Journal of Science Engineering Technology and Management Science
Volume 03, Issue 3(1), March 2026 *ISSN: 3049-0952*
www.jsetms.com

Image Quality Assessment for Fake Biometric detection

[1] Easari Parusha Ramu, [2] M. RUTHIKA GOUD, [3] M. DIVYA, [4] V. RAVI KUMAR, [5] D. KEERTHI
[1] Associate Professor, Department of ECE, Sri Indu College of Engineering & Technology, Hyderabad.
[2,3,4,5] U.G. Scholar, Department of ECE, Sri Indu College of Engineering & Technology, Hyderabad.

Abstract

In biometric authentication systems, distinguishing between genuine traits and fake or artificially generated samples is a critical challenge, requiring the development of effective security mechanisms. This paper presents a novel software-based fake detection approach that can be applied across multiple biometric systems to identify fraudulent access attempts.

The primary goal of the proposed system is to improve the security of biometric recognition frameworks by incorporating liveness detection in a fast, user-friendly, and non-intrusive manner using image quality assessment techniques. The method is designed with low computational complexity, making it suitable for real-time applications. It utilizes 25 general image quality features extracted from a single captured image—the same image used for authentication—to differentiate between genuine and fake samples. Experimental results on publicly available datasets, including fingerprint, iris, and 2D face images, demonstrate that the proposed method performs competitively compared to existing state-of-the-art techniques. The study highlights that analyzing general image quality provides valuable information, enabling efficient and accurate discrimination between authentic biometric traits and spoofed samples.

Keywords: Image Quality, Fake Biometric Detection, self-manufactured synthetic, fingerprint recognition.

I. Introduction

Images may be two-dimensional, such as a photograph, screen display, and as well as a three-dimensional, such as a statue or hologram. They may be captured by optical devices – such as cameras, mirrors, lenses, telescopes, microscopes, etc. and natural objects and phenomena, such as the human eye or water.

The word image is also used in the broader sense of any two-dimensional figure such as a map, a graph, a pie chart, or a painting. In this wider sense, images can also be rendered manually, such as by drawing, the art of painting, carving, rendered automatically by printing or computer graphics technology, or developed by a combination of methods, especially in a pseudo-photograph.

A volatile image is one that exists only for a short period of time. This may be a reflection of an object by a mirror, a projection of a camera obscure, or a scene displayed on a cathode ray tube. A fixed image, also called a hard copy, is one that has been recorded on a material object, such as paper or textile by photography or any other digital process.
A mental image exists in an individual's mind, as something one remembers or imagines. The subject of an image need not be real; it may be an abstract concept, such as a graph, function, or "imaginary" entity. For example, Sigmund Freud claimed to have dreamed purely in aural-images of dialogs. The development of synthetic acoustic technologies and the creation of sound art have led to a consideration of the possibilities of a sound-image made up of irreducible phonic substance beyond linguistic or musicological analysis.
A still image is a single static image, as distinguished from a kinetic image. This phrase is used in photography, visual media and the computer industry to emphasize that one is not talking about movies, or in very precise or pedantic technical writing such as a standard.
A film still is a photograph taken on the set of a movie or television program during production, used for promotional purposes.
Many different aspects of human physiology, chemistry or behavior can be used for biometric authentication. The selection of a particular biometric for use in a specific application involves a weighting of several factors.identified seven such factors to be used when assessing the suitability of any trait for use in biometric authentication. Universality means that every person using a system should possess the trait. Uniqueness means the trait should be sufficiently different for individuals in the relevant population such that they can be distinguished from one another. Permanence relates to the manner in which a trait varies over time. More specifically, a trait with 'good' permanence will be reasonably invariant over time with respect to the specific matching algorithm. Measurability (collectability) relates to the ease of acquisition or measurement of the trait. In addition, acquired data should be in a form that permits subsequent processing and extraction of the relevant feature sets. Performance relates to the accuracy, speed, and robustness of technology used. Acceptability relates to how well individuals in the relevant population accept the technology such that they are willing to have their biometric trait captured and assessed. Circumvention relates to the ease with which a trait might be imitated using an artifact or substitute. No single biometric will meet all the requirements of every possible application.

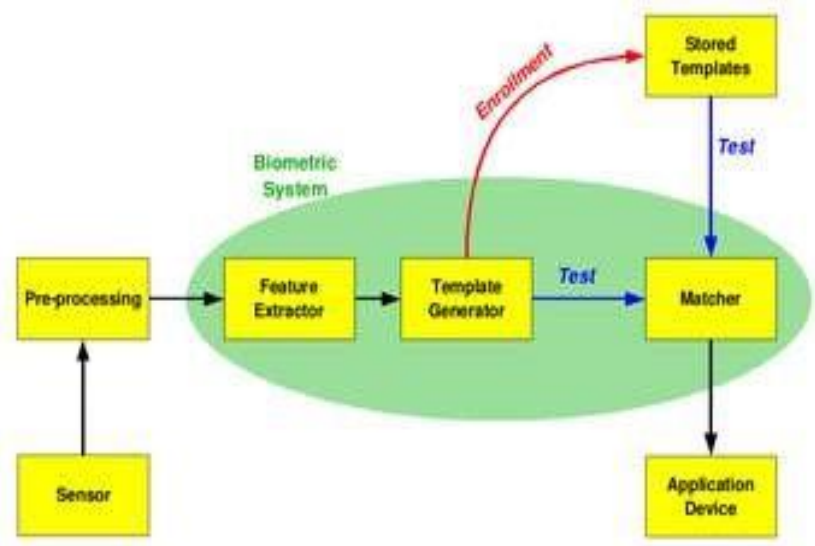

Fig 1. basic biometric system

The block diagram illustrates the two basic modes of a biometric system.[1] First, in verification (or authentication) mode the system performs a one-to-one comparison of a captured biometric with a specific template stored in a biometric database in order to verify the individual is the person they claim to be. Three steps are involved in the verification of a person.[2] In the first step, reference models for all the users are generated and stored in the model database. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold. Third step is the testing step. This process may use a smart card, username or ID number (e.g. PIN) to indicate which template should be used for comparison. 'Positive recognition' is a common use of the verification mode, "where the aim is to prevent multiple people from using same identity". [1]

Second, in identification mode the system performs a one-to-many comparison against a biometric database in attempt to establish the identity of an unknown individual. The system will succeed in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold. Identification mode can be used either for 'positive recognition' (so that the user does not have to provide any information about the template to be used) or for 'negative recognition' of the person "where the system establishes whether the person is who she (implicitly or explicitly) denies to be".[3] The latter function can only be achieved through biometrics since other methods of personal recognition such as passwords, PINs or keys are ineffective.

The first time an individual uses a biometric system is called enrollment. During the enrollment, biometric information from an individual is captured and stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The second block performs all the necessary pre-processing: it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrolled.

During the enrollment phase, the template is simply stored somewhere (on a card or within a database or both). During the matching phase, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area. Selection of biometrics in any practical application depending upon the characteristic measurements and user requirements.[2] We should consider Performance, Acceptability, Circumvention, Robustness, Population coverage, Size, Identity theft deterrence in selecting a particular biometric. Selection of biometric based on user requirement considers Sensor availability, Device availability, Computational time and reliability, Cost, Sensor area and power consumption

II. Previous Work

Due to the rapid growth of biometric technology, template protection becomes crucial to secure integrity of the biometric security system and prevent unauthorized access. Cancellable biometrics is emerging as one of the best solutions to secure the biometric identification and verification system. We present a novel technique for robust cancelable template generation algorithm that takes advantage of the multimodal biometric using feature level fusion. Feature level fusion of different facial features is applied to generate the cancellable template. A proposed algorithm based on the multi-fold random projection and fuzzy communication scheme is used for this purpose [3].

A binary iris code is a very compact representation of an iris image. For a long time it was assumed that the iris code did not contain enough information to allow for the reconstruction of the original iris. The present work proposes a novel probabilistic approach based on genetic algorithms to reconstruct iris images from binary templates and analyzes the similarity between the reconstructed synthetic iris image and the original one. The performance of the reconstruction technique is assessed by empirically estimating the probability of successfully matching the synthesized iris image against its true counterpart using a commercial matcher. The experimental results indicate that the reconstructed images look reasonably realistic. While a human expert may not be easily deceived by them, they can successfully deceive a commercial matcher. Furthermore, since the proposed methodology is able to synthesize multiple iris images from a single iris code, it has other potential applications including privacy enhancement of iris-based systems [4].

III. Proposed work

Due to the rapid growth of biometric technology, template protection becomes crucial to secure integrity of the biometric security system and prevent unauthorized access. Cancellable biometrics is emerging as one of the best solutions to secure the biometric identification and verification system. In this paper t a novel technique for robust cancellable template generation algorithm that takes advantage of the multimodal biometric using feature level fusion. Feature level fusion of different facial features is applied to generate the cancellable template. A proposed algorithm based on the multi-fold random projection and fuzzy communication scheme is used for this purpose.

IV. Different Techniques of Biometric Technology

Currently used for identity, confirmation and forensic purposes, biometric technologies can be broadly grouped into four areas with several techniques in each:

- Hands;
- Heads and face;
- Other physical characteristics; and
- Behavioural characteristics.

The first three categories are physiological and are based on measurement of physical characteristics. Except in the case of a serious disaster or operation, this biometrics is generally unaffected over time. Behavioural characteristics are more susceptible to change and can be affected by age, illness, disease, tiredness and can also be deliberately altered.

Cancellable biometrics

Cancellable biometrics refers to the intentional and systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. If a cancellable feature is compromised, the distortion characteristics are changed, and the same biometrics is mapped to a new template, which is used subsequently. Cancellable biometrics is one of the major categories for biometric template protection purpose besides biometric cryptosystem.

Although biometrics is a powerful tool against repudiation and has been widely deployed in various security systems, biometric characteristics are largely immutable, resulting in permanent biometric compromise when a template is stolen. The concept of cancelable biometrics was introduced to make a biometric template can be cancelled and be revoked like a password, as well as being unique to every application. Cancelable biometrics requires storage of the distorted version of the biometric template which provides high privacy level by allowing multiple templates to be associated with the same biometric data. This helps to promote non-likability of user's biometric data stored across various databases.

Objectives

Four objectives of designing a cancelable biometric scheme are as followed:

- Diversity: No same cancelable features can be used across various applications; therefore a large number of protected templates from same biometric feature is required.
- Reusability/Revocability: Straightforward revocation and reissue in the event of compromise.
- Non-inevitability: Non-inevitability of template computation to prevent recovery of original biometric data.
- Performance: The formulation should not deteriorate the recognition performance.

V. Algorithms Steps

Step 1: Browse Iris image

Step 2: Image Pre-processing (By using this user get the information about the image)

Step 3: Browse Finger print image

Step 4: Image Pre-processing (By using this user get the information about the image)

Step 5: Browse Facial Image

Step 6: Image Pre-processing (By using this user get the information about the image)

Step 7: Retrieve the secrete image by using above steps

Results

Below Fig. 2 Shows that the original captured image of eye.

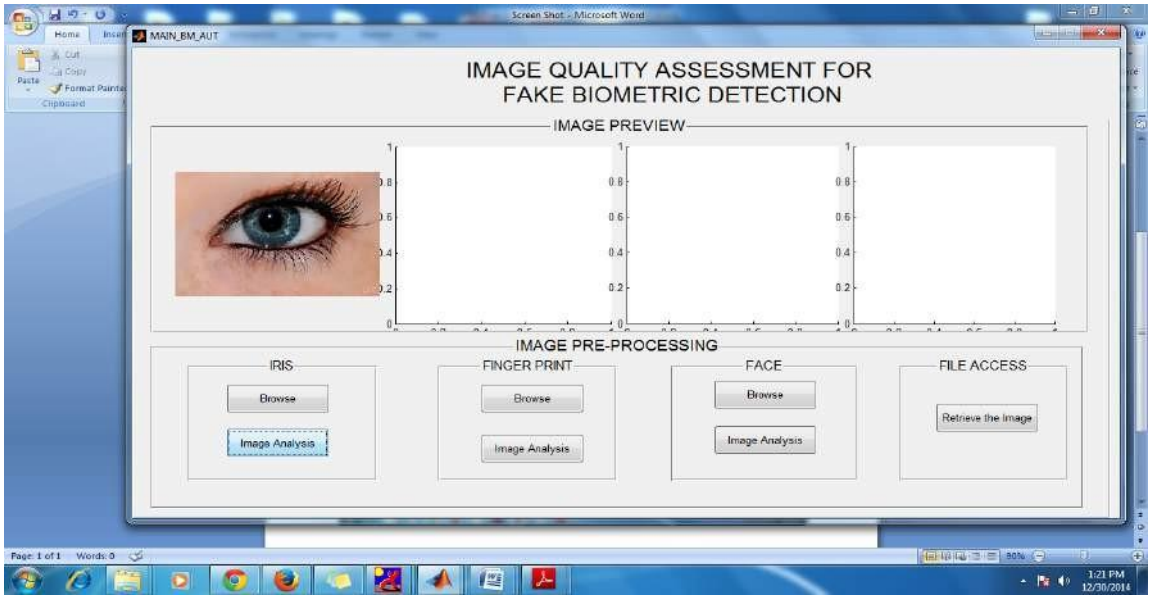

Fig 2. Image Pre-processing

Below fig.3 shows the image preview after the process of image analysis.

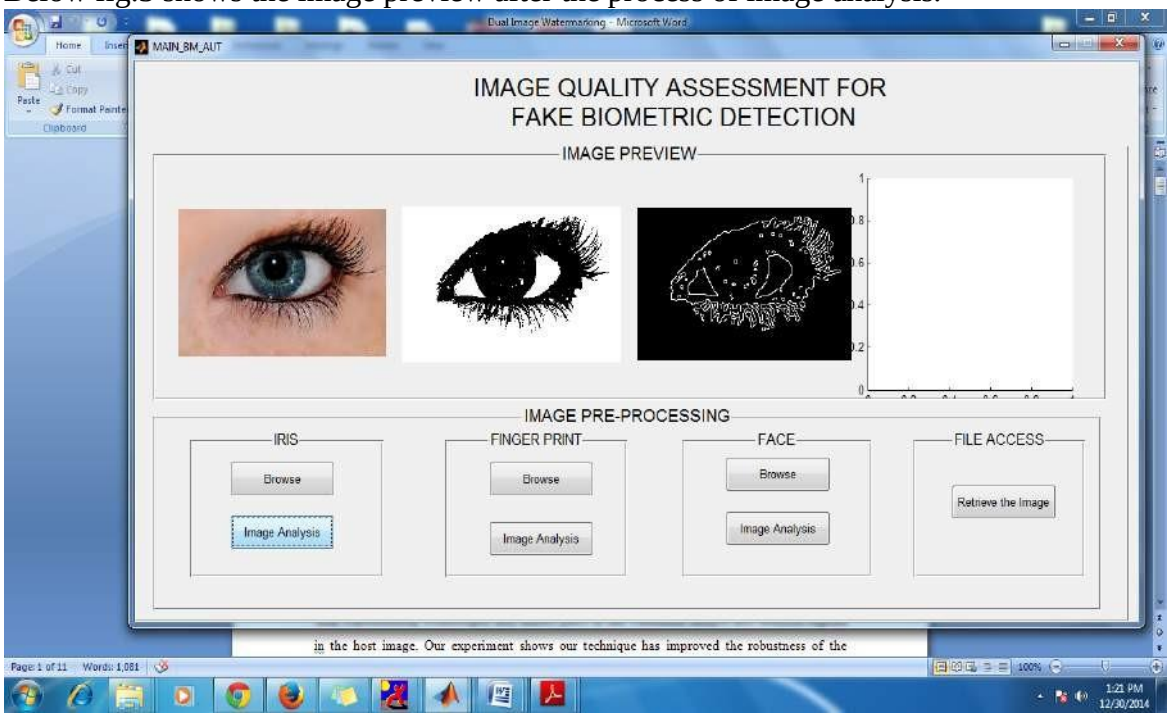

Fig 3.Image Analysis of Eye

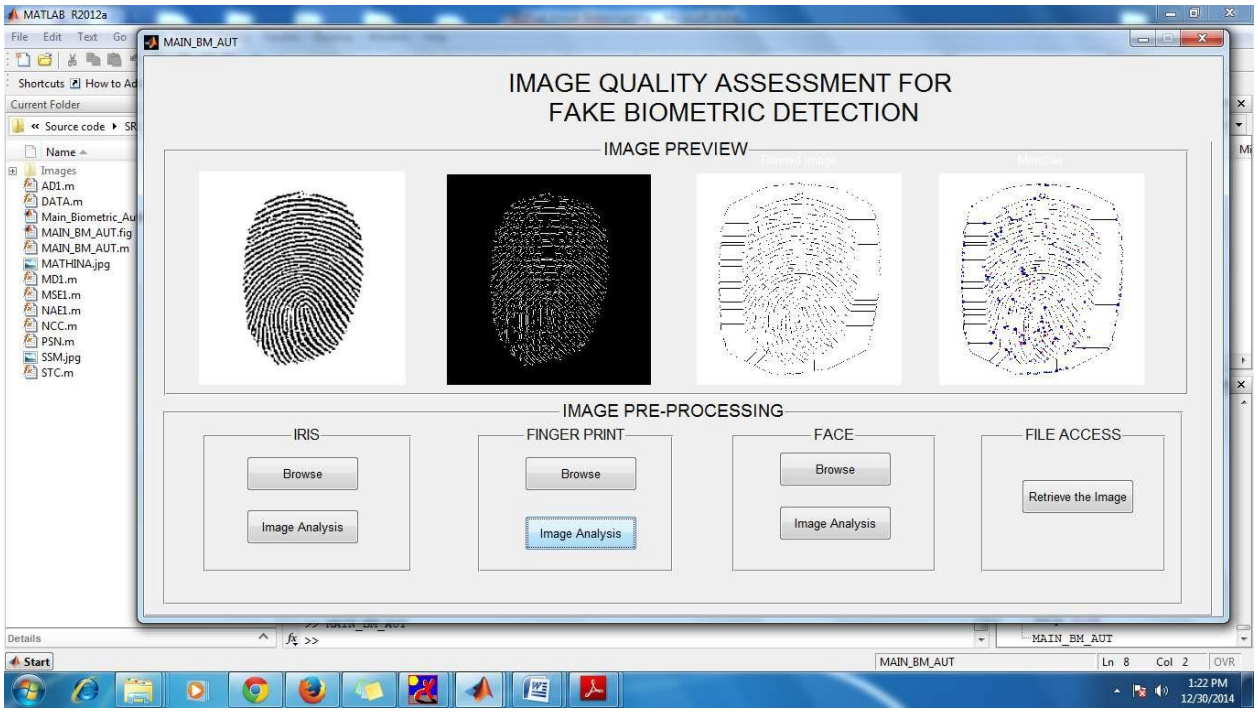

Fig 4.Image Analysis of Finger print

Above fig.4 shows the image analysis of finger print,similary this process can be applied for the face .

Conclusion

The study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years. This interest has lead to big advances in the field of security-enhancing technologies for biometric-based applications. However, in spite of this noticeable improvement, the development of efficient protection methods against known threats has proven to be a challenging task. In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different.

Future Scope

In future need for independent evaluation of biometric devices is clear. Adequate testing usually requires a special version of the software. Fingerprints have been widely used as a form of identification for many years and are well-established in many places.

References

1. Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A. Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.
2. Sahoo, SoyujKumar; Mahadeva Prasanna, SR, Choubisa, Tarun; Mahadeva Prasanna, SR (1 January 2012). "Multimodal Biometric Person Authentication : A Review". IETE Technical Review 29 (1): 54. doi:10.4103/0256-4602.93139 (inactive 2015-01-04). Retrieved 23 February 2012.
3. S. Prabhakar, S. Pankanti, and A. K. Jain, ―Biometric recognition: Security and privacy concerns,‖ IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
4. T. Matsumoto, ―Artificial irises: Importance of vulnerability analysis,‖ in Proc. AWB, 2004.
5. J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, ―On the vulnerability of face verification systems to hill-climbing attacks,‖ Pattern Recognit., vol. 43, no. 3, pp. 1027–1038, 2010.
6. A. K. Jain, K. Nandakumar, and A. Nagar, ―Biometric template security,‖ EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.
7. J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, ―A high performance fingerprint liveness detection method based on quality related features,‖ Future Generat. Comput. Syst., vol. 28, no. 1, pp. 311–321, 2012.
8. K. A. Nixon, V. Aimale, and R. K. Rowe, ―Spoof detection schemes,‖ Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423
9. ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.
10. Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.
11. K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.