Volume: 10 Issue: VI Month of publication: June 2022

DOI: https://doi.org/10.22214/ijraset.2022.44812

Voter Authentication System Using Feature Level Fusion of Iris, Face and Palmprint

Dr. CH. Ramesh[1], P. Rajesh[2], M. Harika[3], D. Laveen Kumar[4], P. Keerthana[5], G. Aditya Vishnu Vardhan[6]
[1]Professor, Department of CSE, [2],[3],[4],[5],[6] Students from Final year, B.Tech, Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh

Abstract: The authentication scheme is an important cryptographic mechanism, through which two communication parties could authenticate each other in the open network environment. To satisfy the requirement of practical applications, many authenticationschemes using passwords and smart cards have been proposed. However,passwords might be divulged or forgotten, and smart cards might be shared, lost, or stolen.

In contrast, biometric methods such as face or iris scans, have no such drawbacks. Three biometric traits are collected and stored into database at the time of enrollment. The Multimodel Biometric based user authentication systems are highly secured and efficient to use and place total trust on the authentication server where biometric verification data are stored in a database. Such systems are prone to dictionary attacks initiated at the server side. In thispaper, we propose an efficient approach based on multimodal biometrics-based user authentication and key exchange system. In this system,texture properties are extracted from the palm print, face and iris.

Duringlogin procedure the mutual authentication is done between the user and server and a symmetric key is generated on both sides, which could be used for further secure communication between the user and the server can also be overcome.

This system can be directly applied to strengthen existing password or biometric based systems without requiring additional computation.

I. INTRODUCTION

A. Digital Image Processing

The identification of objects in an image and this process would probably start with image processing techniques such as noise removal, followed by (low-level) featureextraction to locate lines, regions and possibly areas with certain textures.

The clever bit is to interpret collections of these shapes as single objects, e.g., cars on a road, boxes on a conveyor belt or cancerous cells on a microscope slide.

One reason this is an AI problem is that an object can appear very different when viewed from different angles or under different lighting.

Another problem is deciding whatfeatures belong to what object and which are background or shadows etc.

The human visual system performs these tasks mostly unconsciously but a computer requires skillful programming and lots of processing power to approach human performance.Manipulation of data in the form of an image through several possible techniques. An image is usually interpreted as a two-dimensional array of brightness values, andis most familiarly represented by such patterns as those of a photographic print, slide, television screen, or movie screen. An image can be processed optically or digitally with a computer.

II. PROBLEM FOMULATION

A. Edge detection (Iris Verification)

It is a linear filter used for edge detection. Frequency and orientation representationsof Gabor filters are similar to those of the human visual system, and they have been found to be particularly appropriate for texture representation and discrimination. In the spatial domain, a 2D Gabor filter is a Gaussian kernel function modulated by a sinusoidal plane wave. Gabor filter: (Dennis Gabor, 1946) is a linear filter whose impulse response is the multiplication of a harmonic function with a Gaussian function [18-20]. As per convolution

The Orem the convolution of Fourier Transformation (FT) of harmonic function and FT of Gaussian function is nothing but FT of a Gabor filter's impulse response

[FT(Gabor) = FT(Harmonic) FT(Gaussian)]. The filter consists of a real and an imaginary component, which represent the orthogonal directions. The two components are used individually or in a complex form. Complex:

$g(x,y;\lambda\theta, \square,\sigma,\gamma) = \exp(-(x12+ \gamma 2y12)/2\sigma 2). \exp(i.(2\pi x1/\lambda+ \square))$ (1) Real:

$g(x,y;\lambda,\theta, \square,\sigma,\gamma) = \exp (-(x12+ \gamma 2y12)/2\sigma 2). \cos (2\pi x1/\lambda+ \square)$ (2) Imaginary:

$g(x,y;\lambda,\theta, \square,\sigma,\gamma) = \exp (-(x12+ \gamma 2y12)/2\sigma 2). \sin (2\pi x1/\lambda+ \square)$ (3) Where,

$x1 = x\cos\theta+y\sin\theta$ and

$y1 = -x\sin\theta+y\cos\theta$ In eq.-1,2,3

λ: wavelength of sinusoidal factor,

θ: orientation of normal to parallel stripes,

□: phase offset,

σ: sigma of Gaussian envelope,

γ: spatial aspect ratio (specifies the ellipticity).

Daugman (J. Daugman; 1980, 1985) extended the Gabor filter into two dimensions[12].

B. Segmentation (Palm print Verification)

Threshold (image cropping) Process Segmentation involves separating an image into regions (or their contours) corresponding to objects. Usually, regions are segmented by identifying common properties. Or, similarly, contours are identified by identifying differences between regions (edges)The simplest property that pixels in a region can share is intensity. So, a natural way to segment such regions is through thresholding, the separation of light and dark regions. Thresholding creates binary images from gray-level ones by turning all pixels below some threshold to zero and all pixels about that threshold to one. If $g(x, y)$ is a thresholder version of $f(x, y)$ at some global threshold T,**Thresholding** is the simplest method of image segmentation . From a grayscale image, thresholding can be used to create binary images

C. Feature vector (Finger Print Verification)

Principal Component Analysis

The PCA method uses the statistical distribution of input samples to find the best projection bases. It is widely used in the computer vision application. The advantages of PCA method are that the principal eigenvectors are orthogonal and represent the directions where the signals have maximum variation. This property will speed up the convergence of model training and improve the system performance.

The PCA method tries to find the projection of the feature vector on a set of basevectors. Let X={xt, t=1, 2... M} be a set of M n-dimensional feature vectors.

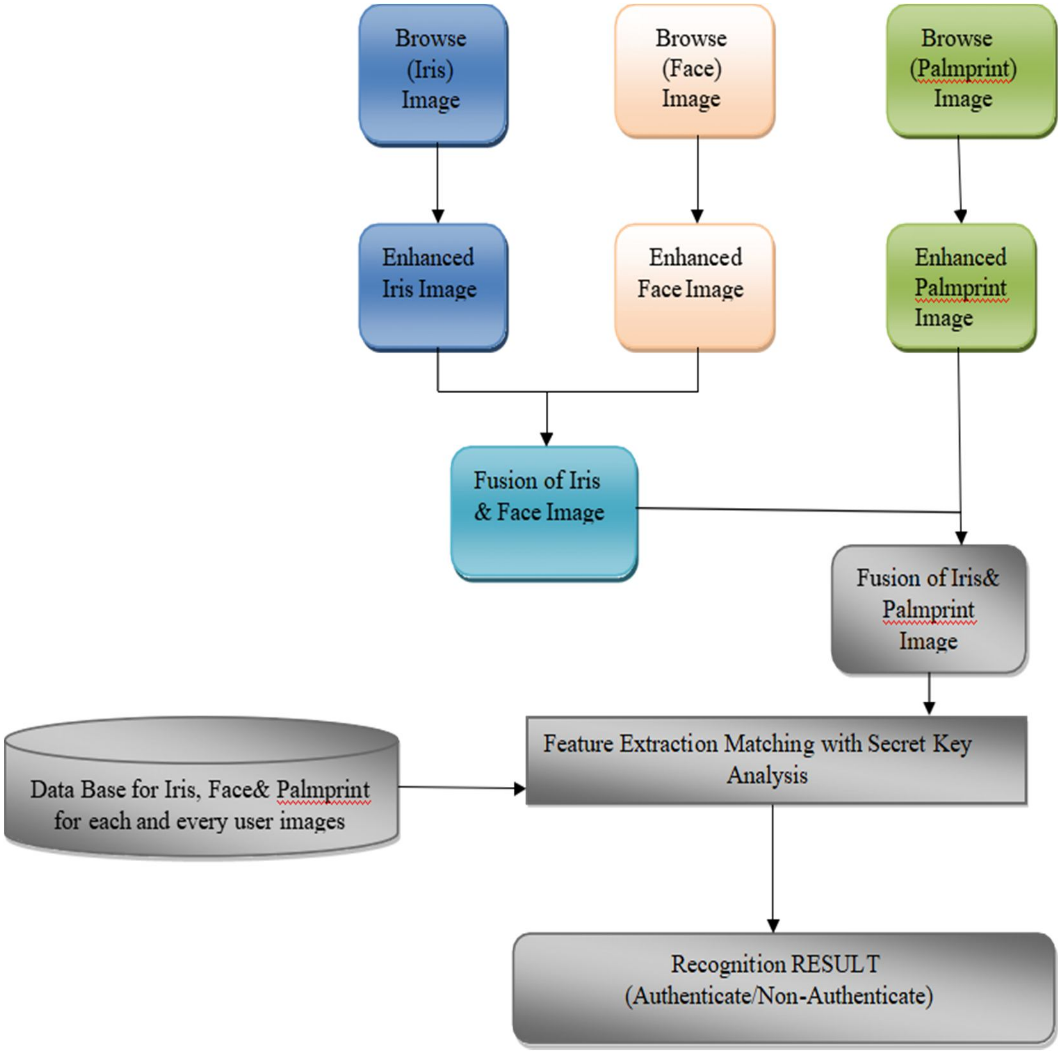
PCA algorithms are generally implemented for pattern recognition systems. Principal component analysis involves a mathematical procedure that transforms anumber of possibly correlated variables into a smaller number of uncorrelated variables called principal components. The first principal component accounts for as much of the variability in data as possible, and each succeeding component accounts for such as much of the remaining variability as possible. It is also named as the Karhunen-Loeve transform which is also called as KLT the hoteling transform.

PCA involves the calculation of eigen value decomposition of a data covariance matrix, usually after mean centering the data for each attribute. The results of PCA are usually discussed in terms of component scores and loadings. PCA involves the calculation of eigen value decomposition of a data covariance matrix. Covariance matrix or singular value decomposition of a matrix, usually after mean centering the data for each attribute. The results of a PCA are usually discussed in terms of component scores and loadings. An eigen vector of a given linear transformation is a vector which is multiplied by a constant called the eigen value as a result of that transformation. The direction of the eigen vector is either unchanged by that transformation(for positive eigen values) or reserved (for negative eigen values).

Every fingerprint in the database undergoes the PCA for obtaining the eigenvector.

The eigen vector is 512 * 1 size and is stored as another feature vector of thefingerprint.

III. BLOCK DIAGRAM


Browse (Iris) Image
Browse (Face) Image
Browse (Palmprint) Image
Enhanced Iris Image
Enhanced Face Image
Enhanced Palmprint Image
Fusion of Iris & Face Image
Fusion of Iris& Palmprint Image
Data Base for Iris, Face& Palmprint for each and every user images
Feature Extraction Matching with Secret Key Analysis
Recognition RESULT (Authenticate/Non-Authenticate)

IV. EXPERIMENTS AND RESULTS

The evaluation experimental protocol has been designed with a two-fold objective:

First, evaluate the “multi-biometric” dimension of the protection method. That is, itsability to achieve a good performance, compared to other trait-specific approaches, under different biometric modalities. For this purpose, three of the most extended imagebased biometric modalities have been considered in the experiments: iris, fingerprints and 2D face.

Second, evaluate the “multi-attack” dimension of the protection method. That is, itsability to detect not only spoofing attacks (such as other liveness detection specific approaches) but also fraudulent access attempts carried out with synthetic or reconstructed samples (see Fig. 1).

With these goals in mind, and in order to achieve reproducible results, we have onlyused in the experimental validation publicly available databases with well describedevaluation protocols. This has allowed us to compare, in an objective and fair way, the performance of the proposed system with other existing state-of-the-art livenessdetection solutions. The task in all the scenarios and experiments described in the next sections is to automatically distinguish between real and fake samples. As explained in Section III, for this purpose we build a 25-dimensional simple classifierbased on general IQMs (see Fig. 2). Therefore, in all cases, results are reported in terms of: the False Genuine Rate (FGR), which accounts for the number of false samples that were classified as real; and the False Fake Rate (FFR), which gives theprobability of an image coming from a genuine sample being considered as fake. The Half Total Error Rate (HTER) is computed as

HTER = (FGR + FFR)/2.

A. Result: Iris

For the iris modality the protection method is tested under two different attack scenarios, namely:

1) Spoofing attack and
2) Attack with synthetic samples.

For each of the scenarios a specific pair of real-fake databases is used. Databases aredivided into totally independent (in terms of users): train set, used to train the classifier; and test set, used to evaluate the performance of the proposed protection method. In all cases the final results (shown in Table II) are obtained applying two-fold cross validation. The classifier used for the two scenarios is based on QuadraticDiscriminant Analysis (QDA) [44] as it showed a slightly better performance than Linear Discriminant Analysis (LDA), which will be used in the face-related experiments, while keeping the simplicity of the whole system.

a) Results: Iris-Spoofing: The database used in this spoofing scenario is the ATVS- FIr DB which may be obtained from the Biometric Recognition Group-ATVS.1

The database comprises real and fake iris images (printed on paper) of 50 users randomly selected from the Bio Sec baseline corpus [52]. It follows the same structure as the original Bio Sec dataset, therefore, it comprises 50 users × 2 eyes ×4 images × 2 sessions = 800 fake iris images and its corresponding original samples.The acquisition of both real and fake samples was carried out using the LG Iris Access EOU3000 sensor with infrared illumination which captures bmp grey-scale images of size 640 × 480 pixels. In Fig. 4 we show some typical real and fake iris images that may be found in the dataset. As mentioned above, for the experiments the database is divided into a: train set, comprising 400 real images and their corresponding fake samples of 50 eyes; and a test set with the remaining 400 real and fake samples coming from the other 50 eyes available in the dataset.

The liveness detection results achieved by the proposed approach under this scenario appear in the first row of Table II, where we can see that the method is ableto correctly classify over 97% of the samples. In the last column we show the averageexecution time in seconds needed to process (extract the features and classify) eachsample of the two considered databases. This time was measured on a standard 64- bit Windows7-PC with a 3.4 GHz processor and 16 GB RAM memory, running MATLAB R2012b. As no other iris liveness detection method has yet been reportedon the public ATVS-FIr DB, for comparison, the second row of Table II reports theresults obtained on this database by a self-implementation of the anti-spoofing method proposed in [28]. It may be observed that the proposed method not only outperforms the state-of-the-art technique, but also, as it does not require any iris detection or segmentation, the processing time is around 10 times faster.

B. Results: Fingerprints

For the fingerprint modality, the performance of the proposed protection method is evaluated using the Liv Det 2009 DB [10] comprising over 18,000 real and fake samples. As in the iris experiments, the database is divided into a: train set, used to train the classifier; and test set, used to evaluate the performance of the protection method. In order to generate totally unbiased results, there is no overlap between both sets (i.e., samples corresponding to each user are just included in the train or the test set). The same QDA classifier already considered in the iris related experiments is used here.

1) Results: Fingerprints Spoofing Liv Det: The Liv Det 2009 DB [10] was captured in the framework of the 2009 Fingerprint Liveness Detection Competition and it is distributed through the site of the competition.4 It comprises three datasets of real and fake fingerprints captured each of them with a different flat optical sensor:
2) Biometric FX2000(569 dpi), ii) Cross Match Verifier 300CL (500 dpi), and iii) Identix DFR2100 (686dpi). The gummy fingers were generated using three differentmaterials: silicone, gelatin and playdoh, always following a consensual procedure (with the cooperation of the user). As a whole, the database contains over 18,000 samples coming from more than 100 different fingers.

Some typical examples of the images that can be found in this database are shown in Fig. 6, where the material used for the generation of the fake fingers is specified (silicone, gelatine or playdoh).
The train and test sets selected for the evaluation experiments on this database are the same as the ones used in the Liv Det 2009 competition, so that the results obtained by the proposed method based on general IQA may be directly compared to the participants of the contest.
The general distribution of the database in the train and test sets is specified in Table
IV. Results achieved on this database are shown in the first two rows of Table III. For clarity, only the best results achieved on LivDet09 for each of the individual datasets is given (second row). The best performance obtained by any of the reportedmethods on each of the three datasets is highlighted in bold in order to facilitate the comparison of the results. In [53], a novel fingerprint liveness detection method combining perspiration and morphological features was presented and evaluated onthe LivDet09 database following the same protocol (training and test sets) used in the competition.
In that work, comparative results were reported with particular implementations (from the authors) of the techniques proposed in: based on the wavelet analysis of the finger tip texture; , based on the curvelet analysis of the finger tip texture; and based on the combination of local ridge frequencies and multiresolution texture analysis. In the rows 3-7 of Table III we also present these results so that they may be compared with our proposed IQA-based method (row one). In the bottom row weshow the average execution time in seconds needed to process (extract the features and classify) each sample of the three datasets. This time was measured on a standard 64-bit Windows7-PC with a 3.4 GHz processor and 16 GB RAM memory,running MATLAB R2012b. Due to the high simplicity of the method, the computational costof processing an image depends almost exclusively on the size of the sample.
The results given in Table III show that our method outperforms all the contestants in Liv Det 2009 in two of thedatasets (Biometric and Identix), while its classificationerror is just slightly worse than the best of the participants for the Crossmatch data.
The classification error rates of our approach are also clearly lower than those reported in for the different liveness detection solutions tested. The results obtained in the fingerprint-based comparative experiments strengthen the first observations made in Section IV-A about the generality of the method, which is not only capableof adapting to different biometric modalities and attacks, but it also performs betterthan well-known methods from the state-of-the-art.

C. Results: 2D Face

The performance of the IQA-based protection method has also been assessed on a face spoofing database: the REPLAY-ATTACK DB which is publicly available from the IDIAP Research Institute.5 The database contains short videos (around 10seconds in mov format) of both real- access and spoofing attack attempts of 50 different subjects, acquired with a 320 × 240 resolution webcam of a 13-inch MacBook Laptop.
The recordings were carried out under two different conditions: i) controlled, with auniform background and artificial lighting; and ii) adverse, with natural illuminationand non-uniform background.
Three different types of attacks were considered: i) print, illegal access attempts arecarried out with hard copies of high-resolution digital photographs of the genuine users; ii) mobile, the attacks are performed using photos and videos taken with the iPhone using the iPhone screen; iii) high def, similar to the mobile subset but in thiscase the photos and videos are displayed using an iPad screen with resolution 1024× 768.

In addition, access attempts in the three attack subsets (print, mobile and high def) were recorded in two different modes depending on the strategy followed to hold theattack replay device (paper, mobile phone or tablet):

1) Hand-based

2) Fixed-support

Such a variety of real and fake acquisition scenarios and conditions makes the REPLAY- ATTACK DB a unique benchmark for testing anti-spoofing techniques for face-based systems. As a consequence, the print subset was selected as the evaluation dataset in the 2011 Competition on Counter Measures to 2D Facial Spoofing Attacks. Some typical images (frames extracted from the videos) from realand fake (print, mobile and high def) access attempts that may be found in the REPLAY-ATTACK DB are shown in Fig. 7.

The database has a perfectly defined associated evaluation protocol which considers three totally independent datasets (in terms of users): train, used to tunethe parameters of the method; development, to fix the decision threshold; and test,where final results are computed. The protocol is released with the database and has been strictly followed in the present experiments. The general structure of theprotocol is specified in Table VI.

The database is also released with face detection data. These data was used to cropand normalize all the faces to a 64×64 bounding box prior to the anti-spoofing experiments. This way the final classification results are ensured to be totally unbiased and not dependent on contextual-specific artifacts such as: unwanted changes in the background; different sizes of the heads a black frame due to an imperfect fitting of the attack media on the capturing device screen, etc. As the proposed IQA-based method is a single-image technique (i.e., it just needs one input image and not a sequence of them), each frame of the videos in the

REPLAY-ATTACK DB has been considered as an independent sample. Therefore,classification (real or fake) is done on a frame-by-frame basis and not per video. InTable V we show the results obtained on the test set by the proposed method using in this case a standard classifier based on Linear Discriminant Analysis (LDA), as for the face problem it showed slightly better performance than the QDA classifier used in the previous two cases (iris and fingerprints).

In the bottom row we show the average execution time in seconds needed to process(extract the features and classify) each sample of the three datasets (print, mobile and high def, as the grand test scenario is a combination of the previous three as is explained below). As in the iris and fingerprint experiments, this time was measured on a standard 64-bit Windows7-PC with a 3.4 GHz processor and 16 GB RAM memory, running MATLAB R2012b. Recall that the print, mobile and high def scenarios refer to the type of artifact being used as forgery and not to the acquisitiondevice, which is de same for all cases (320×240 resolution webcam of a 13-inch MacBook Laptop). Therefore, as expected, the sample average processing time in all the datasets is almost identical.

In the grand test experiments (also defined in the associated protocol) the protectionmethod is trained using data from the print, mobile and high-def scenarios, and testedalso on samples from the three types of attacks. This is probably the most realistic attack case, as, in general, we cannot know a priori the type of artifact (paper, mobilephone or tablet) that the attacker will use to try to break into the system. Results in Table V are also presented in terms of the type of strategy followed to hold the attackreplay device: hand-based, fixed-support or all (where data of the previous two typesare used)

The performance shown by the proposed algorithm in the face-based evaluation confirm the conclusions extracted from the iris and fingerprint experiments: the IQA-based protection method is able to adapt to different modalities, databases andattacks performing consistently well in all of them.

In different LBP-based anti-spoofing techniques (partially based on the study presented in were tested following the exact same protocol used in the present work.Results were only reported on the grand test scenario considering all types of supports (hand and fixed). A comparison between both protection approaches (IQA-based and LBP-based) appears in Table VII. The error rates of all methods are verysimilar, however, the IQA-based has the advantage of its simplicity and generality.

However, for reference, in Table VIII we present the results obtained by the differentparticipants in the competition compared to the performance of our method withoutdoing the cropping and normalization of the videos.

We can observe that, even though many of the contestants were using a sequence of frames to classify each video (with the complexity and speed decrease that this entails), our proposed IQA-based method performs similarly to the top ranked systems.

Furthermore, several of the algorithms presented to the competition are based on motion- detection of the face and, therefore, their ability to detect fake access attempts carried out with replayed motion videos (mobile and high def scenarios) would be at least under question. It should also be noted that in many applications there is no access to a video of the user (i.e., no temporal information is available).For these scenarios, many of the anti-spoofing solutions presented at the competition (marked with motion in Table VIII) would not be usable as they are not designed to work on a single static face image.

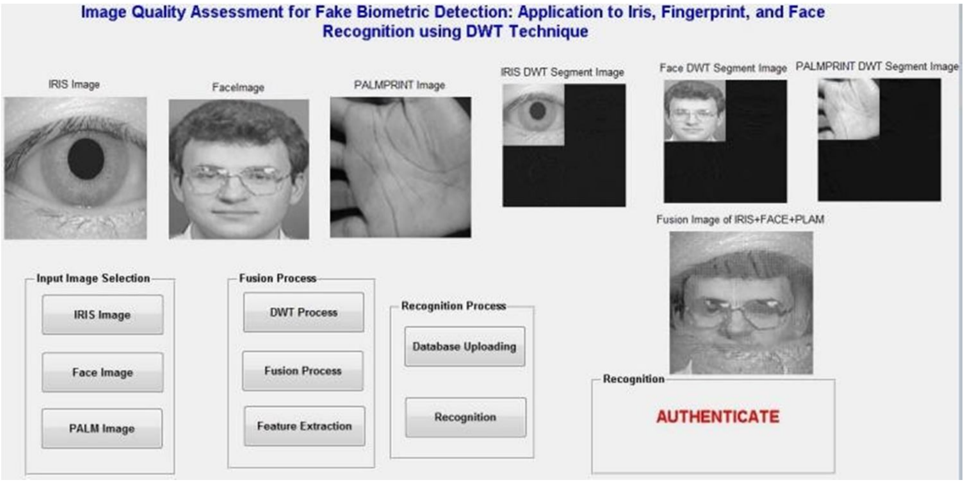


Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition using DWT Technique

AUTHENTICATE

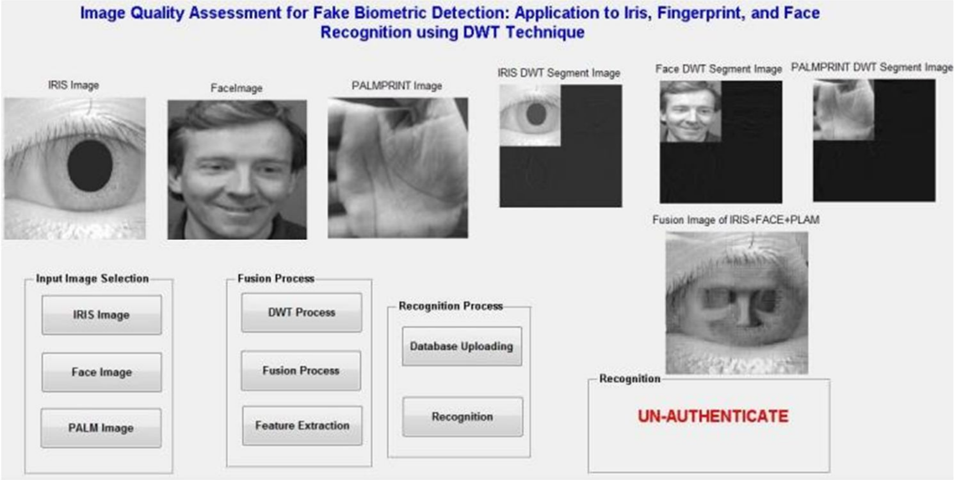


Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition using DWT Technique

UN-AUTHENTICATE

V. 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 inthe 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. Simple visual inspection of an image of a real biometric trait and a fake sample of the same trait shows that the two images can be very similar and even the human eyemay find it difficult to make a distinction between them after a short inspection. Yet,some disparities between the real and fake images may become evident once the images are translated into a proper feature space. These differences come from the fact that biometric traits, as 3D objects, have their own optical qualities (absorption, reflection, scattering, refraction), which other materials (paper, gelatin, electronic display) or synthetically produced samples do not possess. Furthermore, biometric sensors are designed to provide good quality samples when they interact, in a normal operation environment, with a real 3D trait.

If this scenario is changed, or if the trait presented to the scanner is an unexpected fake artifact (2D, different material, etc.), the characteristics of the captured image may significantly vary. In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. Following this “quality-difference” hypothesis, in the present research work we have explored the potential of general image quality assessment as a protection tool against different biometric attacks (with special attention to spoofing).

For this purpose we have considered a feature space of 25 complementary image quality measures which we have combined with simple classifiers to detect real andfake access attempts. The novel protection method has been evaluated on three largely deployed biometric modalities such as the iris, the fingerprint and 2D face, using publicly available databases with well defined associated protocols. This way,the results are reproducible and may be fairly compared with other future analogue solutions.

Several conclusions may be extracted from the evaluation results presented inthe experimental sections of the article:

1) The proposed method is able to consistently perform at a high level for different biometric traits (“multi-biometric”);

2) The proposed method is able to adapt to different types of attacks providing for all of them a high level of protection (“multi-attack”);

REFERENCES

[1] 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.

[2] T. Matsumoto, “Artificial irises: Importance of vulnerability analysis,” inProc. AWB, 2004.

[3] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, “On the vulnerability of face verification systems to hill-climbing attacks,” Pattern Recognize., vol. 43, no. 3, pp. 1027–1038, 2010.

[4] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,”EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.

[5] 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.

[6] 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.

[7] ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.

[8] Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.

[9] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.

[10] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, et al., “First international fingerprint liveness detection competition— LivDet 2009,” in Proc. IAPR ICIAP, Springer LNCS-5716. 2009, pp. 12–23.

[11] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, et al., “Competition on countermeasures to 2D facial spoofing attacks,” in Proc. IEEE IJCB, Oct. 2011, pp. 1–6.

[12] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, “Evaluation of direct attacks to fingerprint verification systems,” J. Telecommunication. Syst., vol. 47, nos. 3–4, pp. 243–254, 2011.

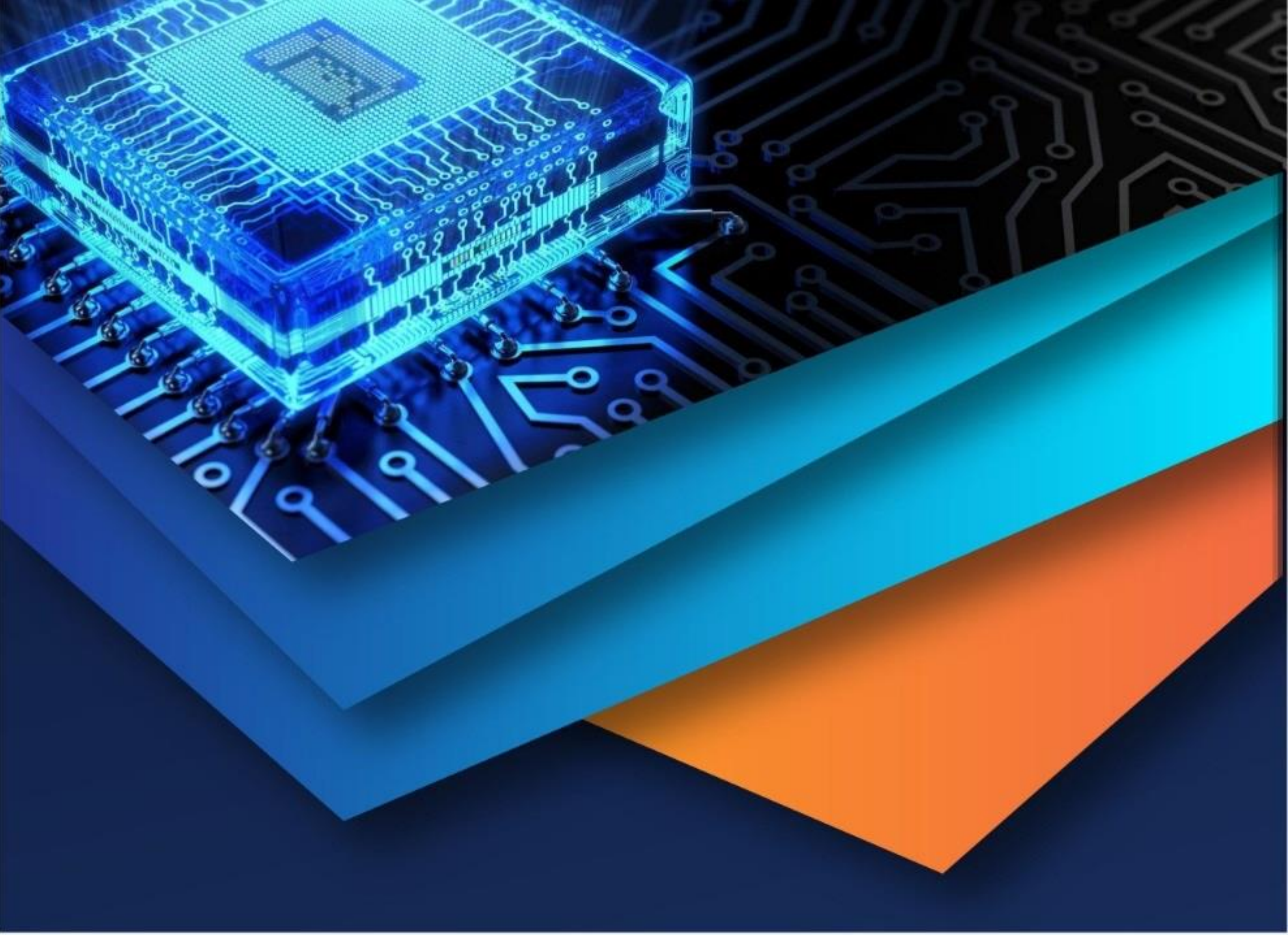
[13] A. Anjos and S. Marcel, “Counter-measures to photo attacks in face recognition: A public database and a baseline,” in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.

[14] Biometrics Institute, London, U.K. (2011). Biometric Vulnerability Assessment Expert Group [Online]. Available: http://www.biometricsinstitute.org/pages/biometric-vulnerability- assessment- expertgroup-bvaeg.html

[15] (2012). BEAT: Biometrics Evaluation and Testing [Online]. Available: http://www.beat-eu.org/

[16] (2010). Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available: http://www.tabularasa-euproject.org/

[17] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, et al., “An evaluation of direct and indirect attacks using fake fingers generated from ISO templates,” Pattern Recognize. Lett., vol. 31, no. 8, pp. 725–732, 2010.



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR:
7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR:
7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY