Volume 5, Issue 2, February 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Image worth Evaluation for False Biometric Detection: Submission to Iris, Fingerprint and Face Recognition

[1]Boggarapu Srinivasulu, [2] Dr. M. Ekambaram Naidu, [3]Dr. E. Sreenivasa Reddy
[1]Assistant Professor, Dept of CSE, Mother Theresa Institute of Engineering & Technology Palamaner, Chittoor Dist, AP, India
[2]Principal & Professor (CSE), TRR Engineering College, Hyderabad, India
[3]Dean& Professor (CSE), Acharya Nagarjuna University, Nagarjunanagar, Guntur, India

Abstract: ***To ensure the actual presence of a real legitimate trait in contrast to a false self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. Present a new software-based false detection method that can be used in multiple biometric systems, face reorganization to detect different types of counterfeit access attempts. The idea of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality measurement. The planned approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to differentiate between valid and impostor samples. The untried results, obtained on publicly available data sets of fingerprint, iris, and 2D face. To provide a forceful proof that a new method is better than the state-of-the-art, computer graphics projects are often accompanied by user studies, in which a group of observers rank or rate results of several algorithms. Such user studies, known as subjective image worth evaluation experiments, can be very time consuming and do not guarantee to produce conclusive results.***

Keywords: Image quality assessment, attacks, biometrics, countermeasures, security, Face hallucination.

I. INTRODUCTION

In recent years, the increasing interest in the evaluation of biometric systems security has led to the creation of numerous and very diverse initiatives focused on this major field of research : the publication of many research works disclosing and evaluating different biometric methods, the proposal of new protection methods ,related book chapters , the publication of several standards in the area , the dedication of specific tracks, sessions and workshops in biometric-specific and general signal processing conferences, the organization of competitions focused on vulnerability assessment , the acquisition of specific datasets, the creation of group sand laboratories specialized in the evaluation of biometric security , or the existence of several European Projects with the biometric security topic as main research interest. All these initiatives clearly highlight the importance given by all parties involved in the development of biometrics Among the different threats analyzed, the so-called director spoofing attacks have motivated the biometric community to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris, the fingerprint, the face , the signature , or even the gait and Multimodal approaches.

In these attacks, the intruder uses some type of synthetically produced artifact , or tries to mimic the behavior of the genuine user (e.g., gait, signature), to fraudulently access the biometric system. As this type of attacks is performed in the analogy domain and the interaction with the device is done following the regular protocol, the usual digital protection mechanisms (e.g., encryption, digital signature or watermarking) are not effective. The aforementioned works and other analogue studies have clearly shown the necessity to propose and develop specific protection methods against this threat. This way, researchers have focused on the design of specific countermeasures that enable biometric systems to detect false samples and reject them, improving this way the robustness and security level of the systems. Besides other anti-spoofing approaches such as the use of multi biometrics or challenge-response methods, special attention has been paid by researchers and industry to the livens detection techniques, which use different physiological properties to distinguish between real and false traits. Livens assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user friendly, people should not be reluctant to use it, fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time, low cost, a wide use cannot be expected if the cost is excessively high performance, in addition to having a good false detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

© 2015, IJARCSSE All Rights Reserved

In the present work we lean upon the previous work and broaden the application of the method pursuing more unconstrained conditions. The methods for liveness detection may be hardware or software based. In the present work we use a software based approach. These countermeasures are to prevent attacks at sensor level. So, the false irises are detected once the sample has been acquired with a standard sensor. The key point of the process is to find a set of discriminate features which permits to build an appropriate classifier which gives the probability of the sample vitality given the extracted set of features. In the previous work, the segmentation of iris was done manually; however, this is unrealistic if we are aiming a real world application. To overcome this less realistic scenario, in the present work we applied a automatic segmentation method. Therefore some of the implemented state-of-the-art methods were adapted to the non-circular contours obtained by the segmentation method.

II. RELATED WORK

2.1 Iris Liveness Detection:

The problem of liveness detection of a biometric trait can be seen as a two class classification problem where an input trait sample has to be assigned to one of two classes: real or false. The key point of the process is to find a set of discriminate features which permits to build an appropriate classifier which gives the probability of the sample vitality given the extracted set of features

Biometric recognition systems are vulnerable to be spoofed by false copies, for instance, false finger tips made of commonly available materials such as clay and gelatin. Iris is no exception. There are potential threats for iris-based systems, the main are Eye image (Screen image, Photograph, Paper print, video signal), artificial eye (Glass/plastic etc), Natural eye (user Forced use), Capture/replay attacks (Eye image, Iris Code template), Natural eye (Eye removed from body, Printed contact lens).

2.2 Liveness Detection Methods:

Liveness detection methods are generally classified into two types (i) Software-based techniques, in this type the false trait is Detected once the sample has been acquired with a normal sensor (i.e., features used to Differentiate between real and false traits are extracted from the biometric sample, and not from the trait itself); and Hardware-based techniques, which add some particular device to the sensor in order to detect Exacting properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye).

2.3 Image Quality Assessment For Liveness Detection:

The use of image quality assessment for liveness detection is motivated by the supposition that: "It is expected that a false image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed."[1] Predictable quality differences between real and false samples may contain: color and luminance levels, general artifacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance. For example, iris images captured from a printed paper are more likely to be unclear or out of focus due to trembling; face images captured from a mobile device will most likely be over- or under-exposed; and it is not rare that fingerprint images captured from a gummy finger present local gaining artifacts such as spots and patches. Also, in an ultimate attack in which an unnaturally produced image is directly injected to the communication channel before the feature extractor, this false sample will most likely lack some of the properties found in natural images.

The potential of general image quality assessment as a protection method against different biometric attacks. Different quality measures present diverse sensitivity to image artifacts and distortions. For example, measures like the mean squared error respond additional to additive noise, while others such as the spectral phase error are extra sensitive to blur; while gradient-related features respond to distortions concentrated around edges and textures. Therefore, using a large range of IQMs exploiting complementary image quality properties should allow detecting the aforementioned quality differences between real and false samples expected to be found in many attack attempts. So consider that there is sound proof for the "quality-difference" theory and that image quality measures have the possible to achieve success in biometric protection tasks.

2.4 Face hallucination:

Image super-resolution is a class of techniques that improve the oath of an image using a set of low oath images. The main difference between both techniques is that face hallucination is the super-resolution for face images and always employs typical face priors with strong cohesion to face domain concept

Face hallucination algorithm:

Face hallucination algorithms have been reported to perform this technique because it can be done in different ways. Although the existing face figments of the imagination methods have achieved great success, there is still much room for improvement. The common algorithms usually perform two steps: i) It generates global face image which keeps the characteristics of the face using probabilistic method maximum a posteriori (MAP). ii) It produces lingering image to recompense the result of the MAP. Any face hallucination algorithm must be based in three constraints:

Data constraint

The output image ought to be nearly to the unique image when it is smoothed or down-sampled.

© 2015, IJARCSSE All Rights Reserved

Global constraint

The resulting image always contains all common features of a human face. The facial features must be coherent always. Without this constraint, the output could be too noisy.

Local constraint

The output image must have very exact features of the face image having difference with photorealistic local features. Without this constraint, the resulting image could be too smooth.

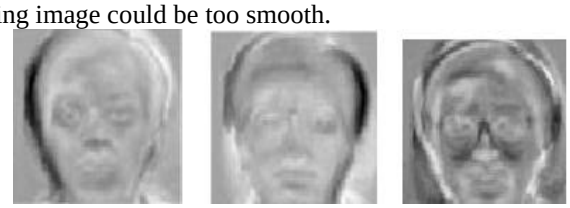


Fig: Eigenfaces of face images

III. MULTI BIOMETRIC SYSTEM

Multi Biometric system is use more than one biometric system for one multi biometric system for more security. Uni-biometric system is easy to hack but multi biometric system is not easy to hack because one person does not obtain two traits of the same individual. This is the reason that multi biometric system is more secure than uni-biometric system. To work the multi biometric system based on the two steps (1) Enrollment on that Multi biometric first creates the data base of users. And (2) verification on that when user try to gate access on the system then at that time first system captures the characteristic of the person then system match the input data to the data base sample. And then person gate authentication or conclude as a false user. An introduction of application of biometric system used in this paper are face recognition system, fingerprint recognition system, iris recognition system.

Face recognition and attack on system:

The most acceptable biometrics is Face reorganization, because it is one of the most universal methods of identification that humans use in their visual interactions and acquisition of faces. The face recognition systems make different between the background and the face. It is most important when the system has to identify a face within a throng. The system then makes use of a person's facial features – its valleys and peaks and landmarks and treats these as nodes that can be compared and measured against those which are stored in the system's database. There are approximately 80 nodes comprising the face print that makes use of the system and this includes the eye socket depth, jaw line length, distance between the eyes, cheekbone shape, and the width of the nose. It is very challenging to develop this recognition technique which can accept the effects of facial expressions, age, slight variations in the imaging environment. Attack on the face recognition system is that figure false and genuine image are shown and that images are find out due to different method of face recognition. In face recognition system false users attack on system by capturing the picture to the mobile devices or camera. And try to authenticate.

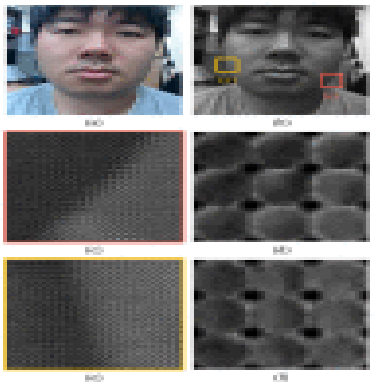


Fig. Examples of real and false face images.

Fingerprint recognition and attacks on system

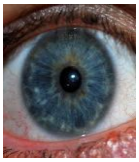
Every fingerprint of each person is considered to be unique, Even the Twins also contain different fingerprint. Fingerprint recognition is the most accepted biometric recognition method. Fingerprints have been used from long time for identifying individuals. Fingerprints consist of ridges and furrows on the surface of a fingertip. Now fingerprint recognition system is used in iphone, there are many areas where the fingerprint recognition system used. But attackers attack on fingerprint recognition system. Attackers first capture real fingerprint then they make false fingerprint by using silicon, playdoh and gelatin and try to access the system.

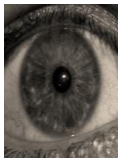
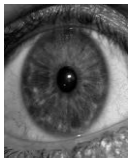
Iris Recognition attacks on system

Iris recognition is a automated method of biometric identification which uses mathematical model recognition techniques on video images of the irises of an individual's eyes, whose Complex random patterns are single and can be seen from some distance. Iris cameras perform detection of a person's identity. The iris scans process start to get something on film.

© 2015, IJARCSSE All Rights Reserved

It combines computer vision, statistical inference, pattern recognition and optics. The iris is the colored ring around the pupil of every human being and like a snowflake; no two are the same. Each one is unique. An attack on the iris is not so easy but how to attack on the system is as shown below. To create a false iris is of tree step 1) Original images are capture for a better quality, then 2) They are printed on a paper using a commercial printer (see fig 8) 3) Printed images are presented at the iris sensor.



Advantages of Multi-biometric Systems over a unibiometric system:

- Better Security: - The multi-biometric system increases the security level. Unibiometric system is easy to attack but the multi-biometric system is not so easy because attacker cannot obtain two traits of the same individual.
- More secure than other system
- Multiple Fingerprint scanner support
- Multiple IRIS Scanner support

Application

- Multi-biometric system is used in India for making Aadhar card this multi-biometric system is used face recognition, iris recognition, and fingerprint recognition
- Multi-biometric system used in Airport.
- Multi-biometric system is used in banking.

IV. CONCLUSION

This paper presented a novel robust regularized coding (RRC) model and an associated effective iteratively reweighted regularized robust coding (IR3C) algorithm for robust face recognition (FR). One important advantage of RRC is its robustness to various types of outliers (e.g., occlusion, corruption, expression, etc.) by seeking for an approximate MAP (maximum a posterior estimation) solution of the coding problem. By 28 assigning adaptively and iteratively the weights to the pixels according to their coding residuals, the IR3C algorithm could robustly identify the outliers and reduce their effects on the coding process. Meanwhile, we showed that the l2-norm regularization is as powerful as l1-norm regularization in RRC but the former has much lower computational cost. The proposed RRC methods were extensively evaluated on FR with different conditions, including variations of illumination, expression, occlusion, corruption, and face validation. The experimental results clearly demonstrated that RRC outperforms significantly previous state-of-the-art methods, such as SRC, CESR and GSRC. In particular, RRC with l2-norm regularization could achieve very high recognition rate but with low computational cost, which makes it a very good candidate scheme for practical robust FR systems.

REFERENCES

[1] W. Zhao, R. Chellppa, P.J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," ACM Computing Survey, vol. 35, no. 4, pp. 399–458, 2003.

[2] M. Turk and A. Pentland, "Eigenfaces for recognition," J. Cognitive Neuroscience, vol. 3, no. 1, pp. 71–86, 1991.

[3] P.N. Belhumeur, J.P. Hespanha, and D.J. Kriengman, "Eigenfaces vs. Fisherfaces: recognition using class specific linear projection," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 711–720, 1997.

[4] B. Heisele, P. Ho, and T. Poggio, "Face recognition with support vector machine: Global versus component-based approach," Proc. IEEE Int'l Conf. Computer Vision, 2001.

[5] A. Lanitis, C.J. Taylor, and T.F. Cootes, "Automatic Interpretation and Coding of Face Images Using Flexible Models," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 19, no. 7, pp. 743-756, 1997.

[6] T. Ahonen, A. Hadid, and M. Pietikainen, "Face description with local binary patterns: Application to face recognition," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 28, no. 12, pp.2037–2041, 2006.

[7] A. Leonardis and H. Bischof, "Robust recognition using eigenimages," Computer Vision and Image Understanding, vol. 78, no. 1, pp. 99-118, 2000.

[8] S. Chen, T. Shan, and B.C. Lovell, "Robust face recognition in rotated eigenspaces," Proc. Int'l Conf. Image and Vision Computing New Zealand, 2007.

[9] A.M. Martinez, "Recognizing Imprecisely localized, partially occluded, and expression variant faces from a single sample per class," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 6, pp. 748-763, 2002.

[10] S.Z. Li and J. Lu, "Face recognition using nearest feature line method," IEEE Trans. Neural Network, vol. 10, no. 2, pp. 439-443, 1999.

[11] J.T. Chien, and C.C. Wu, "Discriminant waveletfaces and nearest feature classifiers for face recognition," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 24, no. 12, pp. 1644-1649, 2002.

© 2015, IJARCSSE All Rights Reserved

[12] J. Laaksonen, "Local subspace classifier", Proc. Int'l Conf. Artificial Neural Networks, 1997.
[13] K. Lee, J. Ho, and D. Kriegman, "Acquiring linear subspaces for face recognition under variable lighting," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 27, no. 5, pp. 684–698, 2005.
[14] S.Z. Li, "Face recognition based on nearest linear combinations," Proc. IEEE Int'l Conf. Computer Vision and Pattern Recognition, 1998.
[15] I. Naseem, R. Togneri, and M. Bennamoun, "Linear regression for face recognition," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 32, no. 11, pp. 2106-2112, 2010.
[16] M. Elad and M. Aharon, "Image denoising via sparse and redundant representations over learned dictionaries," IEEE Trans. Image Processing, vol. 15, no. 12, pp. 3736–3745, 2006.
[17] J. Mairal, M. Elad, and G. Sapiro, "Sparse representation for color image restoration," IEEE Trans. Image Processing, vol. 17, no. 1, pp. 53–69, 2008.
[18] J. Wright, A.Y. Yang, A. Ganesh, S.S. Sastry, and Y. Ma, "Robust face recognition via sparse representation," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 31, no. 2, pp. 210–227, 2009.
[19] J. Wright and Y. Ma, "Dense error correction via l1 minimization," IEEE Trans. Information Theory, vol. 56, no. 7, pp. 3540–3560, 2010.
[20] M. Yang and L. Zhang, "Gabor Feature based Sparse Representation for Face Recognition with Gabor Occlusion Dictionary," Proc. European Conf. Computer Vision, 2010.
[21] J. Mairal, F. Bach, J. Ponce, G. Sapiro, and A. Zisserman, "Learning discriminative dictionaries for local image analysis," Proc. IEEE Conf. Computer Vision and Pattern Recognition, 2008.
[22] K. Huang and S. Aviyente, "Sparse representation for signal classification," Proc. Neural Information and Processing Systems, 2006.
[23] B.A. Olshausen and D.J. Field, "Sparse coding with an overcomplete basis set: a strategy employed by V1?" Vision Research, vol. 37, no. 23, pp. 3311–3325, 1997.

© 2015, IJARCSSE All Rights Reserved