Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Hierarchical Approach of Discriminative Common Vectors for Bio Metric Security

S. Dhanarajan
M. Tech Computer Science
Bharath University, India

Abstract— Face recognition research still facing challenges in some specific areas such as identification and illumination changes. Although lots of methods have been proposed to solve such problems and have given good results, the difficulties still remain. The matching performance in current linear face recognition systems is relatively poor compared to Kernel Eigen Spaces. A novel modular kernel eigenspaces approach is developed and implemented on the phase congruency feature maps extracted from the visual and thermal images individually. The proposed localized nonlinear feature selection procedure helps to overcome the illumination variations, partial occlusions, expression variations and variations due to temperature changes that affect the visual and thermal face recognition techniques.

Keywords— Biometric, Biometric techniques, kernel eigen spaces, Face Recognition

INTRODUCTION

Face recognition has received significant attention in the last 15 years, due to the increasing number of commercial and law enforcement applications requiring reliable personal authentication (e.g. access control, surveillance of people in public places, security of transactions, mug shot matching, and human-computer interaction) and the availability of low-cost recording devices. Despite the fact that there are more reliable biometric recognition techniques such as fingerprint and iris recognition, these techniques are intrusive and their success depends highly on user cooperation, since the user must position her eye in front of the iris scanner or put her finger in the fingerprint device. On the other hand, face recognition is non-intrusive since it is based on images recorded by a distant camera, and can be very effective even if the user is not aware of the existence of the face recognition system. The human face is undoubtedly the most common characteristic used by humans to recognize other people and this is why personal identification based on facial images is considered the friendliest among all biometrics. Depending on the application, a face recognition system can be working either on identification or verification mode. In a face identification application, the system recognizes an individual by matching the input image against images of all users in a database and finding the best match. In a face verification application the user claims an identity and the system accepts or rejects her claim by matching the input image against the image that corresponds to this specific identity, which can be stored either in a database or an identification card (e.g. smart card). In other words, face identification is a one-to-many comparison that answers the question "Who is the person in the input image? Is she someone in the database?", while face verification is a one-to-one comparison that answers the question "Is the person in the input image who she claims to be?" In the sequel the term face recognition will be used for both identification and verification unless a distinction needs to be made.

Phase congruency features

Security analysis of leading privacy enhanced technologies (PETs) for biometrics including biometric fuzzy vaults (BFV) and biometric encryption (BE). The lack of published attacks, combined with various "proven" security properties has been taken by some as a sign that these technologies are ready for deployment. While some of the existing BFV and BE techniques do have "proven" security properties, those proofs make assumptions that may not, in general, be valid for biometric systems. We briefly review some of the other known attacks against BFV and BE techniques. We introduce three disturbing classes of attacks against PET techniques including attack via record multiplicity, surreptitious key-inversion attack, and novel blended substitution attacks. The paper ends with a discussion of the requirements for architecture to address the privacy and security requirements.

Although biometric systems can be used for reliable user authentication, a biometric system itself is vulnerable to a number of threats. The goal of this project is to identify the vulnerabilities of a biometric system and provide solutions to counter these threats. Biometric cryptosystems combine biometrics and cryptography effectively to improve the security and privacy of biometric systems. A critical issue in biometric systems is protecting the template of a user which is typically stored in a database or a smart card. Cryptographic constructions such as fuzzy vault can be used for template protection and secure biometric matching.

Cryptographic transactions form the basis of many common security systems found throughout computer networks. Supporting these transactions with biometrics is very desirable, as stronger non-repudiation is introduced, along with enhanced ease-of-use. In order to support such transactions, some sort of secure template construct is required that, when re-encoded, can release session specific data. The construct we propose for this task is the bipartite biotoken . In this paper, we define the bipartite biotoken, describe its implementation for fingerprints, and present an analysis of its security. No other technologies exist with the critical reissue and secure embedding properties of the bipartite biotoken. Experimental results for matching accuracy are presented for the FVC 2002 data set and imposter testing on 750 Million matches.

MD 5 Algorithm Features

MD5 stands for "Message-Digest algorithm 5 " in cryptography. MD5 is in fact a widely used cryptographic hash function with a 128-bit hash value.

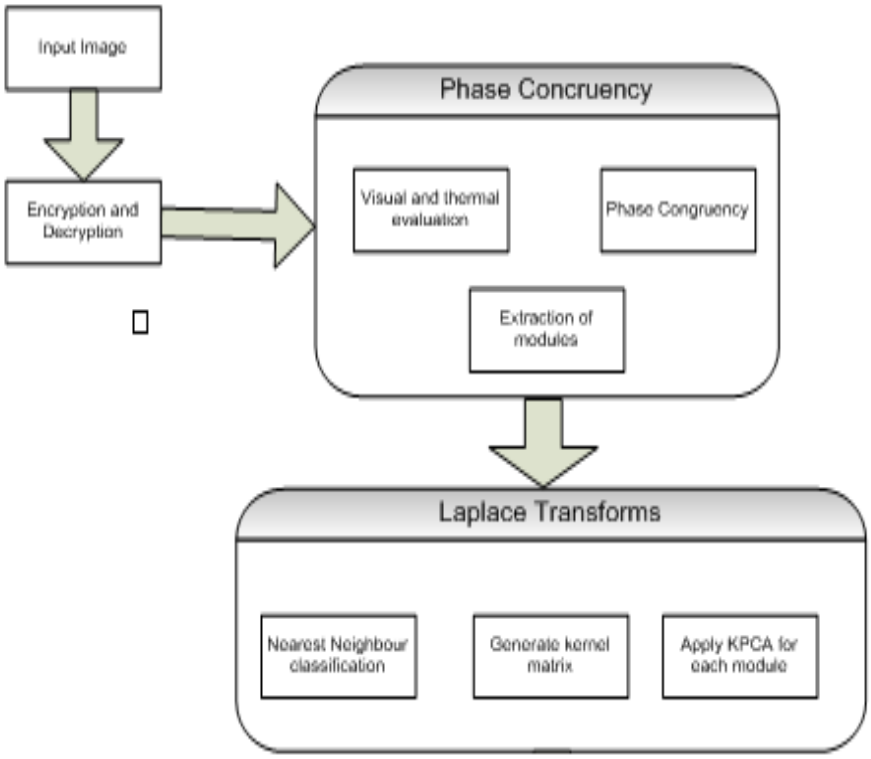
As an Internet standard, MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An MD5 hash is typically expressed as a 32 digit hexadecimal number.

MD5 was designed by Ron Rivest in 1991. The earlier hash function MD4 replaced by MD5 had some serious weaknesses.

We begin by supposing that we have a b-bit message as input, and that we wish to find its message digest. Here b is an arbitrary nonnegative integer; b may be zero, it need not be a multiple of eight, and it may be arbitrarily large. We imagine the bits of the message written down as follows:

m_0 m_1 ... m_{b-1}

Architecture



Kernel Eigen Faces Process

In our system the user side input of the image is forwarded into the server side verification. In here the image has been included into the checking algorithm method of kernel Eigen faces process. In this algorithm make a value (Frequency) level of each and every image. Then it verified into database of the image matching.

CONCLUSIONS

The novel modular kernel eigenspaces approach has been able to provide high recognition accuracy in images affected due to partial occlusions, expressions and nonlinear lighting variations. But in our proposed system has been show significant improvement in the recognition accuracy of thermal images. In that procedure has outperformed the individual modalities as well as other data fusion techniques in terms of recognition accuracy.

ACKNOWLEDGMENT

The additional computation that needs to be carried out can be divided into two parts:

1) Modulo multiplications to be done for encryption/decryption and inner product, and

2) The additional time spent in the computation of random numbers, products, and sums.

As modulo multiplications and encryption decryption operations can be done efficiently using dedicated hardware available, we analyze the time required for both, separately. Consider a biometric with feature vector of length. In the protocol, the client needs to do encryptions for the test vector. The total run time required for all these computations together on current desktop machines is less than 10 ms.

REFERENCES

1. Dieckmann et al, [1997] Dieckmann, U., Plankensteiner, P., and Wagner, T.: "SESAM: *A biometric person identification system using sensor fusion*," In *Pattern Recognition Letters*, Vol. 18, No. 9, pp. 827-833, 1997
2. Hankan Ceviklp, [2005] , *"Discriminative Common vector for face recognition" , IEEE Transactions on patten analysis and machine intelligence,* vol.27.No.1, pp 4-13.
3. Rama Chellapa, [1995], *"Human And Machine Recognition of faces : A Survey "*, proc. IEEE, Vol.83 pp.705-740.
4. W.zhao, [1998], *"Discriminative Common vector for face recognition" , Proc. Third IEEE Int'l conf. Automatic Face and Gesture Recognition,* pp 336-341.
5. P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. Fisherfaces: *Recognition using class specific linear projection,"* IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, pp. 711–720, 1997.
6. M. Turk and A. Pentland, *"Eigenfaces for recognition*," J. Cogn. Neurosci., vol. 3, no. 1, pp. 71–86, 1991.
7. A. Pentland, B. Moghaddam, and T. Starner, "*View-based and modular eigenspaces for face recognition,"* in Proc. IEEE Conf. Computer Vision and Pattern Recognition, 1994, pp. 84–91.
8. J. Huang, P. C. Yuen, W. S. Chen, and J. H. Lai, *"Kernel subspace LDA with optimized Kernel parameters on face recognition,"* in Proc. IEEE Int. Conf. *Automatic Face and Gesture Recognition*, 2004, pp. 327–332.
9. M. H. Yang, N. Ahuja, and D. Kriegman, *"Face recognition using kernel eigenfaces*," Adv. NIPS, vol. 14, pp. 215–220, 2002.
10. M. H.Yang, "Kernel eigenfaces vs. kernel fisherfaces: Face recognition using kernel methods," presented at the IEEE Conf. Automatic Face and Gesture Recognition, 2002.
11. J. Yang, Z. Jin, J. Y. Yang, D. Zhang, and A. F. Frangi, *"Essence of kernel fisher discriminant: KPCA plus LDA,"* Pattern Recognit., vol. 10, pp. 2097–2100, 2004.
12. D. A. Socolinsky and A. Selinger, *"Thermal face recognition in an operational scenario,"* in Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR), Washington, DC, 2004, pp. 1012–1019.

