ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

Forgery Detection in Biometric System with Efficient Image Analysis

Priyanka C. Wankar[1], Prof. Mrudula S. Nimbarte[2]

M. Tech Student, Dept. of Computer Science & Engineering, B.D. College of Engineering, Sevagram, Wardha, India

Assistant Professor, Dept. of Computer Science & Engineering, B.D. College of Engineering, Sevagram, Wardha, India

ABSTRACT: To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. The iris and finger print are among the most promising biometric authentication that can precisely identify and analysis a person as their unique textures can be quickly extracted during the recognition process. This biometric detection and authentication often deals with non-ideal scenarios such as blurred images, off-angles, reflections, expression changes. In this project, we presented a fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to detect the fraudulent biometric samples. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using Gabor wavelet for features extraction. The experimental results, obtained on publicly available data sets of fingerprint and iris, show that the proposed method is highly competitive compared with other state-of-the-art approaches. For the preprocessing we used low pass filter. For the Feature Extraction we have used Gabor wavelet. The classification is done by SVM which is an efficient classification.

KEYWORDS: SVM, PSNR, MSE, NCC, Gabor Wavelet

I. INTRODUCTION

Security field uses three different types of authentication: Something you knows password, PIN, or piece of personal information, something you have a card key, smart card, or token (like a Secure ID card), something you area biometric. The word biometrics comes from two Greek words “bio” and “metrics” which means life measurement. Any characteristic can be used as a biometric identifier if every person possesses the characteristic, it varies from person to person, its properties do not change considerably over time, and it can be measured manually or automatically.

Biometrics is the measurement of biological data. The term biometrics is commonly used today to refer to the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics, such as signatures. Since many physical and behavioral characteristics are unique to an individual, biometrics provides a more reliable system of authentication than ID cards, keys, passwords, or other traditional systems. With the increasing requirements for higher security level, biometric systems have been widely used for many applications. Iris recognition is one of the most promising methods because the iris has the great mathematical advantage that its pattern variability among different persons is enormous. In addition, as an internal (yet externally visible) organ of the eye, the iris is well protected from the environment and stays unchanged as long as one lives.

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. Fake biometrics means by using the real images (figure 1 Iris images captured from a printed paper and figure 2 Fingerprint captured from a dummy finger) of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Biometrics system is more secure than other security methods like password, PIN, or card and key. Biometric systemic of different type that are face recognition system, fingerprint recognition system, iris recognition system, hand geometry recognition system (physiological biometric), signature recognition system, voice recognition system (behavioural biometric). Among the different threats analysed, the so-called direct or spoofing attacks have motivated the biometric community to study the

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

vulnerabilities against this type of fraudulent actions in modalities such as the iris, the fingerprint, the face and the signature, or even the gait and multimodal approaches. In these attacks, the intruder uses some type of synthetically produced artefact (e.g., gummy finger, printed iris image or face mask), 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 are 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.

Multi biometric system means a biometric system with more than one biometric system. A multi biometric system uses the multiple source of information for recognition of person authentication. Multi biometric system is more secure than single biometric system. Liveness detection technique is used to find out the fake biometrics. Image assessment is forced by supposition that is predictable that a fake image and real sample will have different quality acquisition. Predictable quality differences between real and fake samples may contain: colour and luminance levels, general artefacts, quantity of information, and quantity of sharpness, found in both type of images, structural distortions or natural appearance.

For example, figure 1 shows iris images captured from a printed paper are more likely to be fuzzy or out of focus due to shaky; face images captured from mobile device will almost certainly be over-or under-discovered; and it is not rare that fingerprint images which is shows in figure 2 captured from a dummy finger. In addition in ultimate attack in which an unnaturally produced image is directly injected to the communication channel before the feature extractor, this fake sample will most probably not have some of the properties found in natural images.

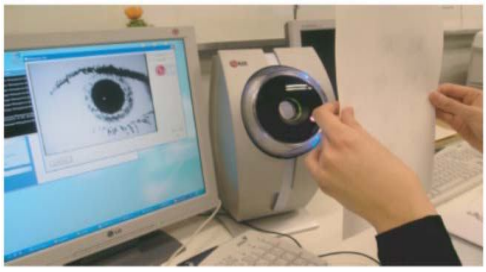

Figure 1: Fake iris sample

Figure 2: Fake fingerprints sample

II. RELATED WORK

Javier Galbally, Sébastien Marcel [1], proposed software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts 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 assessment. The proposed 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 distinguish between legitimate and impostor samples. The face, iris and finger print are among the most promising biometric authentication that can precisely identify and analysis a person as their unique textures can be quickly extracted during the recognition process. This biometric detection and authentication often deals with non-ideal scenarios such as blurred images, off-angles, reflections, expression changes. These precincts imposed by uni modal biometrics can be pound by incorporating multimodal biometrics. For this reason, S. Wilson and 2A, Lenin Fred [2], proposed a new Effective fake detection method that can be used in multiple biometric systems to detect different types of fake access attempts. An important feature and objective of the proposed system is to enhance the image quality and very low degree of complexity for security of biometric recognition frameworks.

S.Hemalatha, Amitabh Wahi, Ph.D [3], “Biometrics” refers to the technologies that measure and analyse human body characteristics for security purposes. It identifies and verifies the identity of a person based on one or more physiological and behavioural characteristics. That is Human body as password. The most common physical biometric traits includes fingerprint, face, ear, iris, retina, hand geometry, palm print, DNA etc. Behavioural biometric traits include signature, gait, key strokes, speech patterns etc. Each biometric has its own strength and limitations and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

accordingly each biometric is used in identification (authentication) application. This paper concentrates on spoof attack against face recognition system, i.e. in this type of attack a fake biometric can be presented to sensor. This paper discusses about Introduction to The Face biometric system, Spoofing attack in Face recognition system, Liveness detection in face recognition system. Mukesh Rinwa, Bharat Borkar[4], given the information on the developments in person's identification using Biometric technology method. They used this technology to ensure to identify a person weather he/she is real person or a fake person and to increase the security of biometric reorganization frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner.

For the weakness in the Gabor wavelet transform, Zhang Chun[11], proposes the improved algorithm. The improved algorithm first transforms and extracts the face image by using Gabor wavelet transform and then reduces dimensions of the image by using PCA algorithm for extracted high-dimension face feature vector. Smriti Rastogi, Dr. D. Malath [12], in which four existing methods of detecting coloured texture lenses and high resolution iris images in iris recognition systems, are compared and analyzed based on – False Acceptance Ratio (FAR), False Reject Ratio (FRR), Correct classification Rate (CCR). Anmin Liu, Weisi Lin, Senior Member, IEEE, and Manish Narwaria[15], proposed a new image quality assessment(IQA) scheme, with emphasis on gradient similarity.

Recent advances in biometric technologies coupled with the increased threatsin information security has proliferated the applications of biometric systems to safe-guard information and its supporting processes, systems and infrastructures. In this paper, Sharifah Mumtazah Syed Ahmad, Borhanuddin Mohd Ali and Wan Azizun Wan Adnan [17], discusses the technical issues and challenges faced by biometric technologies within the physical and logical access control applications of information security.

Younghwan Kim, Jang-HeeYoo, and Kyoungho Choi[22], presented a motion and similarity-based fake detection algorithm for biometric face recognition systems. First, an input video is segmented as foreground and background regions. Second, the similarity is measured between a background region, i.e., a region without a face and upper body, and an original background region recorded at an initializing stage. Third, a background motion index is calculated to indicate the amount of motion in the background region compared with the motion in the foreground region. By combining the result of similarity and the result of background motion index, a fake video can be detected robustly with a regular USB camera.

III. PROPOSED METHODOLOGY

1. Gabor Wavelet

Gabor expansion is a method to indicate a time function by using time and frequency. The equation for solving Gabor expansion factor is called as Gabor transform. The weakness of the traditional Gabor transform is that the window size can not be changed after it is fixed, so the focus cannot be changed and the signals can not be analyzed with multiple resolutions. To solve this problem, researchers combine Gabor theory with the wavelet theory and propose Gabor wavelet. The Gabor wavelet features multi-resolution feature of the wavelet transform and restriction and direction of the Gabor function.

$$G f(w,\tau) = \int_{-\infty}^{\infty} f(t)\, g(t-\tau) e^{-i\omega t}\, dt \qquad (1)$$

$g(t-\tau)e^{-i\omega t}$ is the integral kernel. The magnitude of the sine component of the frequency ω is measured around the point τ in this transform. Generally the real dual function with centralized energy at the low frequency is selected as $g_a(t)$. Gauss function is selected as the window function in Gabor. After corresponding Fourier transform, the obtained function is still a Gauss function, so the window Fourier transform has local function in time domain and frequency domain. Assume that the window function is $g_a(t)$, we can get:

$$g_{a(t)} = \frac{1}{2\sqrt{\pi a}} e^{-t^2/4a} \qquad (2)$$

A decides the window width. The Fourier transform of ga(t)is expressed as ga(w) ,

$$G_{a(w)} = \int_{-\infty}^{\infty} g_a(t) e^{-i\omega t} dt$$

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

$$= \int_{-\infty}^{\infty} \frac{1}{2\sqrt{\pi a}} e^{-\frac{t^2}{4a}} e^{-i\omega t} dt = \frac{1}{2\sqrt{\pi a}} \int_{-\infty}^{\infty} e^{-(\frac{t^2}{4a}+jwt)} dt e^{-aw^2} \quad (3)$$

From the above equation, we can get:

$$\int_{-\infty}^{\infty} Gf(w,\tau)d\tau = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} f(t)\, g_a(t-\tau)e^{-i\omega t} d = F(w) \quad (4)$$

Obviously the signal f (t) decomposes the spectrum F(w) of the f(τ) by the window width after Gabor transform and extracts local information. When τ shifts in the whole time axis, the complete Fourier transform is proposed. The corresponding reconstruction equation is:

$$f(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} G_a(w)\ g(t-\tau)e^{-i\omega t}\, dwdt \quad (5)$$

The window Fourier transform complies with the law of the energy conservation, namely:

$$\int_{-\infty}^{\infty}|f(t)|^2\, dt = \frac{1}{2\pi}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty}|G_a(t)|^2 dwd\tau \quad (6)$$

Notice that the integral kernel $g(t - \tau)e^{- jwt}$ has same supporting area for all ω and τ , but the cycle will change with ω. The supporting area indicates the definition domain of a function or the variant t of the signal f(t) . When t takes a value in the definition area, the value domain of f(t) is not zero. The signal or process decreases to zero outside the support area. To study the local feature of the time domain of the window Fourier transform, we should study the feature of $|g_{w,\tau}|^2$, and $|G_{w,\tau}|^2$, . Here $G_{w,\tau}$ is the Fourier transform of $g_{w,\tau}$. The Fourier transform complies with the law of the energy conservation, so Parseval theorem is applicable, namely:

$$\int_{-\infty}^{\infty} f(t)\overline{g_{w,\tau}}(t) = \frac{1}{2\pi}\int_{-\infty}^{\infty} F(w)\overline{G_{w,\tau}}(w)dw \quad (7)$$

Here g(t) and G(w) are the complex conjugate function of $g_{w,\tau}$ and $G_{w,\tau}$. For real number, two expression modes are equivalent. If the integral calculation of the multiplication in the above function is expressed with the inner product symbol, we can get:

$$\langle f, y\rangle = \int_{-\infty}^{\infty} f(x)y(x)dx \qquad f, y \in L^2(R) \quad (8)$$

f and y are the square integral function in the real number domain, we can get:

$$\langle f, g_{w,\tau}\rangle = \frac{1}{2\pi}\langle G_{w,\tau}, F(w)\rangle \quad (9)$$

For f(x) = y(x) , we can get:

$$\langle f, f\rangle = \int_{-\infty}^{\infty}|f(x)|^2\, dt = \|f(x)\|^2$$

f(x) is called as f(x) norm.

This physical meaning of this expression indicates that the conjugate variant (w,t) of the time domain t and frequency domain w is symmetric in Fourier transform, so the Fourier transform and Fourier transform of the adding window are symmetric. If the angle frequency variant r replaces the time variant t and the frequency domain window function G(r-w) is used to replace the time domain window function g(t-τ) , we can get:

$$Gf(w,t) = \frac{1}{2P}F(r)G(r-w)e^{-i\omega t}e^{-j\omega t}dr = \frac{1}{2P}F(r)G_{w,t}(r)e^{-j\omega t}dr \quad (10)$$

$\overline{G_{w,\tau}}(r)$ is the Fourier transform of the time domain window function $G_{w,\tau}(t)$. This equation indicates that the signal F(r) of the frequency domain gets the local information of F(r) around the frequency domain ω via the window adding of the window function $G_{w,\tau}(r)$.

$$F(w) = \overline{G}(r-w)F(r) \quad (11)$$

If the selected window function has good local nature in the time domain and frequency domain, the Fourier transform gives the local time-frequency of the signal f(t) , so it can facilitate to extract precise information of the signal f(t) in the time domain and time.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

IV. 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, its ability to achieve a good performance, compared to other trait-specific approaches, under different biometric modalities. For this purpose two of the most extended image-based biometric modalities have been considered in the experiments: iris and fingerprints.
• Second, evaluate the "multi-attack" dimension of the protection method. That is, its ability to detect fraudulent access attempts carried out with synthetic or reconstructed samples.

With these goals in mind, and in order to achievers producible results, we have only used in the experimental validation publicly available databases. This has allowed us to compare, the performance of the proposed system with other existing state-of-the-art liveness detection solutions. The task in *all* the scenarios and experiments described in the next sections is to automatically distinguish between real and fake samples. For this purpose we used Gabor wavelet. 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 the probability 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.

- Results of Iris

For the iris modality the protection method is tested under two different attack scenarios, namely: *i*) spoofing attack and *ii*) attack with synthetic samples. For each of the scenarios a specific pair of real-fake databases is used. Databases are divided 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.

1) 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.The database comprises real and fake iris images (printed on paper) of 50 users randomly selected from the Bio Sec baseline corpus. 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 IrisAccessEOU3000 sensor with infrared illumination which captures bmp grey-scale images of size 640 × 480 pixels. In Figure 4 we show some typical real and fake iris images that may be found in the dataset.

REA

2)

FAK

3)

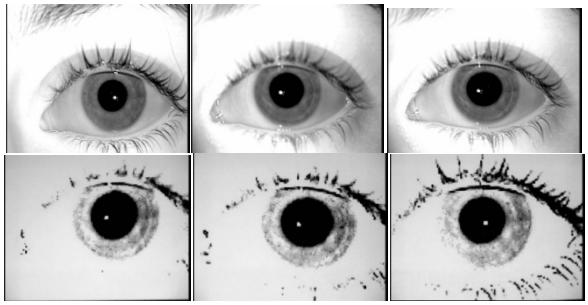

Figure 4 : Typical real iris images (top row) and their corresponding fake samples (bottom row) that may be found in the ATVS-FIrDB .The database is available at http://atvs.ii.uam.es/.

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 detection results achieved by the proposed approach under this scenario appear in the first row of Table 1, where we can see that the method is able to correctly classify over 97.5% of the samples.

2) Results: Iris-Synthetic: In this scenario attacks are performed with synthetically generated iris samples. The real and fake databases used in this case are:

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

• Real database: CASIA-IrisV1. This dataset is publicly available through the Biometric Ideal Test (BIT) platform of the Chinese Academy of Sciences Institute of Automation (CASIA). It contains 7 grey-scale 320×280 images of 108 eyes captured in two separate sessions with a self developed CASIA close-up camera and are stored in bmp format.
• Synthetic database: CASIA-Iris-Syn contains 10,000 synthesized iris images of 1,000 classes. The iris textures of these images are synthesized automatically from a subset of CASIA-IrisV1. Then the iris ring regions were embedded into the real iris images, which makes the artificial iris images more realistic. The intra-class variations introduced into the synthesized iris dataset include deformation, blurring, and rotation, which raise a challenge problem for iris feature representation and matching. More importantly, the performance results tested on the synthesized iris image database have similar statistical characteristics to genuine iris database.

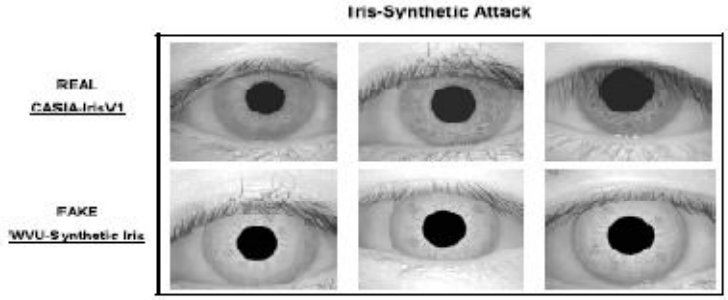

Figure 5: Typical real iris images from CASIA-Iris V1 (top row) and fake samples from Synthetic Iris DB (bottom row), used in the iris-synthetic experiments. The databases are available at http://biometrics.idealtest.org.

In Figure 5, we show some typical real and fake iris images that may be found in the CASIA-IrisV1 DB and in the Synthetic Iris DB. It may be observe that, as a consequence of the training process carried out on the CASIA-IrisV1 DB, the synthetic samples are visually very similar to those of the real dataset, which makes them specially suitable for the considered attacking scenario.
The detection results achieved by the proposed approach under this scenario appear in the second row of Table 1,where we can see that the method is able to correctly classify over 100% of the samples. And the other two rows shows the results obtained by [1].

Table 1: Results (in percentage) obtained by the proposed biometric System for Iris

	FFR	FGR	HTER
Iris – ATVS	3.75	1.25	2.5
Iris – Synthetic	0.0	0.0	0.0
Iris – ATVS [1]	4.2	0.25	2.2
Iris – Synthetic [1]	3.4	0.8	2.1

- Results of Fingerprints

For the fingerprint modality, the performance of the proposed protection method is evaluated using the ATVS-FFp_DB comprising over 816 real and fake samples. As in the iris experiments, the database are 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).

1) Results: Fingerprints ATVS-FFp_DB, It comprises the gummy fingers from which the fake fingerprint images were taken, were generated with the cooperation of the user according to the methodology described in [TS2010].

It contains fingerprint samples of the index and and middle fingers of both hands of 17 users (17 × 4 = 68 different fingers).Four samples of each fingerprint (fake and real) were captured in one acquisition session with:

- The sweeping thermal sensor by Yubee with Atmel's Fingerchip (500 dpi)

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

- The flat capacitive sensor by Precise Biometrics model Precise 100 SC (500 dpi).

This way the dataset comprises 68 fingers × 4 samples × 3 sensors = 816 real image samples and as many fake images.

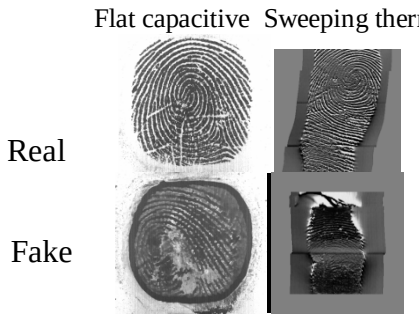

Figure 6: Typical examples of real and fake fingerprint images that can be found in the public ATVS-FFp_DB used. The database is available at http://biometrics.idealtest.org/db.

Some typical examples of the images that can be found in this database are shown in Figure 6. Results achieved on this database are shown in the Table 2. For clarity, the results achieved on ATVS-FFp_DB for each of the individual datasets are given first row and previously results obtained by [1] are shown in second row.

Table 2: Results Obtained in the ATVS-FFp_DB by the proposed method (top row) , IQA based in [1] (second row)

	Flat capacitive			Sweeping thermal		
	FFR	**FGR**	**HTER**	**FFR**	**FGR**	**HTER**
ATVS FFp_DB	0.0	2.5	1.25	2.5	7.5	5
IQA Based [1]	14.0	11.6	12.8	1.1	1.4	1.2

The results given in Table 2 show that our method out performs all the contestants in ATVS-FFp_DB in two of the datasets (Flat capacitive and Sweeping thermal), The classification error rates of our approachare also clearly lower for sweeping thermal than those reported in [1] for the different liveness detection solutions tested.

V. CONCLUSION AND FUTURE WORK

The study of the vulnerabilities of biometric systems against different types of attacks has been a very active field of research in recent years. 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 eye may find it difficult to make a distinction between them after a short inspection.

In the proposed work we developed a efficient iris and finger print fake detection system using Gabor wavelet. The main aim of this fake system is to find accuracy level of iris and fingerprint detection by pre-processing phase, feature extraction and classification. The accuracy for ATVS-FIr DB is 97.5%, CASIA-IrisV1 is 100% and ATVS-FFp DB is 99.38%.

So, several conclusions may be extracted from the evaluation results presented in the experimental sections:
i) The proposed method is able to generalize well to different databases, acquisition conditions and attack scenarios;
ii) The error rates achieved by the proposed scheme are in many cases lower than those reported by other trait-specific state-of-the-art anti-spoofing systems which have been tested and
iii) In addition to its very competitive performance, the proposed method presents some other very attractive features such as: it is simple, fast, non-intrusive and user-friendly.
The experimental results have achieved a remarkable improvement in the accuracy level.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

The present research also opens new possibilities future work, including: i) Further evaluation on other image-based modalities (e.g., face, palm print, hand geometry, vein); ii) extension of the quality measure set with new image quality measures.iii) use of video quality measures for video attacks (e.g., illegal access attempts considered in the REPLAY-ATTACK DB) and iv) analysis of the features individual relevance.

REFERENCES

1. Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian Fierrez, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition", IEEE Transaction on Image Processing, vol. 23, no. 2, February 2014.
2. S. Wilson and A. Lenin Fred , " An Efficient Biometric Multimodal Face, Iris and Finger Fake Detection using an Adaptive Neuro Fuzzy Inference System (ANFIS)", Middle-East Journal of Scientific Research 22 (6): 937-947, 2014 ISSN 1990-9233 © IDOSI Publications, 2014 .
3. S.Hemalatha, Amitabh Wahi, "A Study of Liveness Detection in Face Biometric Systems", International Journal of Computer Applications (0975 – 8887), Volume 91 – No 1, April 2014
4. Mukesh Rinwa, Bharat Borkar, "Different Modalities in Biometric Detection" in International Journal of Science and Research (IJSR),Volume 3 Issue 3, March 2014.
5. U.L.Sindhu, A.Asha, S.Suganya,M.Vinodha , " Face Recognition in Online Using Image Processing ", in International Journal of Communication and Computer Technologies Volume 02 – No.13 Issue: 02 March 2014 .
6. Manasa Priya K. V. S. N. L., Manasa K., Sumohana S. Channappayya "A Statistical Evaluation of Sparsity-based Distance Measure (SDM) as an Image Quality Assessment Algorithm" in 2014 IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP).
7. Huan Yang, Weisi Lin, Chenwei Dengy, Long Xuz "Study on Subjective Quality Assessment of Digital Compound Images" in IEEE, 2014.
8. Jinjian Wu, Weisi Liny, Guangming Shi, and Long Xuy "Reduced-Reference Image Quality Assessment with Local Binary Structural Pattern" in IEEE, 2014.
9. Ivana Chingovska, André Rabello dos Anjos, and Sébastien Marcel, "Biometrics Evaluation Under Spoofing Attacks", Ieee Transactions On Information Forensics And Security, Vol. 9, No. 12, December 2014.
10. Adam Czajka "Database of Iris Printouts and its Application: Development of Liveness Detection Method for Iris Recognition" in IEEE, 2013.
11. Zhang Chun, "Research on The Multiple Face Detection Algorithm Based on Improved Gabor Wavelet", in International Journal of Digital Content Technology and its Applications (JDCTA), Volume7, Number4, February 2013 , DOI:10.4156/jdcta.vol7.issue4.44
12. Smriti Rastogi, Dr. D. Malath "Performance Comparison Of Fake Iris DetectionMethods" in International Journal of Information and Computation Technology (IJICT), Volume 3, Number 10 (2013).
13. Amani A. Alahmadi, Muhammad Hussain, Hatim Aboalsamh, Ghulam Muhammad, George Bebis, "Splicing Image Forgery Detection Based on DCT and Local Binary Pattern", IEEE-2013.
14. Ivana Chingovska, Andr´e Anjos and S´ebastien Marcel, "On the Effectiveness of Local Binary Patterns in Face Anti-spoofing" in International Conference of the Biometrics Special Interest Group (BIOSIG), 2012.
15. Anmin Liu, Weisi Lin, Senior Member, IEEE, and Manish Narwaria, "Image Quality Assessment Based on Gradient Similarity", in IEEE Transactions On Image Processing, Vol. 21, No. 4, April2012.
16. A. Hadid, M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard, and M. Nixon, "Can gait biometrics be spoofed?" in Proc. IAPR ICPR, 2012, pp. 3280–3283.
17. Sharifah Mumtazah Syed Ahmad, Borhanuddin Mohd Ali and Wan Azizun Wan Adnan, " Technical Issues And Challenges Of BiometricApplications As Access Control Tools Of Information Security ", International Journal of Innovative Computing, Information and Control ICIC International 2012, ISSN 1349-4198 Volume 8, Number 11, November 2012 .
18. 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.
19. M. G. Martini, C. T. Hewage, and B. Villarini, "Image quality assessment based on edge preservation," Signal Process., Image Commun., vol. 27, no. 8, pp. 875–882, 2012.
20. Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in Proc. IEEE 5th Int. Conf. BTAS, Sep. 2012, pp. 283–288.
21. J. Galbally, J. Ortiz-Lopez, J. Fierrez, and J. Ortega-Garcia, "Iris liveness detection based on quality related features," in Proc. 5th IAPR ICB, Mar./Apr. 2012, pp. 271–276.
22. Younghwan Kim, Jang-Hee Yoo, and Kyoungho Choi, Member, IEEE," A Motion and Similarity-Based Fake Detection Method for Biometric Face Recognition Systems", in IEEE International Conference on Consumer Electronics (ICCE), 2011.
23. 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.
24. J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," J. Telecommun. Syst., vol. 47, nos. 3–4, pp. 243–254, 2011.