International Journal of Advanced Research in Engineering Technology & Sciences ISSN: 2394-2819
July-2016 Volume 3, Issue-7
Email:editor@ijarets.org www.ijarets.org

BIOMETRIC SECURITY THROUGHLIVELINESS DETECTION

Er. Pawan Kumar
Assistant Professor
HCTM Kaithal

Rashika Gupta
M.Tech (CSE) Scholar
HCTM Kaithal

ABSTRACT*: with the quick progress of electronic data and present association, the demand for data and protection association is producing urgently. At present there are countless identification data association technologies. The accepted methods contain face credit, fingerprint credit and iris recognition. Iris credit is one of the most enthusing biometric credit metho. It has countless good features: elevated credit rate, non link and fraudulence proof. It has vital request prospects because of elevated protection and elevated accuracy. Liveliness detection mentions to the detection of living symptomsi.e., identification of liveliness symptoms that might clarify the authenticity of the eye and the willingness of the subject to be registered by the sensor, and hence is a distinct case of a wider class of methods aiming at detection of each presentation attack.Instead of extra usually utilized static properties of the eye or its tissue, we will use dynamics of the acolyte registered below visible light stimuli. As the acolyte reacts involuntarily after the light intensity adjustments, it is tough to obscure this phenomenon. ISO/IEC defines the presentation attack as 'presentation of an artifact or human characteristic to the biometric arrest subsystem in a style that might inhibit alongside the aimed strategy of the biometricsystem'. This paper is concerning liveliness detection approached that have been studies in the literature.*

Keywords*: Biometrics, Iris Recognition, Liveliness Detection, presentation attack.*

INTRODUCTION

A biometric authentication arrangement is basically a outline credit arrangement that makes a confidential identification by ascertaining the authenticity of a specific physiological and/or behavioral characteristic owned by the user. Physiological characteristics are connected to the form of the body, such as hand geometry, Palm print, face credit, fingerprint, DNA, iris credit, retina and odor. Behavioral characteristics are connected to the deeds of a person, such as typing rhythm, gait, and voice. The person to be recognized is needed to be physically present at the period of identification and identification established on biometric methods obviates the demand to recall a password or hold a token.

The selection of a particular biometric for use in a specific request involves a weighting of countless factors. Seven such factors to be utilized after assessing the suitability of each trait for use in biometric authentication: Universality, Uniqueness, Permanence, Measurability, Performance, Acceptability and Circumvention. Universality way that every single person employing a arrangement ought to own the trait. Uniqueness way the trait ought to be sufficiently disparate for people in the relevant populace such that they can be discriminated from one another. Permanence relates to the manner in that a trait varies above time. Measurability or collectability relates to the ease of buy or measurement of the trait. In supplement, acquired data ought to be in a form that permits consecutive processing and extraction of the relevant feature sets. Presentation relates to the accuracy, speed, and robustness of knowledge used. Acceptability relates to how well people in the relevant populace accord the knowledge such that they are keen to have their biometric trait seized and assessed. Circumvention relates to the ease alongside that a trait could be copied employing an artifact or substitute.

BIOMETRIC AUTHENTICATION SYSTEM

Practically all the biometric authentication arrangements work in the alike manner. The early procedure is shouted enrollment in that every single new user is registered into a database. Data concerning a

precise characteristic of the person is captured. This data is normally bypassed across an algorithm that turns the data into a template that the database stores. Note that it is the template that is upheld in the arrangement, but not the early biometric measurement as countless people could suspect. Contrasted alongside the early measurement of the biometric trait, the template has a extremely tiny number of information; it is no extra than a collection of numbers alongside slight meaning except to the biometric arrangement that produced them. After a person needs to be understood, the arrangement will seize the appropriate measurement, elucidate this data into a template employing the alike algorithm that the early template was computed alongside, and next difference the new template alongside the database to ascertain if there is a match,and hence, whichever an verification or identification is completed as shown in figure 1.

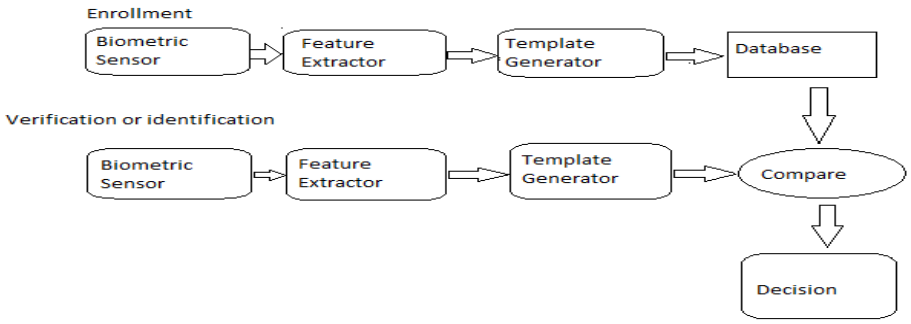

Fig.1 Biometric authentication process

An important distinction between biometric verification and identification lies in that verification is a one-to-one comparison, while identification is a one-to-many search in a database. They perform different functions since verification is used to confirm one's identity and identification is used to find one's identity.

IRIS LIVELINESS DETECTION

Liveliness detection mentions to the detection of living symptoms, and hence is a distinct case of a wider class of methods aiming at detection of each presentation attack. ISO/IEC defines the presentation attack as 'presentation of an artifact or human characteristic to the biometric arrest subsystem in a style that might inhibit alongside the aimed strategy of the biometricsystem'. This way that each subversive deed (i.e., alongside the aim to subvert a biometric system) ought to be noticed as a presentation attack. Though, the aim of the attacker cannot be inferred. Hence the presentation attack becomes a extremely broad-ranging earth that includes presentation of fake objects, as well as cadaver portions, incongruous or coerced presentations, and even zero-effort impostor attempts. This unfamiliar aim additionally reasons fake alarms by categorizing a little dubious deeds as possible presentation aggressions, e.g., non-conformant presentation due to illness, exhaustion or presentation of manmade objects for cosmetic or condition reasons. This perplexes the association of aggressions and stimulates on-going logical discussion in the earth of how to effectually deal alongside presentation attack detection (abbreviated more as PAD).

2. LITERATURE SURVEY

Jeffrey F., Cohn et al. (2003) [1] In this paper, previous research in automatic facial expression recognition has been limited to recognition of gross expression categories (e.g., joy or anger) in posed facial behavior under well-controlled conditions (e.g., frontal pose and minimal out-of-plane head motion). We have developed a system that detects a discrete and important facial action (e.g., eye blinking) in spontaneously occurring facial behavior that has been measured with a non frontal pose, moderate out-of-plane head motion, and occlusion. The system recovers three-dimensional motion parameters, stabilizes facial regions, extracts motion and appearance information, and recognizes discrete facial actions in

spontaneous facial behavior. We tested the system in video data from a two-person interview. The 10 subjects were ethnically diverse, action units occurred during speech, and out-of-plane motion and occlusion from head motion and glasses were common.

Jong Hyun, Park et al. (2005) [2] In this paper, we present an iris recognition system considering counterfeit attacks. The proposed system takes multi-spectral images instead of one infrared iris image. The energy of the multi-spectral images is checked and the authentication is failed if the amount of the energy is not in the proper range. Then the images are normalized and merged into a grayscale image by using a gradient-based image fusion algorithm. In the fusion process, the images considered to be from a counterfeited iris are merged into a poor-quality image which successively generates poor matching score.

EuiChul, Lee et al. (2005) [3]In this paper, fake iris detection is to detect and defeat a fake (forgery) iris image input. To solve the problems of previous researches on fake iris detection, we propose the new method of detecting fake iris attack based on the Purkinje image. Especially, we calculated the theoretical positions and distances between the Purkinje images based on the human eye model and the performance of fake detection algorithm could be much enhanced by such information. Experimental results showed that the FAR (False Acceptance Rate for accepting fake iris as live one) was 0.33% and FRR(False Rejection Rate of rejecting live iris as fake one) was 0.33%.

Andrzej, Pacut et al. (2006) [4] In this paper, various experiments show an alarming lack of anti-spoofing mechanisms in devices already protecting many sensitive areas all over the world, proving that aliveness detection methods must be quickly included in commercial equipment. To introduce and systemize the topic, the paper begins with a survey of possible types of eye forgery, together with possible countermeasures. The authors introduce three solutions of eye aliveness detection, based on analyses of image frequency spectrum, controlled light reflection from the cornea, and pupil dynamics. A body of various fake (printed) eye images was used to test the developed methodologies, including different printers and printout carriers. The proposed methodology was embedded into the NASK iris recognition system and showed its large potential. For a local database of pairs of alive and printed eyes, all methods proposed in the paper revealed zero false acceptance rate of fakes FAR-F.

Sung Joo, Lee et al. (2006) [5] In this paper, we propose a new fake iris detection method based on the changes in the reflectance ratio between the iris and the sclera. The proposed method has four advantages over previous works. First, it is possible to detect fake iris images with high accuracy. Second, our method does not cause inconvenience to users since it can detect fake iris images at a very fast speed. Third, it is possible to show the theoretical background of using the variation of the reflectance ratio between the iris and the sclera. To compare fake iris images with live ones, three types of fake iris images were produced: a printed iris, an artificial eye, and a fake contact lens.

Masashi, Kanematsu et al. (2007) [6]In this paper, the importance of personal authentication is increasing with the development of the information society. The accuracy of personal authentication by identifying the iris is higher than that by using other biometric traits such as faces or fingerprints. However, the iris authentication system is vulnerable to deception by a fake iris even though the recognition accuracy is high. In this study, we developed a liveness detection method by using a variation in the brightness of an iris pattern induced by a pupillary reflex. The live and artificial irises were classified by a decision threshold of 7% brightness variation rate.

Xiaofu, He et al. (2008) [7]In this paper, in recent years, iris recognition is becoming a very active topic in both research and practical applications. However, fake iris is a potential threat there are potential threats for iris-based systems. This paper presents a novel fake iris detection method based on the analysis of 2-D Fourier spectra together with iris image quality assessment. First, image quality assessment method is used to exclude the defocused, motion blurred fake iris. Then statistical properties of Fourier spectra for fake iris are used for clear fake iris detection. Experimental results show that the proposed method can detect photo iris and printed iris effectively.

3. PROBLEM FORMULATION

Liveliness detection mentions to the detection of living symptoms, and hence is a distinct case of a wider class of methods aiming at detection of each presentation attack ISO/IEC defines the presentation attack as 'presentation of an artifact or human characteristic to the biometric arrest subsystem in a style that might inhibit alongside the aimed strategy of the biometric system'. This way that each subversive deed (i.e., alongside the aim to subvert a biometric system) ought to be noticed as a presentation attack. Though, the aim of the attacker cannot be inferred. Hence the presentation attack becomes a extremely broad-ranging earth that includes presentation of fake objects, as well as cadaver portions, incongruous or coerced presentations, and even zero-effort impostor attempts. This unfamiliar aim additionally reasons fake alarms by categorizing a little dubious deeds as possible presentation attacks, e.g., non-conformant presentation due to illness, exhaustion or presentation of manmade objects for cosmetic or condition reasons. This perplexes the association of aggressions and stimulates on-going logical discussion in the earth of how to effectually deal alongside presentation attack detection (abbreviated more as PAD).

4. PROPOSED WORK

In this work we focus on iris liveliness detection, i.e., identification of liveliness symptoms that might clarify the authenticity of the eye and the willingness of the subject to be registered by the sensor. Instead of extra usually utilized static properties of the eye or its tissue, we use dynamics of the acolyte registered below visible light stimuli. As the acolyte reacts involuntarily after the light intensity adjustments, it is tough to obscure this phenomenon. As will be shown in the paper, the acolyte dynamics are not trivial, making it tough to imitate them for manmade objects. In our examinations we selected not to use static objects such as iris paper printouts or patterned link lenses, as in such cases we should be assured of accomplishment (static objects do not present momentous dynamics, separately from a little measurement sound, and therefore are facilely recognizable after dynamics is the key). Instead, to assess the counseled method presentation, we categorize spontaneous acolyte oscillations (often called hippus) and normal acolyte replies to a affirmative surge of visible light, therefore making the examinations extra realistic. To our best vision, this is the merely work that employs acolyte dynamics for liveliness detection and that is assessed on vibrant, real objects rather than static artifacts.

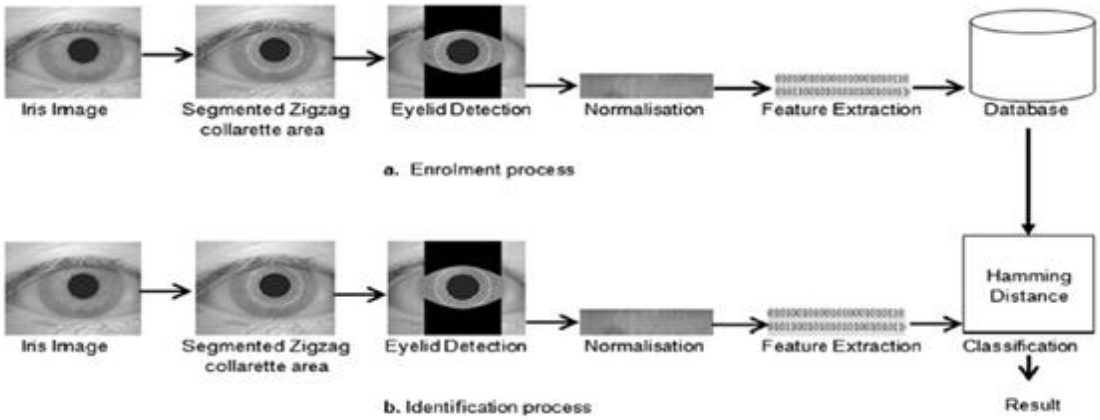

Figure 4.1Flow diagram of proposed system.

5. RESULT

An picture histogram is a kind of histogram that deeds as a graphical representation of the tonal allocation in a digital image. It plots the number of pixels for every single tonal value. By looking at the histogram for a specific picture a viewer will be able to judge the whole tonal allocation at a glance.

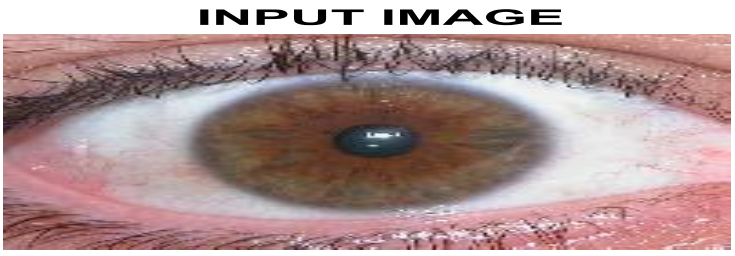

Fig 5.1 Input Image taken from the UBIRIS Dataset of Person 1

Fig 5.2 Image after grayscale conversion, conversion to grayscale is done to reduce complexity

Fig 5.3 Image Histogram of the input image

Fig 5.4 Canny Image

Edges describe borders and are consequently a setback of frank significance in picture processing. Borders in pictures are spans alongside forceful intensity contrasts a hop in intensity from one pixel to the next. Frontier noticing an picture considerably reduces the number of data and filters out unusable data, as maintaining the vital structural properties in an picture.

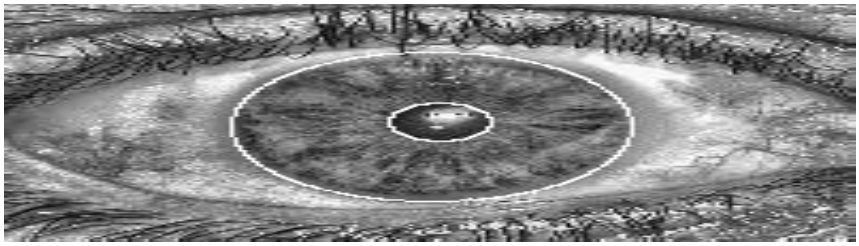

Fig 5.5 Iris Template of Person 1 in UBIRIS Dataset using Proposed Method

A template crafted by imaging an iris is contrasted to stored template(s) in a database. If the Hamming distance is below the decision threshold, a affirmative identification has efficiently been made because of the statistical great improbability that two disparate persons might concur by chance ("collide") in so countless bits, given the elevated entropy of iris templates.

Fig 5.6 Iris Mask of Person 1 in UBIRIS Dataset using Proposed Method

The aim of matching is to assess the similarity of two iris representations. Crafted templates are contrasted employing the Hamming distance. The normalized Hamming distance utilized measures the fraction of bits for that two iris codes disagree. A low normalized Hamming distance implies forceful similarity of the iris codes. If portions of the irises are occluded, the normalized Hamming distance is the fraction of bits that differ in the spans that are not occluded on whichever image. To report for rotation, analogy amid a pair of pictures involves computing the normalized Hamming distance for countless disparate orientations that correspond to circular permutations of the program in the angular coordinate. The minimum computed normalized Hamming distance is consented to correspond to the correct alignment of the two images.

Confusion matrix custom to assess the quality of the output of a classifier on the iris data set. The diagonal agents embody the number of points for that the forecasted label is equal to the real label, as off-diagonal agents are those that are mislabeled by the classifier. The higher the diagonal benefits of the confusion matrix the larger, indicating countless correct predictions. The figures below display the confusion matrix alongside and lacking normalization by class prop size.

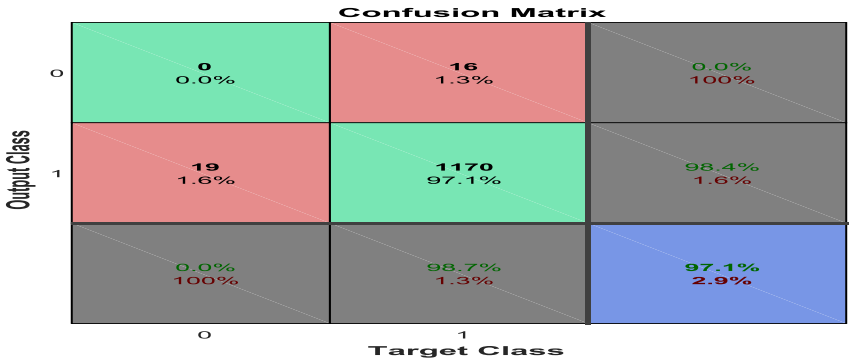

Fig 5.7 Confusion Matrix

For Analogy database were utilized for the training and pictures for the assessing purpose. The credit accuracy was contrasted amid the counseled method and beforehand described work. Analogy of credit accuracy alongside disparate feature vectors such as Haar wavelet, 1D Gabor wavelet or combination as input across matching procedure is given in Table 4. The counseled method has an accuracy of 97.1% on this database.

6. CONCLUSION AND FUTURE SCOPE

The works relevant to iris biometrics is not colossal, but is producing quickly and ranges across a expansive collection of sources. This survey suggests a construction for the iris biometrics works and summarizes the present state-of-the art. There are yet a number of alert research cases inside Iris biometrics. Countless of these are connected to the desire to make iris credit useful in less-controlled conditions and additionally a real period procedure as far as possible. This survey additionally highlights the insufficient upcoming trials and continuing difficulties that can be addressed in more research, e.g. extra research ought to be completed to discern how credit might be enhanced for extra robust populaces and conditions. Also, research on iris biometrics for people wearing glasses can be one more trial in this field. One more span that has not consented far investigation is the combination of several pictures or the use of several biometrics (e.g. iris and iris recognition) to enhance performance. The efficiency of the matching algorithms will additionally come to be extra vital as iris biometrics are used in credit requests for colossal populations. Assorted health conditions and supplementary situations altering the credit debated in this paper ought to be resolved in upcoming research. More research can additionally be commenced for growing datasets of iris pictures in multi angle pictures, pictures seizing disparate health conditions and pictures at distance. Research work on growing synthetic iris datasets can be one more scope of investigation in this area. We yearn that this work will assist to focus extra researcher attention towards the growing iris biometric.

REFERENCES

1. Jeffrey F., Cohn, Jing Xiao, Tsuyoshi Moriyama, Zara Ambadar, and Takeo Kanade. "Automatic recognition of eye blinking in spontaneously occurring behavior." Behavior Research Methods, Instruments, & Computers 35, no. 3 (2003): 420-428.
2. Jong Hyun, Park, and Moon Gi Kang. "Iris recognition against counterfeit attack using gradient based fusion of multi-spectral images." In Advances in Biometric Person Authentication, pp. 150-156. Springer Berlin Heidelberg, 2005.
3. EuiChul, Lee, Kang Ryoung Park, and Jaihie Kim. "Fake iris detection by using purkinje image." In Advances in biometrics, pp. 397-403. Springer Berlin Heidelberg, 2006.
4. Andrzej, Pacut, and Adam Czajka. "Aliveness detection for iris biometrics." In Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International, pp. 122-129. IEEE, 2006.
5. Sung Joo, Lee, Kang Ryoung Park, and Jaihie Kim. "Robust fake iris detection based on variation of the reflectance ratio between the iris and the sclera." In Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the, pp. 1-6. IEEE, 2006.
6. Masashi, Kanematsu, Hironobu Takano, and Kiyomi Nakamura. "Highly reliable liveness detection method for iris recognition." In SICE, 2007 Annual Conference, pp. 361-364. IEEE, 2007.
7. Xiaofu, He, Yue Lu, and Pengfei Shi. "A fake iris detection method based on fft and quality assessment." In Pattern Recognition, 2008. CCPR'08. Chinese Conference on, pp. 1-4. IEEE, 2008.
8. Zhuoshi, Wei, XianchaoQiu, Zhenan Sun, and Tieniu Tan. "Counterfeit iris detection based on texture analysis." In Pattern Recognition, 2008. ICPR 2008. 19th International Conference on, pp. 1-4. IEEE, 2008.
9. Xiaofu, He, Yue Lu, and Pengfei Shi. "A new fake iris detection method." In Advances in Biometrics, pp. 1132-1139. Springer Berlin Heidelberg, 2009.
10. Zhaofeng, He, Zhenan Sun, Tieniu Tan, and Zhuoshi Wei. "Efficient iris spoof detection via boosted local binary patterns." In Advances in biometrics, pp. 1080-1090. Springer Berlin Heidelberg, 2009.