[RACE: March 2017]
ISSN 2348 – 8034
Impact Factor- 4.022

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

A SURVEY ON IRIS, FACE, AND FINGERPRINT SPOOFING DETECTION SYSTEMS

Aswathi S[*1] & Mr. Anoop K[2]
[*1]M.Tech scholar, College of Engineering Thalassery
[2]Assistant Professor, College of Engineering Thalassery

ABSTRACT

Biometrics systems have significantly improved person identification and authentication, playing an important role in personal, national, and global security. However, these systems might be deceived (or spoofed) and, despite the recent advances in spoofing detection, current solutions often rely on domain knowledge, specific biometric reading systems, and attack types. We assume a very limited knowledge about biometric spoofing at the sensor to derive outstanding spoofing detection systems for iris, face, and fingerprint modalities Iris recognition is an automated method that uses pattern-recognition techniques for biometric identification. The aim of iris image classification is to find common texture primitive in the same category of different subject and classify them to an application specific category. A Hierarchical Visual Codebook (HVC) proposed to extract the texture primitives of iris images. User authentication is an important step to protect information, and in this context, face biometrics is potentially advantageous .This paper introduces a novel and appealing approach to detect face spoofing using the spatiotemporal (dynamic texture) extensions of the highly popular local binary pattern operator. The key idea of the approach is to learn and detect the structure and the dynamics of the facial micro-textures that characterise real faces but not fake ones fingerprint liveness detection is a very difficult and challenging task. In this paper, a novel fingerprint liveness descriptor named "BSIF" is described, which, similarly to Local Binary Pattern and Local Phase Quantization-based representations, encodes the local fingerprint texture on a feature vector..

Keywords- *spoofing detection systems,Hierarchical Visual Codebook (HVC),Face recognition, LBP Operator,Liveness detection, BSIF*

I. INTRODUCTION

Biometrics human characteristics and traits can successfully allow people identification and authentication and have been widely used for access control, surveillance, and also in national and global security systems. In the last few years, due to the recent technological improvements for data acquisition, storage and processing, and also the scientific advances in computer vision, pattern recognition, and machine learning, several biometric modalities have been largely applied to person recognition, ranging from traditional fingerprint to face, to iris, and, more recently, to vein and blood flow. Simultaneously, various spoofing attacks techniques have been created to defeat such biometric systems.

There are several ways to spoof a biometric system. Indeed, previous studies show at least eight different points of attack that can be divided into two main groups: direct and indirect attacks. The former considers the possibility to generate synthetic biometric samples, and is the first vulnerability point of a biometric security system acting at the sensor level. The latter includes all the remaining seven points of attacks and requires different levels of knowledge about the system, e.g., the matching algorithm used, the specific feature extraction procedure, database access for manipulation, and also possible weak links in the communication channels within the system.

Given that the most vulnerable part of a system is its acquisition sensor, attackers have mainly focused on direct spoofing. This is possibly because a number of biometric traits can be easily forged with the use of common apparatus and consumer electronics to imitate real biometric readings (e.g., stampers, printers, displays, audio recorders). In response to that, several biometric spoofing benchmarks have been recently proposed, allowing researchers to make steady progress in the conception of anti-spoofing systems. Three relevant modalities in which

spoofing detection has been investigated are iris, face, and fingerprint. Benchmark across these modalities usually share the common characteristic of being image- or video-based.

Besides other anti-spoofing approaches such as the use of multi biometrics or challenge-response methods, special attention has been paid by researchers and industry to the liveness detection techniques, which use different physiological properties to distinguish between real and fake traits. Liveness assessment methods represent a challenging engineering problem as they have to satisfy certain demanding requirements : (i) non-invasive, the technique should in no case be harmful for the individual or require an excessive contact with the user; (ii)user friendly, people should not be reluctant to use it; (iii) fast, results have to be produced in a very reduced interval as the user cannot be asked to interact with the sensor for a long period of time; (iv) low cost, a wide use cannot be expected if the cost is excessively high; (v) performance, in addition to having a good fake detection rate, the protection scheme should not degrade the recognition performance (i.e., false rejection) of the biometric system.

II. IRIS SPOOFING DETECTION

Biometrics means life measurement. It analyses the characteristics such as Fingerprints, eye retina, iris, facial pattern, DNA etc. It can be an authentication system or Identification System. Iris recognition is one of the consistent accurate, fast and secure biometric techniques for human identification. The system captures an image from an individual's eye.

The iris in the image is then segmented and normalized for feature extraction process and then matching or classification is performed. Researchers has taken iris recognition into consideration as one of the common methods of identification like passwords, keys or credit cards. In evolution of the authentication systems, password making them subject to problems such as forgetting the password and passwords being stolen. One way to overcome the harms of authentication is to utilize biometrics traits. Iris has been preferred due to its accuracy, reliability and simplicity as compared to other biometric. The iris is surrounded by the sclera, a white region of connective tissue and blood vessels.

The iris and the pupil is covered by a clear covering known as the cornea. It displays rich texture determined by distinctive minutes.

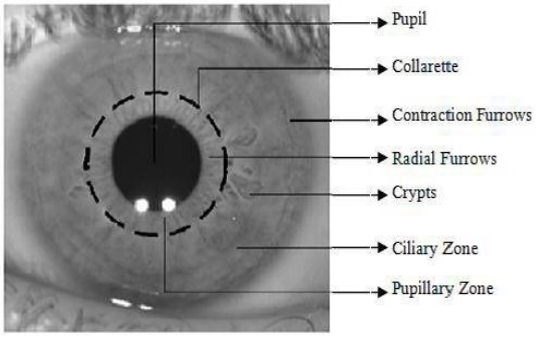

Figure 1: Eye image

Such iris texture is commonly thought to be highly discriminative between eyes and stable over individual's lifetime, which makes iris particularly useful for personal identification. In order to recognize individuals the system uses texture information of the iris.

An approximation of its statistical complexity in a sample of the human population reveals distinction corresponding to some hundred self-governing degrees-of-freedom. The significant application is to match an individuals biometrics beside a database of biometrics or classify them accordingly. Iris recognition is defined as same class such that different subjects with dissimilarity could be identified. But some application want to determine the similarity between iris images to classify them into categories i.e. live or fake, Asian or Non- Asian etc. The

classification of iris image helps to speed up large scale iris identification [1]. In this paper, two applications are consolidated into a framework for classification of iris images using Hierarchical Visual Codebook method. This method reduces the root level error accumulation.

A. Proposed work

The proposed system is organized into two phase, preprocessing phase and classification phase respectively. The system architecture is as shown in figure 2. A texture pattern representation method known as H VC is described in this section. The system contains four modules: iris image preprocessing, feature extraction, iris image representation based on HVC method, iris image classification.

a. Preprocessing phase

Iris image preprocessing is performed to enhance the image. Input images not only contain useful information but also contain noise. The noise in iris image is may be due to the eyelid, eyelashes, poor illumination etc. Preprocessing must be performed to localize, segment and normalize the iris zone. The phase includes segmentation of the iris region from original iris image and normalization of the iris regions into coordinate system.

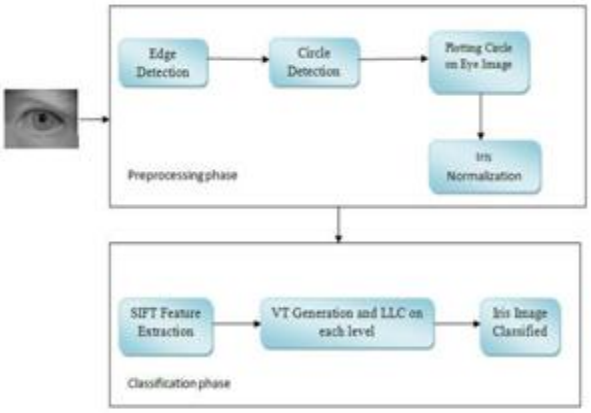

Figure 2: System architecture

1. Segmentation

Edge detection is a fundamental tool used in most image processing applications to obtain information from the image as a precursor step to feature extraction. This process detects object outline and boundaries between objects and the background in the image. Some examples of gradient-based edge detectors are Roberts, Prewitt, and Sobel operators. A Canny edge detector could be used for segmentation. It includes four steps, firstly it smoothes the image to eliminate the noise, then finds the image gradient to highlight regions with high spatial derivative, thirdly the algorithm tracks along these regions and suppresses any pixel that is not at the maximum and the gradient array is reduced by hysteresis. We adopt Canny Edge detector for edge Detection. The Hough transform is an algorithm that can be used to decide the parameters of straightforward geometric items, such as lines and circles, there in an image. The Circluar Hough transform is used to detect the pupilian and iris boundaries.

2. Normalization

The size of captured iris image is of distinct size. The same person may have the varying size because of variations in illumination, So once the iris region is successfully segmented from an eye image, the next stage is to normalize the iris region in rectangular block so that it has fixed dimensions in order to allow comparisons. The Daugman rubber sheet model is used for normalization which linearly maps the iris texture in the radial direction from pupil border and creates a dimensionless transformation in the radial direction as well. The purpose of normalization is to make iris images of equal size.

ISSN 2348 – 8034
Impact Factor- 4.022

b. Classification phase

Once the iris region is normalized in rectangular block then iris features are extracted, HVC is used to represent visual feature and for classification of iris images into different categories.

1. Feature extraction

To build a statistical representation and to obtain the common components of texture primitive in different iris images feature extraction is performed. Since in iris recognition feature extraction aims to identify local feature unique to each subject. The proposed system used Scale Invariant Feature Transform (SIFT) descriptors since it provides a generic description of local regions and in image analysis it is the most robust descriptor.

2. Hierarchical Visual Codebook (HVC)

Once the visual features are extracted then statistical texture representation using BoW model could be obtained. Visual concepts can be generated in different ways, usually through the extraction of discriminate and invariant descriptors (features) around local primitives like interest points, patches, regions, edges, followed by clustering in order to identify clusters in feature space of descriptors. The obtained clusters are considered as visual concepts or visual codeword‟s. A set of such visual codeword‟s produces a visual codebook. Traditionally, a visual codebook is learned by unsupervised clustering or vector quantization of feature vectors extracted from the local primitives in the image, often with algorithms such as k-means or robust forest. But visual codebook learning and coding are issues in BoW model. Considering these characteristics of iris image the Hierarchical Visual Codebook is used. The method includes codebook learning phase and feature coding phase.

III. FACE SPOOFING DETECTION

User authentication is an important step to protect information, and in this context, face biometrics is potentially advantageous. Face biometrics is natural, intuitive, easy to use, and less human-invasive. Unfortunately, recent work has revealed that face biometrics is vulnerable to spoofing attacks using cheap low-tech equipment. This paper introduces a novel and appealing approach to detect face spoofing using the spatiotemporal (dynamic texture) extensions of the highly popular local binary pattern operator. The key idea of the approach is to learn and detect the structure and the dynamics of the facial micro-textures that characterise real faces but not fake ones.

In authentication systems based on face biometrics, spoofing attacks are usually perpetrated using photographs, videos or forged masks. While one can also use make-up or plastic surgery as means of spoofing, photographs and videos are probably the most common sources of spoofing attacks Micro-texture analysis has been effectively used in detecting photo attacks from single face images. Recently, the micro-texture-based analysis for spoofing detection was extended in the spatiotemporal domain in which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.. In both papers, the authors introduced a compact face liveness description that combines facial appearance and dynamics using spatiotemporal (dynamic texture) extensions of the highly popular local binary pattern (LBP) approach [20]. More specifically, local binary patterns from three orthogonal planes (LBP-TOP) were considered. This variant has shown to be very effective in describing the horizontal and vertical motion patterns in addition to appearance .

LBP-based countermeasures to spoofing attacks based on the hypothesis that real faces present different texture patterns in comparison with fake ones. However, the proposed techniques analyse each frame in isolation, not considering the behavior over time. Motion is a cue explored in some works and in combination with texture can generate a powerful countermeasure. For describing the face liveness for spoofing detection, we considered a spatiotemporal representation which combines facial appearance and dynamics. We adopted the LBP-based spatiotemporal representation because of its recent convincing performance in modeling moving faces and facial expression recognition and also for dynamic texture recognition.

The LBP texture analysis operator is defined as a gray-scale invariant texture measure, derived from a general definition of texture in a local neighborhood. It is a powerful texture descriptor, and among its properties in real-

world applications are its discriminative power, computational simplicity and tolerance against monotonic gray-scale changes. The original LBP operator forms labels for the image pixels by thresholding the 3 ×3 neighborhood with the center value and considering the result as a binary number. The histogram of these 28 = 256 different labels is then used as an image descriptor. The original LBP operator was defined to only deal with the spatial information. However, more recently, it has been extended to a spatiotemporal representation for dynamic texture (DT) analysis. This has yielded to the so called volume local binary pattern operator

(VLBP). The idea behind VLBP consists of looking at dynamic texture (video sequence) as a set of volumes in the (X, Y, T) space where X and Y denote the spatial coordinates and T denotes the frame index (time). The neighborhood of each pixel is thus defined in a three-dimensional space. Then, similar to basic LBP in spatial domain, volume textons can be defined and extracted into histograms. Therefore, VLBP combines motion and appearance into a dynamic texture description.

To make VLBP computationally treatable and easy to extend, the co-occurrences of the LBP on the three orthogonal planes (LBP-TOP) was also introduced. LBP-TOP consists of the three orthogonal planes - XY, XT and YT - and the concatenation of local binary pattern co-occurrence statistics in these three directions. The circular neighborhoods are generalized to elliptical sampling to fit to the space-time statistics. The LBP codes are extracted from the XY, XT and YT planes, which are denoted as XY-LBP, XT-LBP and YT-LBP, for all pixels, and statistics of the three different planes are obtained and concatenated into a single histogram. The procedure is shown in Figure 3.1. In this representation, DT is encoded by the XY-LBP, XT-LBP and YT-LBP. Using equal radii for the time and spatial axes is not a good choice for dynamic textures , and therefore, in the XT and YT planes, different radii can be assigned to sample neighbouring points in space and time. In addition to the computational simplification, compared with VLBP, LBP-TOP has the advantage to generate independent histograms for each of the intersecting planes, in space and time, which can be treated in combination or individually. Because of the mentioned complexity issues on the implementation of a VLBP based processor, the developed spatiotemporal face liveness description uses LBP-TOP to encode both facial appearance and dynamics.

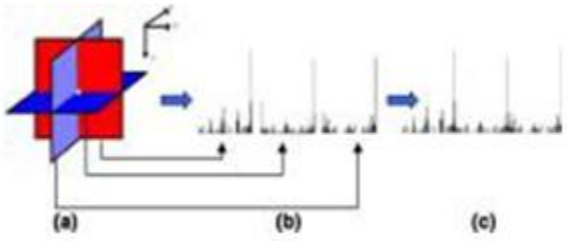

Figure 3 LBP from three orthogonal planes.

Our key idea is to learn and detect the structure and the dynamics of the facial micro-textures that characterize real faces but not fake ones. Due to its tolerance against monotonic gray-scale changes, LBP-based representation is adequate for measuring the facial texture quality and determining whether degradations due to recapturing process, e.g. the used spoofing medium, are observed. Instead of just applying static texture analysis, we exploit also several dynamic visual cues that are based on either the motion patterns of a genuine human face or the used display medium.

A. Proposed countermeasure

Figure 3 shows a block diagram of the proposed countermeasure. First, each frame of the original frame sequence was gray-scaled and passed through a face detector using modified census transform (MCT) features. Only detected faces with more than 50 pixels of width and height were considered. The detected faces were geometric normalized

ISSN 2348 – 8034
Impact Factor- 4.022

to 64 × 64 pixels. In order to reduce the face detector noise, the same face bounding box was used for each set of frames used in the LBP-TOP calculation.

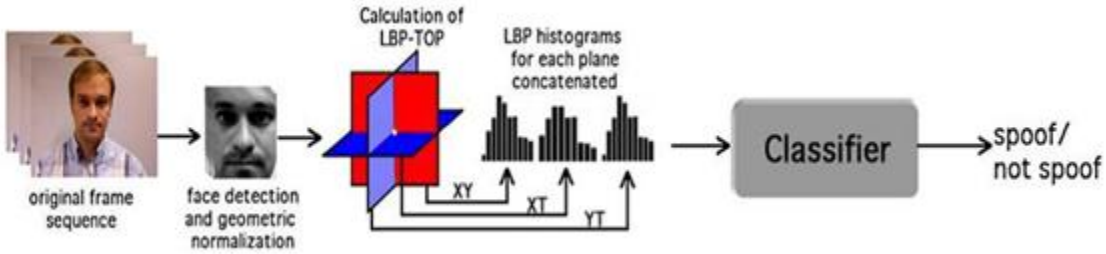

Figure 4. Block diagram of the proposed countermeasure.

Unfortunately, the face detector is not error free, and in case of error in the middle frame face detection, the nearest detection was chosen; otherwise, the observation was discarded. After the face detection step, the LBP operators were applied for each plane (XY, XT and YT) and the histograms were computed and then concatenated. After the feature extraction step, binary classification can be used to discriminate spoofing attacks from real access attempts.

IV. FINGERPRINT SPOOFING DETECTION

In Fingerprint Liveness Detection additional information is used to verify if a fingertip image is authentic. Hardware based systems use additional sensors to gain measurements outside of the fingerprint image itself to detect liveness (biometric measurements as that of the heartbeat or the blood pressure on the fingertip). Software-based systems use image processing algorithms to gather information directly from the collected fingerprint to detect liveness . This work is focused on software-based systems.

Over the years several algorithms based on the measurement of live-based characteristics (the shape of ridges, the pores presence or the perspiration), or the measurement of the amount of details lost and the presence of artifacts during the fake production have been proposed. These algorithms extract from a fingertip image a certain number of features that will be used to classify the fingerprint as either live or fake. If initially most of them seem to provide satisfying results, the introduction of new spoofing materials, beside the LivDet event, led to a general error rate increase. Among others two texture classification algorithms provided better performances: LBP (Local Binary Pattern) and LPQ (Local Phase Quantization). They were tested on the four LidDet 2011 datasets (Biometrika, Italdata, Digital and Sagem from the names of the sensors used to collect the images) and, whilst the results change depending on the considered dataset, these two algorithms always worked better than the others leading to a 12.25% error rate on average for LPQ and a 12.20% for LBP. These performances convinced us of the effectiveness of a textural analysis approach to liveness detection. But, because of the alternating success of the two algorithms, we were looking for something able to combine their qualities.

In this paper we propose the use of another texture classification algorithm, the BSIF (Binarized Statistical Image Features). It is a local image descriptor constructed by binarizingthe responses to linear filters but, in contrast to previous binary descriptors, the filters are learnt from natural images using independent component analysis (ICA). The BSIF descriptor has two parameters: the filter size and the number of features extracted. Our experiments proved that, with a sufficient number of features, this algorithm clearly outperformed both LBP and LPQ.

ISSN 2348 – 8034
Impact Factor- 4.022

A. Fingerprint representaion with binarized statistical image features

Figure 5. Learnt filters of size 9 × 9.

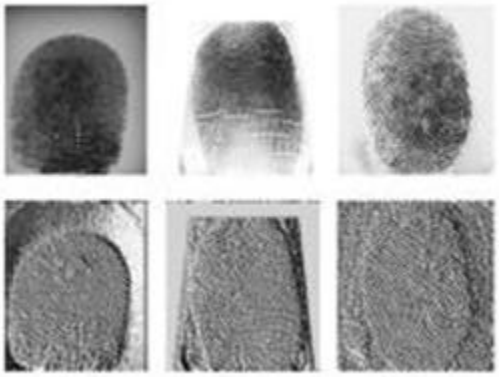

Figure 6. Some fingerprint images and corresponding BSIF codes.

Local image descriptors make the backbone of the current approaches for visual object recognition. The function of descriptors is to convert the pixel-level information into a useful form, which captures the most important image and video contents but is insensitive to irrelevant aspects caused by varying environment. In contrast to global descriptors which compute features directly from the entire image, local descriptors, which have proved to be more effective in real world conditions, represent the features in small local image patches.

Many popular local descriptors such as LBP and LPQ can be seen as statistics of labels computed in the local pixel neighborhoods through filtering and quantization. These methods describe each pixels neighborhood by a binary code which is obtained by first convolving the image with a manually predefined set of linear filters and then binarizing the filter responses. The bits in the code string correspond to binarized responses of different filters. These methods showed very good results in different computer vision problems.

For efficiently representing fingerprint images for liveness detection, we adopt a new local descriptor called BSIF (binarized Statisitcal Image features) which was recently proposed by Kannla and Rahtu for face recognition and texture classification. Inspired by LBP and LPQ, the idea behind BSIF is to automatically learn a fixed set of filters from a small set of natural images, instead of using handcrafted filters such as in LBP and LPQ. Our proposed approach for fingerprint representation consists of apply learning, instead of manual tuning, to obtain statistically meaningful representation of the fingerprint data, which enables efficient information encoding using simple element-wise quantization. Learning provides also an easy and flexible way to adjust the descriptor length and to adapt to applications with unusual image characteristics such as fingerprints.

To characterize the texture properties within each fingerprint sub-region, the histograms of pixels BSIF code values are then used. The value of each element (i.e. bit) in the BSIF binary code string is computed by binarizing the response of a linear filter with a threshold at zero. Each bit is associated with a different filter and the desired length of the bit string determines the number of filters used. The set of filters is learnt from a training set of natural image patches by maximizing the statistical independence of the filter responses.

Given an image patch X of size l × l pixels and a linear filter Wi of the same size, the filter response si is obtained by

$$S_i = \sum_{u,v} W_i(u,v)X(u,v) = W_i^T$$

where vectors w and x contain the pixels of Wi and X. The binarized feature bi is obtained by setting b_i = 1 if S_i > 0 and b_i = 0 otherwise. The filters Wi are learnt using independent component analysis (ICA) by maximizing the statistical independence of S_i. In our experiments, we used the set of filters provided by the authors of and learnt from a set of 13 natural images. There are two parameters in the BSIF descriptor: the filter size l and the length n of the bit string. The filters Wi were learnt using different choices of parameter values, each set of filters was learnt using 50000 image patches. The filters obtained with l = 9, n = 8 are illustrated in Figure 1. Some fingerprint images and corresponding BSIF codes are shown in Figure 6.

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 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. 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. 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

In iris spoofing detection, a Hierarchical Visual Codebook (HVC) method is used for iris classification. Iterative application of K-means is adopted to generate hierarchically classified irises which make a good sense about hierarchical classification. The method integrates the advantage of Vocabulary Tree and Locality-constrained Linear Coding. It avoids accumulation of errors at root level.

Inspired by the recent progress in dynamic texture, the problem of face spoofing detection was recently investigated in two independent articles using spatiotemporal local binary patterns. The key idea of the proposed countermeasures consists of analysing the structure and the dynamics of the micro-textures in the facial regions using LBP-TOP features that provide an efficient and compact representation for face liveness description Best results were achieved using a nonlinear SVM classifier, but it is important to note that experiments with a simpler LDA-based classification scheme resulted in comparable performance under various spoofing attack scenarios.

In fingerprint spoofing detection we introduced the use of BSIF, a textural analysis algorithm, in fingerprint liveness detection. We test it on the four LivDet 2011 datasets with more than promising results. There are still some open issues: how to find the right window size, the bits number or, alternatively, how to perform a features selection since the best results are obtained extracting a large number of them.

A future work should be focused on filters. We used a set of predefined filters learned from a small set of natural images. With the use of filters learned from a set of images acquired from a particular sensor (and then customized for that sensor) the results might be further improved.

ISSN 2348 – 8034
Impact Factor- 4.022

REFERENCES

[1] *Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris image classification based on hierarchical visual codebook," IEEE Trans. Pattern Anal. Mach. Intell., vol. 36, no. 6, pp. 1120–1133, Jun. 2014.*

[2] *T. de Freitas Pereira et al., "Face liveness detection using dynamic texture," EURASIP J. Image Video Process., vol. 2014, p. 2, Jan. 2014.*

[3] *L. Ghiani, A. Hadid, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection using binarized statistical image features," in Proc. IEEE Int. Conf. Biometrics, Theory, Appl., Syst. (BTAS), Sep./Oct. 2013, pp. 1–6.*