International Journal of Digital Crime and Forensics
Volume 10 • Issue 4 • October-December 2018

Fingerprint Image Hashing Based on Minutiae Points and Shape Context

Sani M. Abdullahi, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China
Hongxia Wang, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China
Asad Malik, School of Information Science and Technology, Southwest Jiaotong University, Chengdu, China

ABSTRACT

Fingerprint minutiae is the unique representation of fingerprint image feature points as terminations and bifurcations. Therefore, generating a hash signature from these feature points will unarguably meet the desired properties of a robust hash signature and which will accurately fit in for fingerprint image content authentication purposes. This article proposes a novel minutiae and shape context-based fingerprint image hashing scheme. Fingerprint image minutiae points were extracted by incorporating their orientation and descriptors, then embedded into the shape context-based descriptors in order to generate a unique, compact, and robust hash signature. The robustness of the proposed scheme is determined by performing content preserving attacks, including noise addition, blurring and geometric distribution. Efficient results were achieved from the given attacks. Also, a series of evaluations on the performance comparison between the proposed and other state-of-art schemes has proven the approach to be robust and secure, by yielding a better result.

KEYWORDS

Fingerprint Image, Hashing, Image Hashing, Minutiae Points, Shape Context

1. INTRODUCTION

Since the discovery of biometrics, fingerprint image biometric remains the most versatile, prominent and reliable form of individual authentication in comparison to other biometric techniques. The unique sufficient details that aid in this human identification lies within the minutiae feature points which are the terminations and bifurcations of ridges and valleys in the texture pattern of the fingerprint image (Anil, Arun, & Karthik, 2011). The distribution of this patterns is unique in every individual and on each separate finger, hence the reason it is primarily used for collective fingerprint image identification and verification.

It motivates us to know that the distribution of minutiae points composes the main content structure of fingerprint images. Therefore, embedding these feature points as well as their orientation descriptor into the shape context descriptor is eventually feasible in generating a compact, robust and secure hash signature. Also, our proposed hashing scheme will have a better role to play in cases of multimedia authentication where fingerprint image needs to be verified before permission or access is granted. In the current prevailing literatures, such as in (Wang, Li, & Qiu, 2013), (Schmidt, Sharifi, & Moreno, 2014) and (Aravablumi, Chenna, & Reddy, 2010), researchers make use of the generic hashing algorithm for such multimedia authentication which eventually has limited robustness, security

DOI: 10.4018/IJDCF.2018100101

and discriminative capability. Therefore, our proposed approach is a welcome contribution into the realm of fingerprint hashing for multimedia authentication purposes.

Image hashing plays so many important roles in the field of multimedia security, including content identification and authentication (Tang, Wang, Zhang, Wei & Su, 2008), image retrieval (Tang, Wang, Zhang, & Wei, 2011a), tampering detection (Tang, Dai, & Zhang, 2012), digital watermarking (Zhu, Huang, Kwong, & Yang, 2010) and image registration (Chuan, Xueqin, Dengpan, Jinwei & Xingming, 2016). In our scheme, we use it for fingerprint image authentication (identification and/or verification) by compressing the minutiae features into a compact hash and matching the hash during the authentication stage. All desirable properties of image hashing function, i.e. compactness, perceptual robustness, visual fragility, unpredictability and One-way function, randomness and security (Wang et al., 2015) were put into consideration in the process of generating a hash signature.

Some of the early researchers in the area of fingerprint minutiae hashing includes (Tulyakov, Farooq, Mansukhani, & Govindaraja, 2007), (Kumar, Tulyakov, & Govindaraja, 2010) and (Tulyakov, Farooq, & Govindaraja, 2005), they all proposed the use of symmetric hash functions and its combinations for the purpose of securing the fingerprint feature during identification and/or verification. Even with their astounding contribution in this area, their schemes are not robust enough as compared to current state-of-art schemes.

Recently, a prominent approach was introduced by Lv & Wang, (2012). In their scheme, they proposed a SIFT Harris detector by using it to select the most stable key points, thereby employing their proposed shape context approach to embed the detected local key points and their corresponding descriptors. Their work provides an outstanding contribution to the area of image hashing using shape context and local feature points.

Tang, Zhang, & Zhang (2014) also proposed a novel image hashing approach using ring partition and non-negative matrix factorization (NMF). This scheme, for the first time, introduces the rotation-invariant secondary image which enhances the hash signature to become resistant to rotation manipulations. A high discriminative capability was shown in their approach and its robustness against content preserving manipulations also proved very efficient. In their recent scheme (Tang, Zhang, Li & Zhang 2016), they enhance the rotation robustness and discriminative capability of their previous scheme by incorporating ring partition and invariant vector distance instead of NMF. The extracted ring based statistical features are stable and rotation invariant, thus making it have a high resistance capability against rotation in almost every angle. The scheme proves to be robust with a strong discriminative possession even though its security is not put into consideration.

Wang et al., (2015) proposed an approach by putting the human visual perception into consideration in the process of generating a hash function. Their technique starts by extracting visually sensitive features from the image using Watson's visual model. Then the perceptual hash code is generated by combining the features of the key points and image block. Their scheme proved very sensitive to changes caused by malicious attacks and by achieving trade-off against robustness and tampering localization.

Most current perceptual image hashing approaches make use of the local features of images in order to extract the hash signature but (Zhao, Wang, Zhang, & Yao, 2013) ends the trend by combining both global and local features for a hash sequence generation. The global feature is based on Zernike moments representing luminance and chrominance characteristics while the local features comprises the position and texture information of salient regions in the image. Their scheme proves highly secure and robust against content preserving attacks when compared with other recent state-of-art schemes. A similar improved approach was recently proposed by Ouyang, Wen, Liu, & Chen, (2016) using quaternion Zernike moments. Their scheme allows a full joint processing of the three channels color images without eliminating the chrominance information. Experimental result shows that their scheme provides short hash length that is robust against content preserving attacks.