consideration of effects of its rotational blocks on an image and applied non-negative matrix factorization method (NMF) hashing. In the framework discussed by Fridrich et al. [19], a robust hashing method is discussed for forgery control by using key based templates by mapping image blocks. Many prior methods are based either on global or local features [17] [18], [11] [12]. These methods have their own limitations like techniques that uses global features produces short hash but non-sensitive to the changes in the small areas in the image and local feature extraction methods are sensitive to regional modifications but produces longer hash.

Manudhane et al. [21] focused on copy move forgery detection methods that are classified mainly into two broad approaches-block-based and key-point. Methodology (generalized as well as approach specific) of copy move forgery detection is presented in detail. Copied region is not directly pasted but manipulated (scale, rotation, adding Gaussian noise or combining these transformations) before pasting.

Qershi et al. [22] described the current state-of-the-art of passive copy-move forgery detection methods. The current key issues in developing a robust copy-move forgery detector are then identified, and the trends of tackling those issues are addressed. This paper also surveyed the algorithms that were dedicated to copy-move forgery because it is the most common forgery type. For comparison purposes, one algorithm in each category was considered to represent its category.

Chang et al. [23] recognized that most permissible operations on images are global distortions like low-pass filtering and JPEG compression, whereas illegal data manipulations tend to be localized distortions. To exploit this observation, they propose an image authentication scheme where the signature is the result of an extremely low-bit-rate content-based compression.

Ahmed et al. [24] proposed a correlation-based digital watermarking technique for robust image pattern authentication. They hide a phase-based signature of the image back into its Fourier magnitude spectrum in the embedding stage. The detector computes the Fourier transform of the watermarked image and extracts the embedded signature. Authentication performance is measured by a correlation test of the extracted signature and the signature computed from the watermarked image.

Lu et al. [25] presented a new digital signature scheme which makes use of an image's contents (in the wavelet transform domain) to construct a structural digital signature (SDS) for image authentication. The characteristic of the SDS is that it can tolerate content-preserving modifications while detecting content-changing modifications. Many incidental manipulations, which were detected as malicious modifications in the previous digital signature verification or fragile watermarking schemes, can be bypassed in the proposed scheme.

Lee et al. [26] illustrated a new reversible image authentication technique based on watermarking where if the image is authentic, the distortion due to embedding can be completely removed from the watermarked image after the hidden data has been extracted. This technique utilizes histogram characteristics of the difference image and modifies pixel values slightly to embed more data than other lossless data hiding algorithm.

Singh et al. [27] discussed feature extraction of fingerprint image using canny edge detection and Prewitt edge detection. Feature Similarity Indexing of image algorithm is used to generate the matching score between the original image in the database and the input test image. The experimental results achieve recognition accuracy using canny and Prewitt FSIM of 96.77% and 97.16%, respectively, on the publicly available database of Hong Kong Polytechnic University.

Tiwari et al. [28] studied a comprehensive overview of semi fragile based image authentication techniques. In addition to a comparison based on image quality matrix, some observation is also suggested to efficiently develop an effective watermarking technique.

Swathi et al. [29] illustrated a modified digital signature scheme for image authentication has been proposed. Content-dependent structural image features and wavelet filter parameterization are incorporated into the traditional crypto signature scheme to enhance the system robustness and security. Because the proposed scheme does not require any computational overhead, it is especially suited for wireless authentication systems and other real-time applications.

Puhan et al. [30] proposed a novel method for secure, tamper localization in binary document images using erasable watermarks. For binary images, watermarking with the pixel flipping approach is a difficult task, because it can bring noticeable visual distortion. In localization, finding sufficient numbers of low-distortion pixels in a block to embed the cryptographic signature and their blind detection is more difficult. Also, an imperceptible watermark cannot be embedded in white regions of the document image, making such regions insecure against hostile attacks.

Hirakawa et al. [31] presented a user authentication method that is tolerant to attacks when a user's pass-image selection operation is video recorded twice. In addition, usage guidelines recommending eight pass-images are proposed, and its security is evaluated. This paper also discusses a user authentication method in which graphical passwords instead of alphabetic ones are used as passwords in order for it to be tolerant to observation attacks. Bhattacharya et al. [32] proposed an efficient image authentication technique by hiding handwritten signature image in selected DWT sub-band of the image. At the receiver end signature image is extracted and verified with a template signature using Artificial Neural Network and hence image authentication is achieved. Hassan et al. [33] demonstrated a new vector quantization (VQ) attack that can be applied to self-recovery image authentication. In this attack, the codebook contains authenticated blocks with their encrypted codes and displacement vector(s). Consequently, the proposed replacement procedure is used to generate a counterfeit image that can pass the verification process without triggering.

Sathik et al. [34] proposed a semi-fragile watermarking technique which embeds watermark signal into the host image in order to authenticate it. The watermark is designed so that the integrity is proven if the content of the image has not been altered and under any mild processing on the image. The watermark is generated as a binary pattern from the feature of the host image and is embedded in the high frequency sub band in the wavelet domain. Peak Signal to Noise Ratio (PSNR) and Similarity Ratio (SR) are computed to measure image quality

3. PROBLEM IDENTIFICATION

One of the biggest impediments of the standard hashing mechanism (Fig.1) is that it is not directly applicable to images. One of the prime reason behind this is application of standard hashing method considerably alters the perceptual quality of an image, for which reason, it will be easy for someone to understand whether the image is original or secured one. Not only this, for the digital images to be subjected to any security techniques (like hashing), the image has to preliminarily ensure about its compatibility and supportability towards the program using various techniques like pre-processing, scaling, compression, enhancement, color space conversion, deblurring, denoising and many more such operations. The effective hash function should always ensure about the perceptual quality of an image by generating hash values depending on the anticipated visual appearance of an image. In a nutshell, it would mean that original image as well as secured image by hash function should have similar visual quality. The length of the hash value can be maintained lower using error correcting codes while ensuring the low probability of collision. The challenge in building the hash function in our paper is that it should not be sensitive too much like SHA-1, MD5 for small changes but it should take care of malicious modification

4. MOMENT FUNCTIONS

Moment based techniques have been successfully applied to several image processing problems and they represent a fundamental tool for generating feature descriptors. Moment functions exhibit natural invariance properties such as invariance to rotation, translation or scaling. Usually Zernike moments are illustrated over a single disk thereby not affected by any sorts of rotation. Moreover, the computation of Zernike moments are quite challenging as they have quite massive dynamic ranges. Hence, representation of the global features can be effectively done by Zernike moments as they share only little information among each other. Moment functions are defined on images as the weighted sums of the image intensity function. Moment functions of order (p + q) are generally defined as

$$\phi_{pq} = \int_x \int_y \varphi_{pq}(x,y) f(x,y) dxdy \quad (1)$$

Where ψ_{pq} (x, y) is called the moment weighting kernel. For digital images in discrete notation:

$$\phi pq = \sum_x \sum_y \varphi_{pq}(x,y) f(x,y) \quad (2)$$

Some properties of the weighting kernel are passed onto the moments themselves, such as invariance features, and orthogonality. Depending on the function chosen for the weighting kernel, the calculated moments can capture different aspects of the input image. Zernike moments are defined over the unit disk instead of the real plane and exhibit the orthogonality property. Zernike moments are defined using Zernike polynomials as follows

$$Z_{p,q} = \frac{(p+1)}{\pi} \int_0^{2\pi} \int_0^1 V_{p,q}{}^* f(r,\varphi) r dr d\varphi, r \geq 1 \quad (3)$$

The Zernike polynomial $V_{p,q}(r, \varphi)$ is defined as a Zernike polynomial which is a function of the radial polynomial(Eq. 3)

$$V_{p,q} = S_{n,m}(r) e^{iq\varphi} \quad (4)$$

$$S_{n.m} = \sum_{k=m}^{n} C_{n,m,k} r^k \quad (5)$$

$$Cn,m,k = \frac{(-1)^{n-k}(n+k+1)!}{(n-k)!(k+m+1)!(k-m)!} \quad (6)$$

The manipulated version of the Zernike moment can be considered as Pseudo-Zernike moments that posses around double of moments of the order (p + q) compared to conventional Zernike Moments. It is to be noted that both the versions share the similar orthogonality property permitting the robust recovery of the original image data. Not only this, but Pseudo-Zernike moments also exhibits better noise sensitivity as well as optimal control of error rate. They inherit the same orthogonality property, but instead of the radial polynomials pseudo Zernike moments use the following.

Where n=0, 1, 2…, $0 \leq |m| \leq n$, N-|m| i.e. even. If α is a rotational angle, $Z_{p,q}^{(r)} = Z_{p,q} e^{-jm\alpha}$

Thus, the magnitude of Zernike moment is rotation invariant, only phase changes with angle of rotation

$$\arg(Z_{p,q}^{(r)} = \arg(Z_{p,q}) - m\alpha \quad (7)$$

The proposed system uses Zernike moment as one of the media to ensure security of the image. The system adopts cost efficient hashing technique which gives better performance.

5. LOCAL FEATURES EXTRACTION

Identifying visually salient regions is useful in applications such as object based image retrieval, adaptive content delivery, adaptive region-of-interest based image compression, and smart image resizing. According to information theory, effective coding decomposes the image information into Innovation and prior knowledge.

I (image) = I (innovation) +I (Prior Knowledge)

Innovation denotes the novel part and prior knowledge is the redundant information which is not used in effective coding and hence it should be suppressed. Log spectrum of an image, is used to represent general information of the image. Log spectrum is obtained by L(f)=log(A(f)), where A(f) denotes the general shape of log spectra. The information required to be processed is given by

$$H(R(f)) = H(L(f) \mid A(f) \quad (8)$$

Where R(f) represents the spectral residual of the image. The spectrum average A(f) is obtained by convolving the input image with the log spectrum

$$A(f) = h_n(f) * L(f) \quad (9)$$

The spectral residual is obtained by

$$R(f) = L(f) - A(f) \quad (10)$$

Finally Inverse Fourier Transform is applied which gives the saliency map.

$$S_m(x) = \Im^{-1}(R(f)) \quad (11)$$

5.1 Texture Features

Texture of an image is a set of metrics like contrast, coarseness, directionality, regularity line-likeness roughness etc calculated to quantify the perceived texture of an image. It is an important feature to human visual perception. Here we are considering coarseness, contrast, skewness and kurtosis to describe texture features. To evaluate coarseness around a pixel at (x, y), the pixels in its neighborhood sized 2kx2k are averaged

$$C_k(x,y) = \frac{1}{2^{2k}} \sum_{1=x-2^k}^{x+2^k-1} \sum_{j=y-2^k}^{y+2^k-1} g(i,j), k = 0,1,....,5 \quad (12)$$

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

$$E_{k,h}(x,y) = | A_k(x+2^{k-1}, y) - A_k(x-2^{k-1}, y) | \quad (13)$$

$$E_{k,v}(x,y) = | A_k(x, y+2^{k-1}) - A_k(x, y-2^{k-1}) | \quad (14)$$

$$S(x,y) = \arg_{k=0,..5} \max_{d=h,v} E_{k,d}(x,y) \quad (15)$$

Contrast describes the degree of image brightness variation, calculated from variance and the fourth-order moment μ4of the gray values within the region

$$C = \sigma^2 \mu_4^{-4} \quad (16)$$

The measure of asymmetric in the distribution is called skewness and it is given by

$$Skew = \sum \frac{(\frac{x-\bar{x}}{\sigma})^3}{n} \quad (17)$$

Kurtosis the sharpness of the peak of a frequency-distribution curve

$$Kurtosis = \frac{\sum (X-\mu)^4}{N\sigma^4} - 3 \quad (18)$$

6. PROPOSED METHOD

In this section, proposed hashing scheme is described. . Our proposed method is based on the global and local features of the image. The image's global features are calculated by using Zernike moments from the luminance and chrominance components. We extract the local texture features such as contrast, coarseness, skew and kurtosis from the salient regions in the image, which represents the image contents in the corresponding areas. Degree of tampering or similarity between the two hashes is measured by calculating the Euclidian distance. Thresholds are used to decide whether the image is normally processed or maliciously altered one of the original. Location of the tampered regions and the type of tampering like replacement, addition, removal, abnormal color modification etc can be done by using local features. The outcome shows that the proposed method generates a short hash with good performance. Zernike moments are used to characterize global features and texture features of salient regions are evaluated using the equations. Finally hash is constructed using both. Elaborations of the significant steps involved in the proposed system are discussed below:

6.1 Hash Generation

The image is rescaled to a specific size in order to make sure that generated hash has a fixed length with bilinear interpolation and converted from RGB to YCbCr. Luminance and chromium components are separated and are used to form the hash.

6.1.1 Global Feature Extraction

Zernike Moment for Y and CbCr components are calculated. We choose order $n=5$ and repetition $m \geq 0$ and we don't consider $Z_{0,0}$ since it represents average intensity. Absolute values or magnitudes of *ZM* are rounded off and as shown in table 1, we get overall 11 *x* 2=22 Zernike moments and form a global vector Z'= [Z_Y Z_C].

Table 1: ZM of an image for different orders *n*

Order *n*	ZM	No. of Moments
1	$Z_{1,1}$	1
2	$Z_{2,0}$, $Z_{2,2}$	2
3	$Z_{3,1}$, $Z_{3,3}$	2
4	$Z_{4,0}$, $Z_{4,1}$,$Z_{4,2}$	3
5	$Z_{5,1}$, $Z_{5,3}$, $Z_{5,5}$	3

6.1.2 Local Features of Salient Regions

Prominent regions are detected from component Y and co-ordinates of top left corner(x, y), width and height of the bounding box are used to form a vector P which consists of 24 integers, it gives the position of salient regions on the image. For each salient region, the computation is carried out on the coarseness C_1, contrast C_2, kurtosis and skewness are evaluated and placed in a vector T, it is also of 24 integers. If number of salient regions is less than six, the position and texture vectors are filled with zeros. Finally forms a local feature vector S= [P T].

6.1.3 Hash Construction

From local feature vector S and global feature vector Z vectors, final hash is constructed H= [Z S] which of length 560 bits (70 integers) because all integers will be in range of [0 255].

6.2 Image Authentication

In this, the hash of the reference image is available and the hash of the image to be tested is found out by above method. These two hashes are compared; so that if both are same then two images have same contents else received image is tampered one. First the hashes are decomposed into global and local feature vectors. The position P vectors are used to check the matching of salient regions. If the salient regions areas are approximately equal, then they are considered as being matched.

Here we use the hash distance as a metric to judge the similarity or dissimilarity between the two images. The global features represented by ZM are sufficient enough to differentiate similar from dissimilar [ ]. Euclidian distance between the Z_1 and Z_0 gives the hash distance.

$$D = \| Z_1 - Z_0 \| \quad (15)$$

If hash distance D is less than the threshold τ_1, the images are considered as alike otherwise images are dissimilar. Also we need to know whether the test image is a manipulated one of the trusted one. For that, compare the distance with the second threshold τ_2. If $D \geq \tau_2$, test image is completely a different one else it is decided as tampered version of trusted image. The proposed study considers threshold τ_1 that is taken as 7 and τ_2 =50 to distinguish similar, different and forged images.

The next step after finding the hash distance is to locate the tampered region. For this we use the number of matched salient regions. If any of the salient regions is not matched with the corresponding salient region, then the region is considered as being tampered. The nature of tampering can be insertion, removal or replacement of objects. The unusual color changes in the image can be detected by checking the luminance and chrominance components in the Zernike moments by calculating the Euclidian distance for Y and CbCr components. If $\Delta Z_C - \Delta Z_Y \geq 5$, then it is judged as test image contains substantial color changes with respect to the original image.

7. IMPLEMENTATION & RESULTS

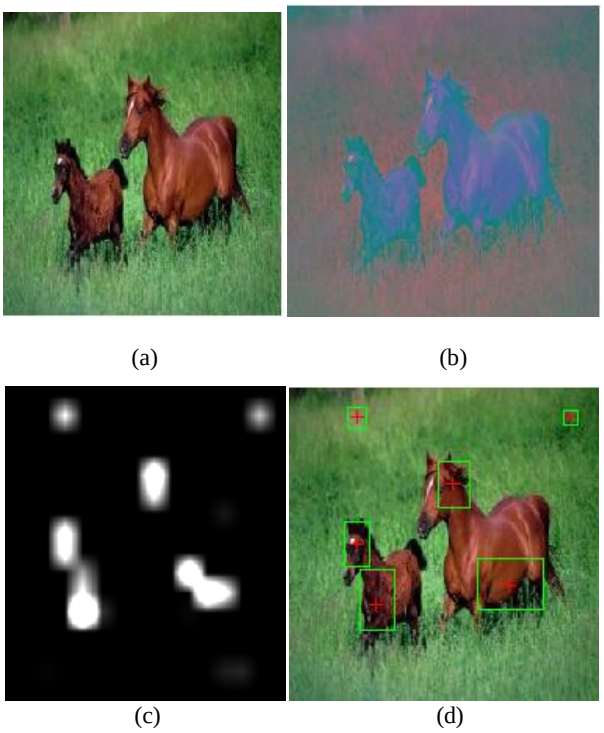
The proposed system is implemented using Mat lab environment using the normal personal computing device. The data set is considered from image forgery database CASIA [35]. The complete algorithm for image authentication using proposed method is given below.

Algorithm: Detection of Forgery in Image using symmetric surround
Input: Images

Output: Hash distance, Salient map, Forged region

START

1. Read the image & Resize to [256 256].
2. Covert from RGB to YCbCr.
3. Separate Luminance & Chrominance components
4. Calculate ZM for Y & CbCr components.
5. Form a vector ZM= [ZY ZC]
6. Find the saliency regions
7. Position P=[x y width height]
7. For i=1:No. of salient regions
8. Find T= [C1, C2, Skew, Kurtosis]
9. End
10. Form a vector S= [P T]
11. Hash H= [ZM S]
12. Follow above steps for original image to find H'
13. Calculate hash distance D=|Z-Z1|
14. Match salient regions.
15. Locate forged regions
16. ***END***

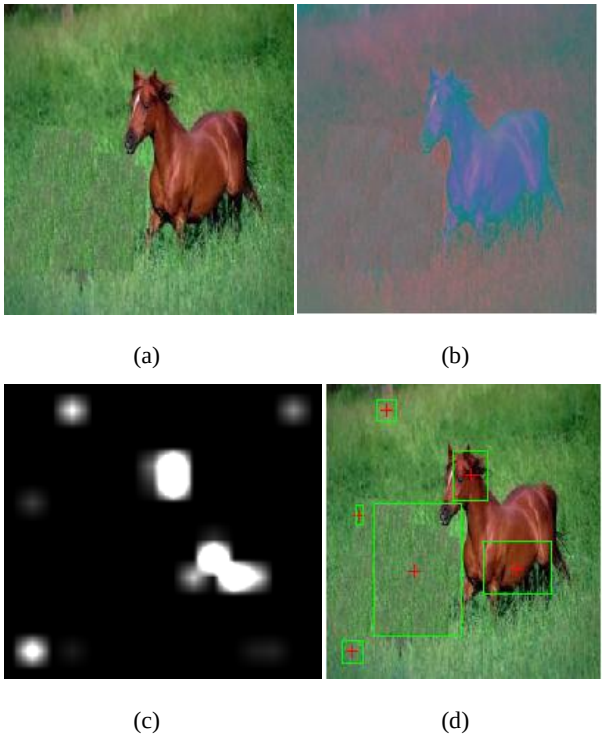


(a) (b)

(c) (d)

Fig 2: Processing Original Image

Fig 2(a) highlights original image whereas Fig.2 (b) represents YCbCr color space, while Fig.2(c) represents salient regions and Fig.2 (d) shows bounding boxes around salient regions.



(a) (b)

(c) (d)

Fig 3: Processing of Test Image

Fig.3 (a) represents original test image. Here test image basically means the input image which is to be tested for authentication. Fig.3 (b) represents YCbCr colorspace, Fig3(c) represents salient regions, while Fig.3 (d) represents bounding boxes around the salient regions of the test image.

Fig 4: Location of Forged Region

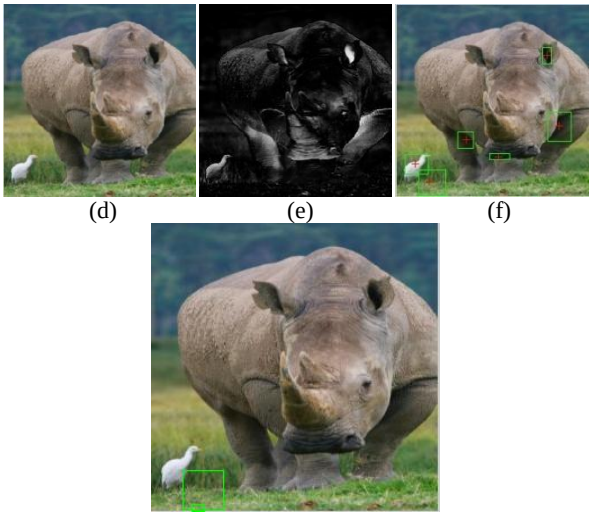
Figure 4 exhibits the location of the forged regions for the test image. Here, the system considers spectral residual approach for salient region mapping. The existing method available for saliency maps suffers from limitations affecting the perceptual quality of an image. Therefore, it can be seen that outcome of the saliency region as exhibited in Fig.2(c) and Fig.3(c) are visually not perceptible for which reason it may render the hash operation vulnerable for attacker. Hence, the proposed system makes use of maximum symmetric surround approach for obtaining much better perceptual quality of an image as exhibited below.

(a) (b)

Fig 5: Saliency mapping using symmetric surrounds

Figure 2 shows the original image and its saliency map using spectral residual approach. The above outcome shows that saliency mapped image in Fig.5 (b) is well resolution image as compared to Fig.2(c) and Fig3(c).

(a) (b) (c)



(d) (e) (f)

Fig 6: Final detection of forged region

Fig.6 discusses the similar implementation of symmetric surround approach in different image sets, where Fig 6(a) (b) (c) shows original image, saliency mapping, and detected salient regions respectively. Fig.6 (d) (e) (f) represents original image, saliency mapping, and detected salient regions respectively for test image. It can seen that the detection performance is quite uniform as well as the saliency mapping image is quite visibly perceptible.

(a) (b)

Fig 7: Analysis considering Color Modification

The proposed system is also evaluated for color modification as exhibited in Fig.7, where Fig.7 (a) represents original image while Fig.7 (b) shows the malicious color modification of the original image. The better performance of the proposed image hashing technique is basically due to the combination of both global and local features. The former reflect the overall structure of the image and rotational invariance, and the latter, based on content saliency, that are used to identify and characterize changes in perceptually significant regions.

8. COMPARATIVE PERFORMANCE ANALYSIS

For the purpose of performing comparative analysis for understanding the effectiveness of the outcomes, the proposed system considers the work done by Zhao et al. [36]. The prime purpose of selecting [36] is because of resemblance of the problems. The author of [36] has used the similar technique like us but was more focused on performing authentication using image hashing technique. The advantage of such approach is that if there are any minor difference between the original image and forged (or query) image, the framework becomes too sensitive to detect the hash distance based on featured vector as well as reshuffled feature vector.

However, there is also one pitfall of the approach. As the framework was evaluated on colored image, so the hash used by the author has become around 560 bits long. Hence, there is a wide scope of optimization by choosing saliency map in spite of constructing hash image using sector keys. The algorithm discussed in the paper doesn't use any secret key for which reason sufficient storage complexity is reduced. Saliency map is introduced for the purpose of identifying the forged region of the queried image

In order to understand the effectiveness of our approach, parametric model is used to illustrate the fact. A parametric modelling is done with outcome of ROC curve as shown in Fig.8. The model takes the input of a column vector with lower / higher values of saliency feature (say *x* and *y*), a scalar value, and number of bootstrap samples for the purpose of inferring the ROC curve. It is also set 95% confidence interval for the area under curve of the ROC curve, partial area, and empirical ROC value itself. Hence, we have two values Zernike moments of original as well as forged image. Hence, if Zhao et al. [36] approach is applied, the empirical ROC is found with smooth increase in True Positive Rate identification with respect to False Positive Rate. However, as our approach are more based on moments and saliency map, which doesn't have to perform extra computation for key management, hence, the result witnesses both local and global optimization with respect to ROC curves. Hence, Fig.7 exhibits better scope of ROC curve of proposed system with respect to Zhao's et al. study. The outcome has also exhibited the value of area under curve for parametric approach to be 0.754, partial area under curve value of 0.176, and empirical value of area under curve is found to be 0.760. There values differs with the changes in the images, however, the means are very close to these values.

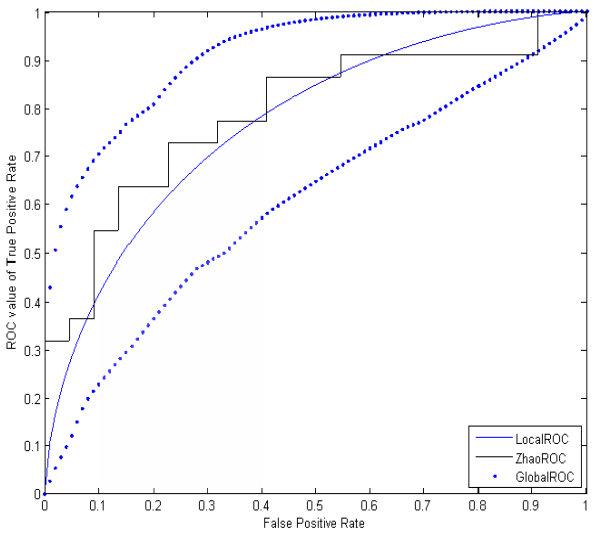


Fig 8 ROC analysis of the proposed system

The comparative analysis of true positive rate (TPR) is exhibited in Fig.9. A simple technique to evaluate the effectiveness of TPR using ROC curves is used. Analysis of positive predictive value (Fig.10) is also performed for evaluating the classifier designed using saliency map.

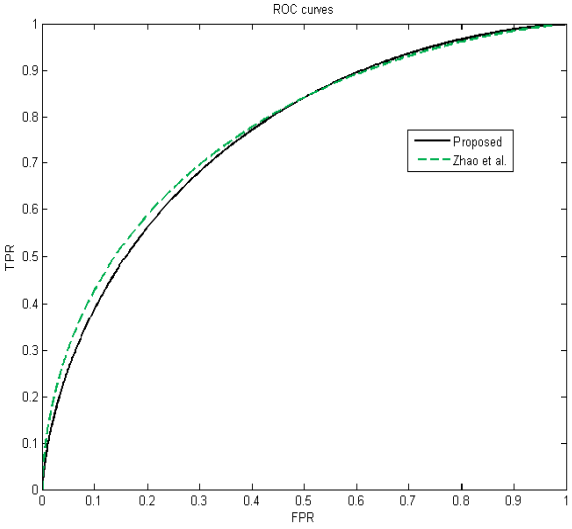


Fig 9: Comparative analysis of TPR

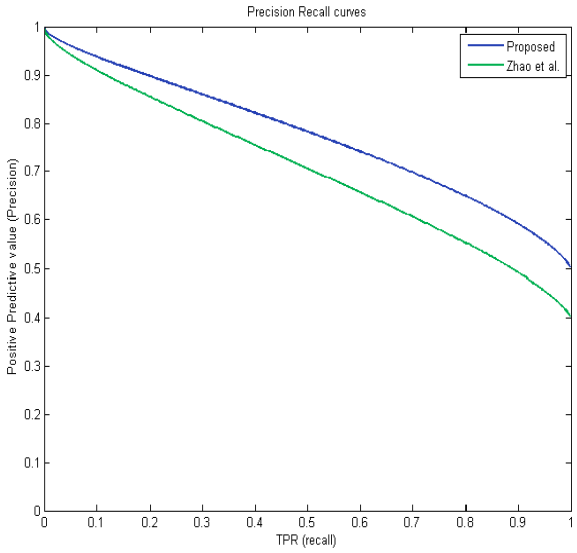


Fig 10: Comparative Analysis of Precision-Recall

100 number of prediction are considered with α (fraction of positive result) as 0.4, μ_{-ve} & σ_{-ve} of -1 and 2while μ_{+ve} & σ_{-ve} was considered as 1 and 2. (μ & σ is mean and standard deviation). The system generates the classifier output and computes all the empirical curves for both using hashing (Zhao et al. [36]) and without using hashing (proposed). Interestingly, it can be seen that there is no statistical significant difference between the TPR of proposed and Zhao et al approach, which means the proposed systems performs the same mechanism with less computational complexity. In case of precision also, it can be seen that with the increase of TPR (recall), proposed system has considerably better precision as compared to Zhao et al [36] approach.

The next set of evaluation is performed to understand time complexity. The average time for the Zhao et al. [AR] approach was found to be 2.7 seconds, whereas, the proposed system gives the average time as 0.38 seconds. Hence, the technique adopted in the proposed study has some obvious benefits with respect to time and space complexity. The prime reasons behind this are as follows-the proposed system performs decomposition of the original image into more dense and perceptual uniform elements that abstracts the unwanted pixel (memory) elements. Depending on such abstraction, the

system evaluates the estimates of contrast using Zernike moment that scales the uniqueness as well as spatial distribution (distance) of such moments. From the moment's perspective, the system performs applying saliency map that generates the pixel-accurate saliency map, much better than what Zhao et al. [36] has used. This fact homogeneously encapsulates the region of interest and spontaneously performs discretion of foreground and background. The proposed technique is completely based on empirical approach of decomposing an original image into fundamental and matrix correlated depiction of moments for filtering the unwanted pixel element and finding the accurate region of forgery.

Therefore, the prime aspect of the proposed technique is that it is extremely simple, lightweight, and doesn't need to store any information in run-time, which also brings higher level of security. The approach of Zhao et al. [36] has key management, which needs to be stored and used; however, we don't need to store any keys. Hence, our approach is simpler and thereby lightweight. Our system derives a saliency map from the Zernike moments based on spatial distribution of the moments. The system is also capable of handling local and global features for better identification rate, which cannot be performed using Zhao et al. [36].

Table 2: Analysis of Time Complexity

Items	Tiger1	Tiger2	Castle	Horse	Cow	Golf	Rhino
For Reading original image	0.097784	0.103656	0.213086	0.100774	0.141220	0.129067	0.156637
For converting to YCbCR	0.030014	0.031204	0.030968	0.031196	0.032355	0.037131	0.031327
Applying Zernike moment	0.739939	0.740918	0.738799	0.741316	0.777076	0.835394	0.755254
For applying Saliency map	0.946148	1.004534	1.117661	1.091698	1.079293	0.959500	1.062611
For Reading forged image	0.017624	0.017590	0.018862	0.016870	0.195484	0.030146	0.116733
For converting to YCbCR	0.011180	0.011390	0.011467	0.011272	0.011216	0.011649	0.011177
Applying Zernike moment	0.710150	0.711044	0.712213	0.710354	0.768328	0.778250	0.709878
For applying Saliency map	1.190489	1.176621	1.126229	1.293935	1.214819	0.634547	0.812133
Computing distance	0.000069	0.000070	0.000738	0.000070	0.000086	0.000089	0.000087
Detection of forged area	0.000001	0.000001	0.000003	0.000001	0.000001	0.000001	0.000001
Mean Processing Time	0.37434	0.379703	0.397003	0.399749	0.421988	0.341577	0.365584

9. CONCLUSION

In this work, an image hashing method that can be used for image forgery detection is presented. It uses both the local and global features of an image. The latter one is based on the complex Zernike moments representing the chrominance and luminance characteristics of the image. Similarly local features include position and textures features of each salient region of the image. In our experiments, image hashes were robust to various attacks like small angle rotation, brightness adjustment, copy-move, splicing and resilient to content-preserving modifications. And hence it can be used differentiate various types of forgery as well as for finding the location of forgery. Also proposed produces reasonably short hash and good performance for both common image processing and malicious distortions. In future, better salient region detection method can increase the accuracy of the proposed method and could better represent the image contents and hence can enhance the hash's sensitivity for accurate tampering detection.

10. REFERENCES

[1] Swaminathan,A., Mao,Y., Wu, M.2006. Robust and Secure Image Hashing. IEEE transaction On Info. Forensics and Security. Vol.1, No, 2, pp.215-230

[2] Xiang, S., Yang, J.2012. Block-Based Image Hashing With Restricted Blocking Strategy For Rotational Robustness. EURASIP Journal on Advances in Signal Processing

[3] Kasza,P.2009. Pseudo-Zernike Moments for Feature Extraction and Chinese Character Recognition. IEEE International Conference on Computer Automation & Engineering

[4] The, C.H., Chin, R. T.1988. On Image Analysis By The Methods Of Moments. IEEE Transactions on Pattern Analysis and Machine Intelligence. Vol.10, Iss.4, pp:496–513

[5] Hou,X., Zhang, L.2007. Saliency detection: A Spectral Residual Approach. Proc. IEEE Int. Conf. Computer Vision and Pattern Recognition, Minneapolis, pp. 1–8

[6] Achanta,R., Susstrunk,S.2007.Saliency Detection Using Maximum Symmetric Surround. International Conference On Computer Vision Systems

[7] Tamura,H., Mori,S., Yamawaki, T.1978. Textural Features Corresponding To Visual Perception. IEEE Trans. Syst., Man, Cybern. Vol. 8, No. 6, pp. 460–472

[8] Zhao,Y., Wang, S., Zhang, X., Yao, H.2013. Robust Hashing for Image Authentication Using Zernike Moments and Local Features. IEEE Transactions On Information Forensics And Security, Vol. 8, No. 1

[9] Ahmed,F., Siyal, M. Y., Abbas, V. U.2010. A Secure And Robust Hash Based Scheme For Image Authentication. Signal Process. Vol. 90, No. 5, pp. 1456–1470

[10] Tang, Z., Wang, S., Zhang, X., Wei, W., Su, S.2008. Robust Image Hashing For Tamper Detection Using Non-Negative Matrix Factorization. Journal of Ubiquitous Convergence Technol. Vol. 2, No. 1, pp. 18–26

[11] Monga,V., Mihcak, M. K.2007. Robust And Secure Image Hashing Via Non-Negative Matrix Factorizations. IEEE Trans. Inf. Forensics Security. Vol. 2, No. 3, pp. 376–390

[12] Fouad, K., Jianmin, J.2010. 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

[13] Tang, Z., Wang, S., Zhang, X., Wei, W., Zhao, Y.2011. Lexicographical Framework For Image Hashing With Implementation Based On DCT And NMF. Multimedia Tools Applicat., Vol. 52, No. 2–3, pp. 325–345

[14] Ahmed,F., Siyal, M. Y., Abbas, V. U.2010. A Secure And Robust Hash based Scheme For Image Authentication. Signal Process, Vol. 90, No. 5, pp. 1456–1470

[15] Lv,X., Wang, Z. J.2012. Perceptual Image Hashing Based On Shape Contexts And Local Feature Points. IEEE Trans. Inf. Forensics Security. Vol. 7, No. 3, pp. 1081–1093

[16] Mihçak,M.K., Koval,O., Voloshynovskiy, S.2007.Robust Perceptual Hashing Of Multimedia Content. EURASIP, Special

[17] Tang,Z., Wang, S., W.Wei, X, Su,S.2008. Robust image hashing for tamper detection using non-negative matrix factorization. Ubiquitous Convergence Technol., Vol. 2, No. 1, pp. 18–26

[18] Swaminathan., Wu, M.2006. Robust and secure image hashing. IEEE Trans. Inf. Forensics Security

[19] Fridrich,J., Goljan, M.2000. Robust hash functions for digital watermarking. Proc IEEE International Conf Information Technology: Coding Computing, Las Vegas, NV , USA, pp. 178–183

[20] Venkatesan, R., Koon, S.M.1999. Robust image hashing into binary strings. manuscript

[21] Manudhane, K., Bartere, M.M.2013. Methodology for Evidence Reconstruction in Digital Image Forensics. Computer Engineering and Intelligent Systems. Vol.4, No. 13

[22] Qershi, A., Osamah, M., Khoo. B.E.2013.Passive detection of copy-move forgery in digital images: State-of-the-art. Forensic science international, Vol. 23, No. 1, pp. 284-295

[23] Chang,E-C., Kankanhalli, M.S., Guan, X., Huang, Z., Wu, Y.2003. Robust image authentication using content based compression. Multimedia Systems, Vol. 9, No. 2, pp. 121-130

[24] Ahmed,F.,Moskowitz. I.S.2004.Correlation-based watermarking method for image authentication applications.Optical Engineering, Vol. 43, No. 8, pp.1833-1838

[25] Lu,C-S., Liao, H-Y.M.2003.Structural digital signature for image authentication: an incidental distortion resistant scheme. Multimedia, IEEE Transactions, Vol. 5, No. 2, pp. 161-173

[26] Lee, S-K., Suh, Y-H., Ho, Y-S.2006. Reversible Image Authentication Based on Watermarking. IEEE International Conference In Multimedia and Expo,, pp. 1321-1324

[27] Singh, H.A., Gayathri, R.2012. Image Authentication Technique Using Fsim Algorithm. International Journal of Engineering Research and Applications (IJERA), Vol.2, No. 2, pp. 1129-1133

[28] A.Tiwari, M.Sharma, "Semifragile Watermarking Schemes for Image Authentication- A Survey", *International Journal of Computer Network and Information Security*, Vol.2, pp. 43-49, 2012

[29] SriSwathi, K., Krishna, S.G.2011.Secure Digital signature scheme for Image authentication over wireless channels. International Journal of Computer Technology and Applications, Vol.2 (5), pp. 1472-1479

[30] Puhan, N.B., Ho, A.T.S.2005. Secure tamper localization in binary document image authentication. In Knowledge-Based Intelligent Information and Engineering Systems, Springer Berlin Heidelberg, pp. 263-271

[31] Hirakawa, Y., Take, M. , Ohzeki. K.2011. Pass-image authentication method tolerant to video-recording attacks. Computer Science and Information Systems (FedCSIS), Federated Conference, pp. 767-773

[32] Bhattacharya, T., Hore, S., Chaudhuri, B.2012.An Image Authentication Technique by Handwritten Signature Verification using DWT and ANN. International Journal of Computer Applications. Vol. 47(21)

[33] Hassan, A. M.., Hasan, M. Y., Wahab, M. A. A.2012. A New Vector Quantization Attack on Self-Recovery Image Authentication.Second International Conference on Communications and Information Technology

[34] Sathik, M.M., Sujatha, S.S.2012. Authentication of Digital Images by using a semi-Fragile Watermarking Technique. International Journal of Advanced Research in Computer Science and Software Engineering.Vol.2, Issue.11

[35] http://forensics.idealtest.org:8080/

[36] Zhao, Y., Wang, S., Zhang, X., Yao, H.2013. Robus1t Hashing for Image Authentication Using Zerbike Moments and Local Features. IEEE Transaction on Information Forensics and Security, Vol.8, No.1