Development and Calibrating Features for Digitally Forged Image Authentication

D. Subitha Priyadharshini[1], P. Maya[2]

[1, 2]BSA University, Vandalur, Chennai, India

Abstract: ***Nowadays image forgeries are done in many ways using software tools. To avoid the image forgery a hash method is been developed which has three secret keys. It is also used to detect image forgery including insertion, removal, object replacement, abnormal colour modification and locating forged areas. Hash values are developed by concatenating local features and global features. For more security skin based biometric values are added with the hash construction. A test image is compared with the hash of a reference image to find whether the image is similar or forged. A network called triple key chaotic neural network is implemented and it's a versatile network to make the image secure. And the image will be retrieved and restored.***

Keywords: robust hashing, forgery detection, skin based biometrics, chaotic neural network

1. Introduction

With the multimedia technology development, most of the people use various image editing software tools to change the image for different purposes. So, to differentiate from original and fake images users find it difficult. Image authentication techniques are developed recently. One of the most important techniques is image hashing. It is very sensitive while any changes are done. Image hashing is a technique that extracts short sequence in image to represent its content. And therefore can be used for image authentication.

2. Feature Extraction

In feature extraction stage each character is represented as a feature vector, which becomes its identity. The major goal of feature extraction is to extract a set of features, which maximizes the recognition rate with the least amount of element.

A. Zernike Moments

In general, moments describe numeric quantities at some distance from a reference point or axis.

- Moments produced using orthogonal basis sets.
- Set of orthogonal polynomials defined on the unit disk.

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

- Simply the projection of the image function onto these orthogonal basis functions.

$$A_{nm} = \frac{m+1}{\pi}\int_x\int_y f(x,y)[V_{nm}(x,y)]^* \, dx \, dy$$

$$\text{where } x^2 + y^2 \leq 1$$

Where |Anm| and φnm represent the magnitude and phase, respectively. In the magnitude remains unchanged while the phase would change with image rotation. Therefore, many applications use ZM magnitude alone as rotation in variant image features. Since the phase component captures much information of the original image, any ZM-based image features without the phase information could have relatively weak descriptive effectiveness. In fact, the phase component may even contain more content information than the magnitude.

B. Saliency Region

A salient region in an image is one that attracts visual attention. According to [17], information in an image can be viewed as a sum of two parts: that of innovation and that of prior knowledge .The information of saliency is obtained when the redundant part is removed.

Figure 1: Reference image

Figure 2: Saliency map

Figure 3: Saliency threshold map

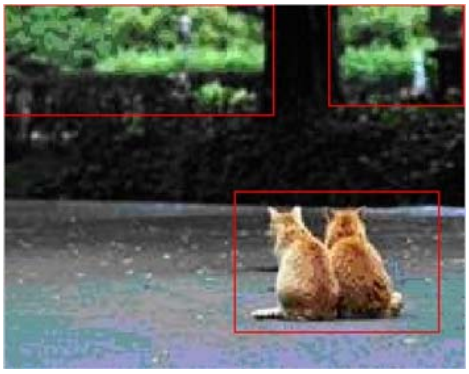


Figure 4: Saliency region marked with circumscribed rectangles

C.Texture Features

Texture is an important feature to human visual perception. In [18] and [19], the authors propose six texture features relating to visual perception: coarseness, contrast, directionality, line-likeness, regularity and roughness. Here coarseness, contrast, skewness and kurtosis are used.

3. Biometric Key Values

(Merriam-Webster online): the statistical analysis of biological observations and phenomena. Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic.

a) Phenotypic biometric – based upon features or behaviors that are acquired through experience and development.
b) Genotypic biometric – based upon genetic characteristics or traits.

Biometric values are used in different technologies. They are;

a) Fingerprint
b) Voice
c) Iris/retina
d) Gait
e) Face Recognition

Face Recognition Techniques

I. Image Based

a) Statistical based on O(2nd)
b) Template matching

Figure 5: Original image

II. Feature Based

a) Geometric
b) Feature metrics (spatial relationships)
c) Morphable models (shape/texture)

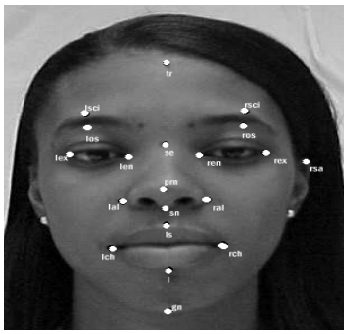
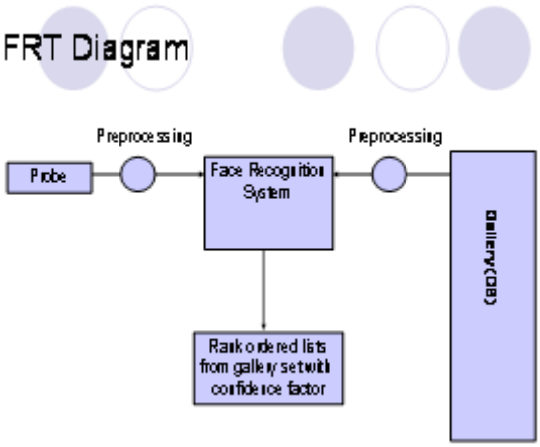


Figure 6: Face detection



4. Proposed Hashing Scheme

In this section, we describe the proposed image hashing scheme and the procedure of image authentication using the hash. The hash is formed from Zernike moments to represent global properties of the image, and the texture features in salient regions to reflect local properties.

A. Image Hash Construction

The image hash generation procedure includes the following steps;

Pre-Processing: The image is first rescaled to a fixed size with bilinear interpolation, and converted from RGB to the YCbCr representation. Y and 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 computation complexity.

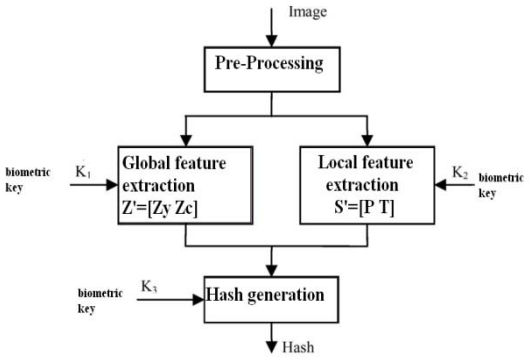


Figure 7: Block diagram of the proposed image hashing method

B. Image Authentication

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. 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. In this case, we say the two images are perceptually the same, or similar. The image authentication process is performed in the following way.

1. Feature Extraction: Pass the test image through the steps as described in Section A to obtain the intermediate hash without encryption, namely.
2. 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 sub vectors in and may either be Matched or unmatched. The vectors and are reshuffled accordingly.
4. Distance Calculation and Judgment: 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, namely. The vector does not contribute to the distance calculation but will be used to locate forged regions. The hash distance between the test image and the reference is the Euclidean distance between and for a pair of similar images; 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. 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.

C. Forgery Classification and Localization

Having found that a test image is a fake, the next job is to locate the forged region and tell the nature of forgery. Four types,

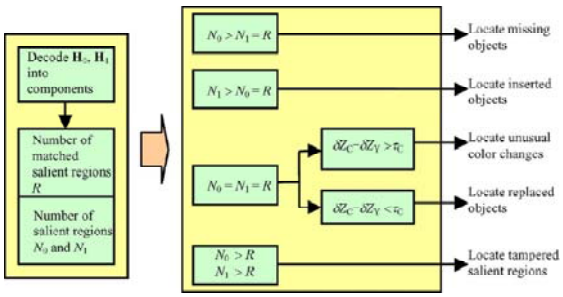


Figure 8: Forgery classification and localization

1. If, some objects have been removed from the received test image, Positions of the missing objects are located by comparing the saliency indices.
2. If, the test image contains some additional objects whose positions are located by comparing the saliency indices.
3. If, check the luminance and chrominance components in the Zernike moments and calculate the following distances: If is greater than by a threshold, the test image contains substantial colour changes with respect to the reference image while the luminance changes are considerably smaller.
4. If and is less than, the test image contains replaced objects because in this case, luminance changes are dominant. Calculate the distance between the texture feature vectors of each salient region, the salient region having maximal is recognized as being replaced.

5. If and, some of the salient regions are not matched. Mark the mismatched salient regions in the test image as being tampered.

5. Chaotic Neural Network

The meaning of chaos is not generally accepted but from a practical point of view chaos can be defined as bounded steady stat behaviour that is not equilibrium point not periodic and not quasi periodic. It is a random and look like a noise but deterministic. Chaotic systems are non periodical sensitive to initial conditions, system parameters and topological transitivity. These properties are also remarkable for cryptanalysts. Noise like behaviour of chaotic system is main reason of using this system in cryptology. Chaotic spectrum does not have discreet frequencies but has a continuous, broad band nature. Chaos signals are considering better for practical because of its characteristics above mentioned. Field of information security is nothing but the combination of two concepts that are cryptography and chaos theory. A network is called chaotic neural network if its weights and biases are determined by chaotic sequence. It is a stochastic behaviour occurring in deterministic system. In this, we consider the Hopfield neural networks which exhibit chaotic phenomenon.

x’ (t)= – Cx(t) + Af (x(t)) + Bf(x (t –_(t)) + I (1)
x’i(t)= -cixi(t) + _ajfi(xi(t)) +_ bj fj(xj(t-_j(t))) + Ii,
i=1, 2, 3……n

Where, n denotes the number of units in a neural network. Pseudorandom number sequences with good properties are frequently used in secure communications and cryptosystem. Iterative equations are used to generate the chaotic dynamics. Computation time for encryption and decryption depends on complexity of equations and value of state variables. If complexity of equation is low, computation time for encryption and decryption will be less otherwise it will take long time for computation. If the equation is with lower complexity then discrete map have to preferred, it involves basic arithmetic operation like addition, subtraction, multiplication and division. On the other hand, if the behaviour of chaotic equation is continuous in nature, it involves differential or integral operations to calculate value of the next state variable. Complexity of equation is low, computation time for encryption and decryption will be less otherwise it will take long time for computation. If the equation is with lower complexity then discrete map have to preferred, it involves basic arithmetic operation like addition, subtraction, multiplication and division. On the other hand, if the behaviour of chaotic equation is continuous in nature, it involves differential or integral operations to calculate value of the next state variable. From complexity point of view, integral value of the state variable is preferred because it takes shorter time for computing next state variable, if it is floating point then takes longer time for computation.

A. Secret Keys

Cryptography is the exchange of information among the users without leakage of information to others. Much public key cryptography is available which are based on number theory but it has the drawback of requirement of large computational power, complexity and time consumption during generation of key. To overcome these drawbacks, a neural network can be used to generate secret key. Many methods use chaotic neural network for cryptography here in this paper ‘Triple key’ is using in the network to encrypt and decrypt the data. Three different parameters which are decided by user are used to scramble the image data and so hackers get many difficulties to hack the data hence providing more security. For simulation MATLAB software is used. The experimental results shows that algorithm successfully perform the cryptography and highly sensitive to the small changes in key parameters.

B. Triple Key Chaotic Neural Network

In triple key chaotic encryption method, 20 hexadecimal characters are entered as a session key. The finalisation of this hexadecimal key gives 80 bits. Some bits are extracted and some manipulations are performed on it to obtain the intermediate key. This intermediate key is combined with initial and control parameters to generate chaotic sequence. This is the concept of ‘Triple key’. In this, there is three step protections to the original image. User has to enter three keys to decrypt the image.

6. Algorithm

1. Read the image.
2. Determine the size and length of image.
3. Converting two dimensional image vector in one dimensional image vector.
4. Computing initial parameter from hexadecimal session key, A=a1a2a3…a20. It consists of 80 bits i.e. binary representation of hexadecimal key.
5. X (1) = (s1+s2+s3) mod 1.
   Where, s1= (a71*2^0+….a84*2^7+a124*2^23)/2^24
   s2= (a13+a14+….a18)/(16*6)
   s3= entered
6. Determine parameter μ.
7. Generate the chaotic sequence x (1), x (2), x (3)…..
   X (M) by the formula
   X (n + 1) = mx(n) (1 – x(n))
   Create b (0), b (l)... b (8M – 1) from x (l), x (2) ... x (M) by the generating scheme that
   b (8m – 8)b(8m – 7)….. b (8m – 2) b(8m – l) … is the binary Representation of x(m) for m = 1, 2….M.
8. Weights and theta are decided
   for n = 0 to M – 1
   For i = 0 to 7
   j={0, 1, 2, 3, 4, 5, 6, 7}
   End
   For i = 0 to 7
   where f(x) is 1 if x >=0`
   End
   End

7. Simulation Results

1. Input Image

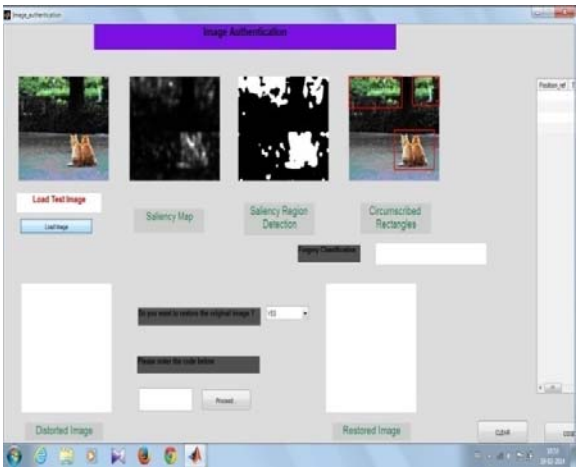


Figure 9: Reference input image

Figure 8 states about the input reference image given for operation.

2. Input Forged Image

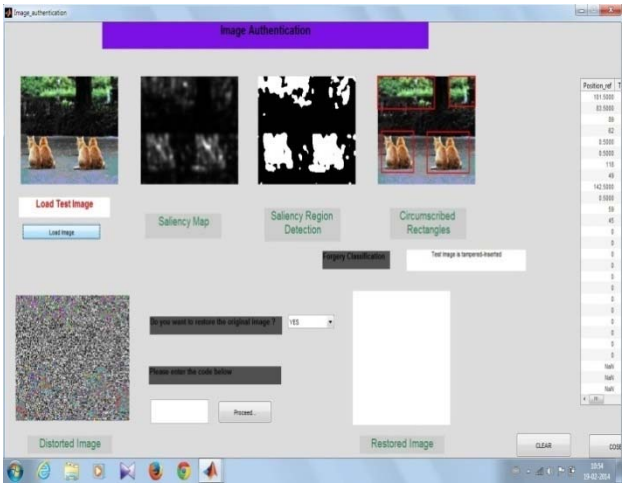


Figure 10: Forged Image

In this fig the input image is forged and given as the second image to be compared.

3. Output Rectangle Image

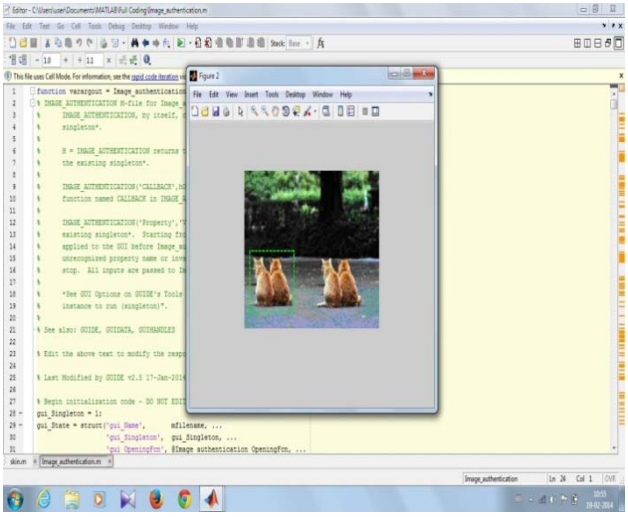


Figure 11: Output Rectangled Forged Image

4. GUI Window

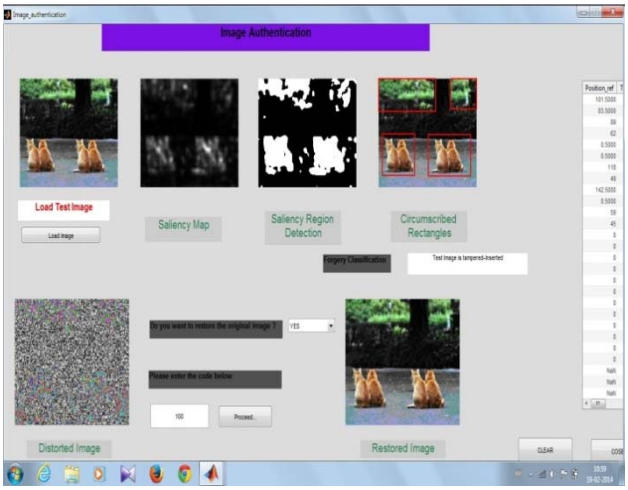


Figure 12: Output Window

4. Image Restoration

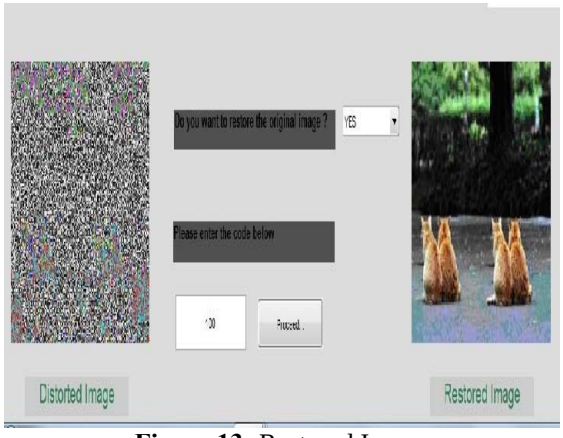


Figure 13: Restored Image

8. Conclusion

The results of salient region detection for position vectors and plotted the rectangles in the reference image and then the texture features are calculated. The Skin based biometric keys of 140 values were added to extract the image in face

detection. Finally decompose the hash in the authentication part and finding the distance to determine whether the image is ‘similar ‘or a ‘forgery one. So if Image is forged it classifies what type of forgeries has occurred i.e. removal, insertion, object replacement and colour modifications and also locate the forged area.. And the image is retrieved and restored as the original image. In future we can reduce the values of hash.

References

[1] F. Ahmed, M. Y. Siyal, and V. U. Abbas, “A secure and robust hash based scheme for image authentication,” Signal Process., vol. 90, no. 5, pp. 1456–1470, 2010
[2] 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
[3] 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
[4] 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
[5] X. Hou and L. Zhang, “Saliency detection: A spectral residual approach,” in Proc. IEEE Int. Conf. Computer Vision and Pattern Recognition, Minneapolis, MN, 2007, pp. 1–8