International Journal of Computer Applications Technology and Research
Volume 3– Issue 11, 664 - 667, 2014, ISSN: 2319–8656

Proficient Hash Sensitivity Growth for Optimized Image Forgery Detection

K. Anitha
Department of Computer Science
V.S.B Engineering College
Karur, Tamilnadu,
India.

P. Leveen Bose
Department of Computer Science
V.S.B Engineering College
Karur, Tamilnadu,
India.

Abstract: The motive behind the work is to provide an effective solution to the most sensitive issue called image forgery that is occurring due to increase in an availability of enormous image modification software. The image forgery causes drastic bad effects in the society such as copyright misuse, evident change in the court of law, quality control, medical image forgery, etc. There are numerous steps taken in order to detect forgery in images, but how far they are successful is the question here. In this paper, an advanced and efficient solution is provided for the forgery detection which can overcome the drawbacks of the existing works by accurately detecting the salient regions by considering both the local and global features of an image (when considering the whole image it is global and when considering only the specific part of an image it is local) and based on this a technique is proposed called hash sensitivity growth method (HSGM), which can accurately detect the salient regions of an image and extract feature contents from that region, hence provide efficient sensitivity growth to a hash, as the sensitivity of the hash is increased it can accurately detect even smaller area tampering and it is robust to normal image processing.

Keywords: Accurate salient feature detection, Global features, local features, hash sensitivity growth, small area tampering, Image authentication

1. INTRODUCTION

The image forgery becomes popular due to the increased image modification software. There are various Image manipulation software all available which may lead to tampering of images, preserving of those image contents is very much essential. Image hash is the short sequence of message content. The hash must be very sensitive so that even the smaller changes in the content will lead to drastic changes in the value of the hash. Ultimately, the hash value should be, convincingly short and so that it can reduce the complexity and also the sensitive hash should be Robust to normal image processing (e.g., compression) and very sensitive to modification of contents. The key is generated and that should not be traced easily by the intruders. The security has to be ensured at this point. The features are extracted from the images, for that the accurate salient Regions have to be selected and both global and local features are extracted (when we extract features by considering whole image it is global and when considering only part of the image it is local). The global features are generally short, but intensive to changes were as local features are sensitive to regional changes, but produces a longer hash. Here we combine both the local and global features. The main goal is to provide reasonably short hash with good performance and to detect small area tampering. To achieve this, we focus mainly on detecting the accurate salient features of an image. The salient features are detected and for that the local and global features are extracted and that can provide high sensitive hash code by using a technique called hash sensitivity growth method (HSGM), for image authentication. The image along with its encrypted hash and the key is sent to the receiver and there , decomposes the hash and the Distance is calculated between the Original image hash and the decrypted hash. If there is a change then it results in detecting and locating the forgery. The medical image, Military image, Quality control and the evidence in the courts are some of the documents that describe the importance of detecting the forgery. The tamper in these areas are not tolerated. The example of a modified Image is given in the Fig 1 and 2.

Figure 1 Original Image Figure 2 Tampered Image

The original image is shown in Figure 1 and the image is modified as in Figure 2. The Original image is modified or tampered as shown (2 and 3 are modified as 6 and 7). Characteristics, and extract local texture features from salient regions in the image to represent contents in the resultant areas. The degree of similarity between two hashes is indicated by distance metrics, defined to measure the performance of the hash. To decide whether a given image is an original/normally-processed or maliciously doctored version of an original image or just a different image two thresholds are used. The proposed method can be used to locate tampered areas and tell the nature of tampering occurred in that image, e.g., misplacement of objects or anomalous modification of colors. The rest of the paper is

organized as follows. In Section II Related Works is described. Section III presents the proposed stratagem and describes salient region detection and texture features and the process of image authentication. Section IV concludes the paper. Section V Future enhancement Section

2. RELATED WORKS

In most of the existing methods they use the watermarking based approach where the information is attached in the LSB bits of the image. A watermark is of two types, visible watermarking and invisible watermarking. One of the major disadvantages of watermarking is that it will deform the content. Some of the existing methods [1]-[7] uses hash signature based methods. In these methods, a hash code is entrenched with the image before transmission. At the destination the hash code is decomposed and used for verification. The image hash is the signature which represents the visual content of an image, and, the hash should be robust against normal image processing and sensitive to tampering. This proposed method provides systematic evidence against the malicious manipulations. The main contribution of this paper is to accurately detect the saliency regions of an image and extract both local and global features of an image so as to increase the hash sensitivity of an image. If the sensitiveness of a hash code is increased then even a small area tampering can be detected. Many existing methods propose image signature based methods. If the attacker knows the signature means it is relatively easy to do the image forgery. To avoid that, our proposed method does not use signature a automatic key is generated by using advanced encryption algorithm.

3. PROPOSED STRATAGEM

The stratagem for the proposed hash scheme and process involved in the image authentication is as follows

3.1 Coining the Hash

The hash is the short sequence that represents the character of the image and hence it is used for image authentication purpose and generating the image hash involves various procedures and they are

- Image Pre-processing
- Saliency Detection
- Global features extraction
- Local features extraction
- Coining the Hash

The block diagram for the proposed stratagem is shown in Figure 3.

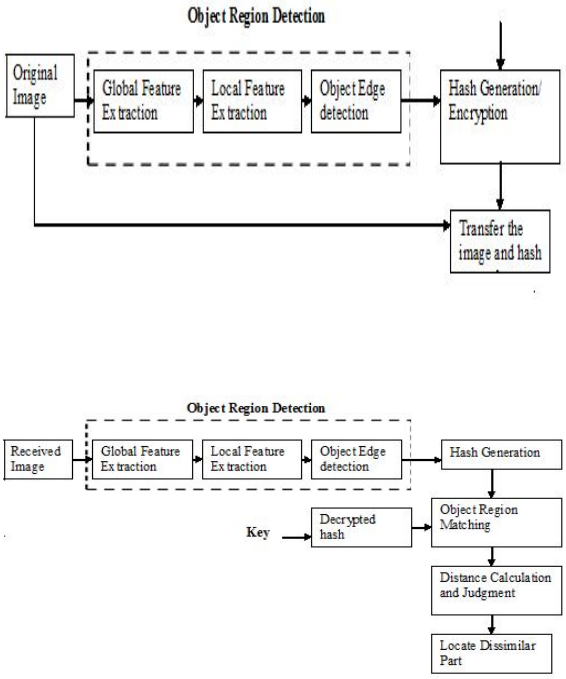

Figure 3 Block diagram of proposed stratagem

3.1.1 Image Pre-processing: The image is first re-sized into fixed size image, and then it is converted from RGB to the YCbCr representation.

***3.1.2 Salient Region Detection*:** Saliency is strong-minded as the local contrast of an image region with respect to its neighborhood at various scales. The saliency evaluated as the distance between the average feature vectors of the pixels of an image sub-region with the average feature vector of the pixels of its neighborhood as shown in Figure 4.

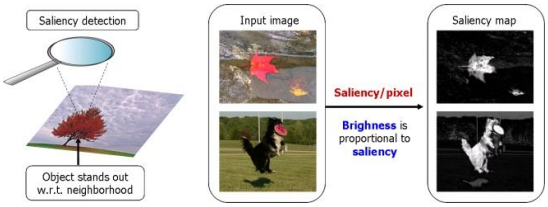

Figure 4 Salient Region Mapping

3.1.3 Saliency Detection Algorithm: This algorithm is used to detect saliency regions by finding the Euclidean distance between the *Lab* pixel vector in a Gaussian filtered image with the average *Lab* vector for the input image [9].

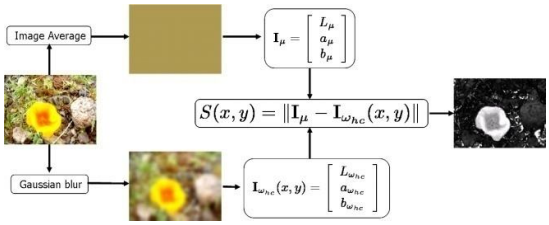

Figure 4 Salient Region Detection

The Figure 4 explains the algorithm of how the salient regions are detected and the accuracy in salient region detection will result in increasing the sensitivity of the hash

3.1.4 Global Feature Extraction: When considering the whole image it is global and for the extraction calculates the Y Cb and Cr using the Zernike moments to form global feature.

3.1.5 Local Feature Extraction: Position and texture of all salient regions to form a local feature. The Salient regions include the coarseness and the contrast of the image.

3.1.6 Coining the Hash: The global and salient local vectors are concatenated to form an intermediate hash and that is then pseudo-randomly scrambled based on a secret key to produce the final hash sequence.

3.2 Proposed Framework for Hash Construction

In [2] the author proposed robust hashing with local models for similarity search and proved it to be efficient. Our idea is to use this concept for Image Authentication for generating sensitive hash values. Considering local features alone is enough for similarity search but for authentication we consider both local and global features and proposed a technique called Hash Sensitivity Growth Model (HSGM). The proposed framework, used for generating the Hash values has two phases.

- Training Phase
- Testing Phase

***3.2.1 Training Phase*:** This phase is offline, it is used to learn hash functions effectively, which is used to map data points located in the testing database into binary hash codes. It has two main components,

- Learning of hash codes
- Learning of hash functions

If a training dataset is given, we first learn the hash codes of the training dataset using our proposed model. Then, in the learning of the hash function component, by considering both the training data and their learned hash codes, a series of hash functions are learned. Each hash function can be used to generate one bit of the hash code for a data point. By specifying the length of the hash code *l*, different sized binary hash codes can be generated.

3.2.2 Testing Phase: At a query point, performing a similarity search is quite simple. First, the given query is mapped into its binary hash code as explained above and, followed by searching the hash table.

***3.2.3 Hamming distance computation*:** The Hamming distance between two binary hash codes is computed by the very much proficient XOR operation. The distance between the test and reference image is calculated so as to identify and locate the forgery in an image.

3.3 Image Authentication

In this image authentication, the receiver decomposes the hash value and compares the hash value with that of the original image and if they both match then it determines the test image is similar to the reference image. The image authentication undergoes the following steps

- Feature extraction
- Hash Value decomposition
- Salient regions matching

3.3.1 Feature Extraction: The received test image is verified by the same procedures as above, except the encryption and the features are extracted

3.3.2 Hash Value Decomposition: With the use of secret keys, the intermediate hash is restored from the reference hash, which is a concatenated feature sequence of the trusted image. Decompose it into global and local features.

***3.3.3 Salient Region Matching**:* Check whether the salient regions detected in the test image are similar to that of the reference image

This process is the reverse process of coining the hash. The hash value is decomposed and the features are extracted from which salient regions are detected and matched.

3.4 Forgery Classification and Localization

The Hamming distance algorithm is used to find the distance between the original and a test image. Based on the difference image forgery is identified in four ways as follows,

- If salient regions of reference image are greater than tested image to know the object has been **removed**.
- If salient regions of tested image are greater than reference image, the image contains **additional image**.
- If salient regions of both reference and tested images are equal, check the luminance and

chrominance components in the Zernike moments if chrominance is greater than luminance, the **color changed** in the reference image.

- If salient regions of both reference and tested images are equal, and (ZC - ZY) is less than the threshold of chrominance, the test image contains **replaced object.**

4. CONCLUSION

In this paper, the robust hashing with local model along with global features combined and a new hashing stratagem is proposed and the new method Hash Sensitivity Growth Model (HSGM) overcomes the drawbacks of the existing image authentications problems. The proposed method preserves the local structural information by a novel local hashing models constructed for each individual data point in the training data set. This produces effective optimized image forgery detection by increasing the sensitivity of the hash by accurately detecting the saliency regions. The accurate saliency region detection and extraction of both local and global features produces highly sensitive hash which can detect even small area tampering. It can proficiently detect forgery and robust to normal image processing. It preserves the contents and local structures of an image and overcomes the drawback of locality sensitive hashing

5. FUTURE ENHANCEMENT

With this proposed hashing scheme, accurate salient regions are detected from that both local and global features are extracted to construct the hash. This preserves the local structure content and hence very sensitive to small area tampering due to increased hash sensitivity. The future enhancement of this will focus mainly reducing the size of the hash value.

6. REFERENCES

[1] Yan Zhao, Shuozhong Wang, Xinpeng Zhang, and Heng Yao, Member, IEEE, "Robust Hashing for Image Authentication Using Zernike Moments and Local Features", IEEE Transactions on Information Forensics and Security, vol. 8, no. 1, January 2013

[2] Jingkuan Song, Yi Yang, Xuelong Li, Fellow, IEEE, Zi Huang, and Yang Yang, "Robust Hashing With Local Models for Approximate Similarity Search", IEEE Transactions on Cybernetics, vol. 44, no. 7, July 2014 1225

[3] V. Monga, A. Banerjee, and B. L. Evans, "A clustering based approach to perceptual image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 1, pp. 68–79, Mar. 2006.

[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, New York, 2007, pp. 121–128.

[5] Z. Tang, S.Wang,X. Zhang, W.Wei, and S. Su, "Robust image hashing for tamper detection using non-negative matrix factorization," J. Ubiquitous Convergence Technol., vol. 2, no. 1, pp. 18–26, May 2008.

[6] Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," IEEE Trans. Inf. Forensics Security, vol. 1, no. 2, pp. 215–230, Jun. 2006.

[7] Y. Lei, Y.Wang, and J. Huang, "Robust image hash in Radon transform domain for authentication," Signal Process.: Image Communication., vol. 26, no. 6, pp. 280–288, 2011.

[8] F. Khelifi and J. Jiang, "Perceptual image hashing based on virtual watermark detection", IEEE Trans. Image Process., vol.19, no.4, pp.981–994, Apr.2010.

[9] R. Achanta, S. Hemami, F. Estrada and S. Süsstrunk, "Frequency-tuned Salient Region Detection", IEEE International Conference on Computer Vision and Pattern Recognition (CVPR 2009), pp. 1597 - 1604, 2009.