Machine Vision and Applications manuscript No.
(will be inserted by the editor)

On the use of fingernail images as transient biometric identifiers

Biometric recognition using fingernail images

Igor Barros Barbosa · Theoharis Theoharis · Ali E. Abdallah

Received: date / Accepted: date

Abstract The significant advantages that biometric recognition technologies offer are in danger of being left aside in everyday life due to concerns over the misuse of such data. The biometric data employed so far focuses on the permanence of the characteristics involved. A concept known as 'the right to be forgotten' is gaining momentum in international law and this should further hamper the adoption of permanent biometric recognition technologies. However, a multitude of common applications are short-term and therefore non-permanent biometric characteristics would suffice for them. In this paper we discuss 'transient biometrics' i.e. recognition via biometric characteristics that *will* change in the short term and show that images of the fingernail plate can be used as a transient biometric with a useful life-span of less than six months. A direct approach is proposed that requires no training and a relevant evaluation dataset is made publicly available.

Keywords Biometric recognition systems · fingernail · non-critical application · transient biometric characteristics · biometric access control · feature extraction · image segmentation

Igor Barros Barbosa
Department of Computer and Information Science,
Norwegian University of Science and Technology,
Sem Sælands vei 7-9
NO-7491 - Trondheim - NORWAY
Tel.: +47 735 93440
E-mail: igor.barbosa@idi.ntnu.no

Theoharis Theoharis
E-mail: theohart@idi.ntnu.no

Ali E. Abdallah
Birmingham City University,
Birmingham B4 7XG
E-mail: ali.abdallah@bcu.ac.uk

1 Introduction

Common non-biometric recognition systems confirm a subject's identity based on what a subject knowns (e.g password) or possesses (e.g access card). Such systems have the inherent risk of disclosure of the recognition token or theft of the possession. Such risks are largely mitigated when biometric recognition systems are employed, as they offer the possibility of confirming a subject's identity based on their own biometric characteristics, rather than what they know or carry. Biometric recognition systems thus offer protection from theft of access data, as well as convenience of use since access data does not have to be remembered or carried.

Recent biometric research has produced compelling results in terms of distinctiveness, universality and performance. However it has also concentrated on permanent biometric features, such as the iris, face or fingerprint. Individuals fearing the misuse of their permanent biometric data and are often unwilling to provide such data to any biometric solution, especially so for noncritical applications. Thus, the benefits granted by biometric technology (i.e. password and device-free access to resources), cannot be fully exploited.

The fear of misuse of biometric data is not unfounded; while an ID-card or password can be canceled, the same cannot be done with one's permanent biometric data. Compromised biometric information may be used for unauthorized recognition purposes while there is also the risk of discrimination via unauthorised use of such data (e.g. by insurance agencies). Cryptography is a plausible solution for the protection of biometric data, but this assumes that the subject trusts the biometric system. Cryptographic solutions are subject to the reliability of the entire computer system, and not just on the cryptographic algorithm used. Furthermore, a subject's trust on a system is not only determined by the quality of the system, but also by the importance and sensitivity of their biometric data. Thus, subjects may be reluctant to offer their biometric information for non-critical applications.

The social acceptability of recognition systems will become increasingly relevant as the 'right to be forgotten' gains momentum in legal systems worldwide [17]. In broad terms, this concept stems from the desire of the individual to determine his or her future without being stigmatized by actions performed in the past.

Research on cancelable biometrics [22,23] concentrates on the acceptability issue. It pre-transforms the biometric information before a biometric signature is extracted. As such a transformation is irreversible, the possibility of exploiting any stolen information is restricted by the fact that the exploiter has no access to the original biometric information. An extra security layer is provided as the transformation can be changed at any given time. Nevertheless, cancelable biometrics has to identify the theft of biometric information in order to change the transformation. Last but not least, a subject still has to entrust the biometric capture point with their permanent biometric information.

This work takes the acceptability matter a step further by proposing the use of biometric data that does change over the short term (i.e. is transient). This concept was discussed in [2] but is extensively explored here. Transient biometrics is defined as the set of biometric recognition technologies which depend on biometric characteristics that are proven to change over time. Thus, such biometric data automatically nullifies itself after a known period of time. In contrast to cancelable biometrics, it is the biometric data itself that changes over time. Transient biometrics is not proposed as a substitute to the cryptographic techniques that should be present in any biometric system, including a transient biometrics system. However, the use of transient data should give the user the assurance that if their data are compromised, it would automatically be rendered useless in a short period of time.

This work discusses the concept of transient biometrics (as a complete version of our initial presentation [2]) and advocates that fingernail plate images constitute a transient biometric characteristic. A set of algorithms for performing biometric recognition using such data are proposed and three methodologies for extracting transient biometric signatures from fingernail plate images are given. It also uses these methodologies in direct approaches (i.e no training or learning phases) for both the verification and the identification tasks. Another contribution is the discussion and selection of a viable signature fusion rule. Finally, a relevant new dataset is presented and made available to the research community to further explore this domain.

This paper is organized as follows. Section 2 presents the biometric literature previous work on biometric recognition based on non-permanent data as well as biometric work embracing fingernails. Section 3 details the technical side of the proposed approach followed by Section 4 that presents the new publicly available fingernail dataset and the experimental results of the proposed method. Finally, Section 5 concludes the paper, envisaging some future perspectives.

2 Previous Work

Transient biometrics is a new area with little previous work to report; we shall thus focus on related fields, the nearest of which is cancelable biometrics [22,23] (see section 1). As mentioned there, the major difference between cancelable biometrics and transient biometrics is that in the case of the former technology, the biometric data are protected via an irreversible transform, while in the case of the latter, the biometric data itself has only temporary recognition value. Individuals are therefore more likely to volunteer such transient data, even for non-critical applications and even when they are not entirely confident on the integrity of the capture point.

Person re-identification is a related transient problem arising in the surveillance area. The objective is to identify if a person has been previously observed in a non-collaborative subject setting using non-invasive techniques. It is therefore usually based on images, from which appearance-based local features are used to re-identify a given subject [3,8]. Such biometric systems produce a transient identification solution since it is only possible to identify a subject until this subject changes clothes or other major appearance characteristics. Appearance is one of the few options to use in re-identification within a surveillance setting where the images are often taken from a distance using a video camera; however it is questionable whether it can be regarded as a biometric trait, since it is rather easy to spoof by knowledgeable subjects.

The Bioelectrical characteristics of a fingernail are used as a biometric signature in [4]. This patent work presents a RFID chip glued over the fingernail. This embedded system measures the subjects' capacitance, which is claimed to be unique, thus creating a biometric solution based over the fingernail region.

The use of fingernail images as biometric data has been the topic of few different lines of research. The skin under a nail plate, called nail bed, is unique for each individual [11]. A special acquisition system has been designed to acquire images of the nail bed. Such images use the grooves of the nail bed for recognition purposes [26]. The fingernail surface has also been explored for a biometric authentication system [12]. This work segments the five fingernails as regions-of-interest (ROI) from a hand image using a contour segmentation algorithm. The hand is photographed while resting on a white surface. This segmentation methodology works but the employed dataset was biased with respect to the subjects' skin tones. Haar wavelet and Independent Component Analysis (ICA) are used to create a biometric signature. From the five fingernail images, three are used for training and two for testing. The methodology yields high recognition rates, yet the paper does not evaluate the effect of the growth of the fingernails on the recognition rates (i.e. no longitudinal analysis is performed). The work of [10] combines biometric information from fingernails and finger knuckles to create a multi-modal biometric system. Mel Frequency cepstral coefficients (MFCC) is employed to create a finger knuckle biometric signature. The fingernail signature is created by using both approximation and detail coefficients of a second level wavelet image decomposition. The final classification is done by a Multilayer Percptron (MLP). Similar to the work of [12], a high classification performance is achieved. Nevertheless, the work does not assess the behaviour of the information over time. In both [10, 12] the final signatures are composed from information of three fingers. There is no special fusion methodology to keep transient characteristics of the data. It is thus likely that the proposed solution learns hard biometric characteristics from the subject's fingers instead of transient information. Thus, none of the above works involving fingernails focus on their transient nature.

The work of [25] shows that the green camera channel and a 3D model of the fingertip can be used for measuring the force exerted by the fingertip. This work explores changes in coloration of the fingernail images to detect the magnitude of the force being applied to/by a specific region. A Bayesian classifier is then used to deduce the relation between force and coloration changes. In their latest work [7], the authors presented an automated calibration for a setup using an adjustable camera, controlled lighting and a magnetic levitation haptic device. Thus they are able to measure forces using only the camera image with higher accuracy. The work also presents three approaches to fingernail registration. The registration results achieved are impressive but depend on a controlled lighting setup.

The work of [6] presents a color based fingernail segmentation. The work found that the third principal component of the RGB color-space can be used to differentiate fingernails from images of skin patches. The work is assessed on a small dataset of five subjects

Our previous work assesses the use of fingernail images to create a transient biometric solution [2]. There, a small dataset was used to evaluate the longitudinal identification rate of fingernails. It was shown that recognition performance decreases to unusable rates after two months . These results are in line with physiological studies showing that healthy fingernails are replaced within three to six months [28]. In the present work we extend and complete the evaluation of fingernail images as transient biometrics by comprehensive testing in terms of algorithms and dataset.

3 Proposed Approach

The transient biometric solution presented in this work is a direct approach to the verification and identification tasks. No training is employed in the task of matching a biometric signature against a database of previously collected signatures.

An image of the right index fingernail is used for the extraction of the biometric signature. The approach will be divided into three parts. The first part outlines the image preprocessing which is necessary in order to make the image suitable for biometric signature extraction. The second part details the extraction of the biometric signature from a fingernail image. The third part describes how signatures are compared and matched.

3.1 Fingernail Plate Image Preprocessing

Image preprocessing ensures that the data delivered to the signature extraction phase fulfills some basic requirements. This should be a square image composed mainly of the fingernail and it eliminates the possibility of using potentially hard biometric information form finger-joints or finger shape [1].

To automatically segment fingernail images, an object detector as proposed in [27] and extended in [15] is employed. In this object detector, a classifier is trained with sample images of manually segmented fingernails, that match the requirements of the signature extractor, generating the so called positive samples. Negative samples are also generated using sample images with no fingernail.

This fingernail image classifier is composed of a cascade of elementary classifiers, also called stages. A given region of interest (ROI) is either rejected by a stage or it proceeds to the next stage. Initial stages are simpler than subsequent ones and focus in rejecting non-positive ROIs, i.e. areas where there is a low chance of detecting a fingernail. As such areas represent larger portions of the images, the overall detection speed is increased. When a stage approves a ROI, this region is passed on to the next stage. If the ROI is approved by every stage, then this region is classified as a fingernail image. Each stage is an Adaboost classifier which relies on haar-like features as input.

A large number of Haar-like features can be computed for every ROI which is significantly larger than the number of pixels of the given region. Thus feature selection is a requirement. Adaboost is employed for both the selection of such features, as well as for the training of the classifiers.

After the input image is converted to grayscale, as required by the object-detection algorithm, a ROI is defined

[1] The used dataset (see Section 4.1) provides already segmented fingernail images using the methodology presented in this Section.

by a scanning window. Robustness to scale variation is due to scaling of the detector, which can be applied at different scales with no extra cost. As the scanning window gazes through the input image, the cascade classifiers detect the fingernail multiple times. To achieve a final detection, as shown in Fig. 1, the detected ROIs are overlaid and merged into a single detection by selecting the average of the bounded regions.

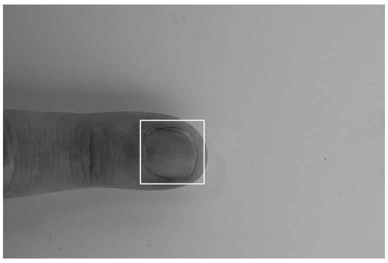


Fig. 1 Result from the object detector proposed by [27, 15] trained to detect fingernails. Detection outlined by a white bounding box.

Given the high resolution of the input images, the final ROI is then scaled to $300px \times 300px$. The original color image of the selected ROI is then sent to the signature extraction stage.

3.2 Signature Extraction

Every individual has a unique fingernail bed pattern, similar to a fingerprint, which influences the texture that constitutes the fingernail plate [11]. This texture is also influenced by the day-to-day interaction of the fingernail plate and the environment. Therefore, it is common to find white spots, marks and scratches over the fingernail plate. It is this rich texture region of the fingernail plate that is analyzed in order to create a texture based signature using a grid implementation of Local Binary Patterns [19]. This signature extraction process is described in Sec. 3.2.1.

The fingernail plate boundary and the unique white spots on it can be quite discriminative, and to exploit such characteristics two feature descriptors were employed. Section 3.2.2 explains how the SIFT[16] and BRISK [14] descriptors are used to create a second signature.

Notice that both the fingernail plate texture and its boundary shape have a transient nature since the fingernail plate changes completely over a period of about 6 months [28].

3.2.1 LBP Based Signature

Local Binary Patterns (LBP) was originally proposed as a reliable texture descriptor [19] and is known for its speed, robustness and capacity to differentiate between micro-patterns. The signature extraction uses a GRID extension of the LBP, based on the work of [1].

For every image pixel an LBP value can be computed by comparing the actual pixel value to its neighborhood. The pixel neighborhood is defined by a circle of radius R and a set of P equally spaced sample points. The LBP value for the central pixel is derived out of a binary comparison against the sample points. One bit is assigned to each sample point. The least significant bit value comes from the comparison against the top-left sampling point. It receives 1 when the central pixel is greater than or equal to the sampling point and 0 otherwise. This procedure is then applied to all other sampling points, in a clockwise manner. Therefore when 8 sampling points are used, there are a total of 256 possible LBP values. Fig. 2 illustrates the LBP calculation with a sample neighborhood of $(P,R) = (8,2)$.

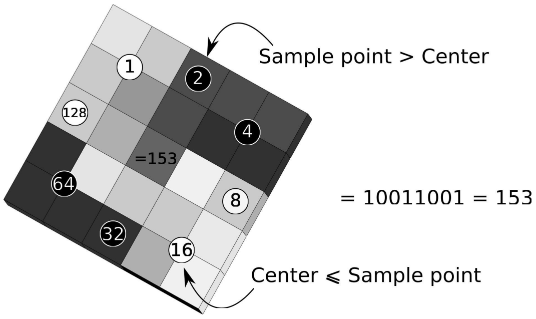


Fig. 2 LBP sample points are shown in red or green circles. The value of a sample point is bilinearly interpolated for sampling points that are not located on the center of a pixel. Dark circles denote sample points that have a lower value than the center pixel. Bright circles denote sample points which have a greater or equal value to the center pixel. Circle numbers indicate the index of the bit position in the LBP code.

LBP values are called uniform if the binary part is composed of one or two bit-wise transitions. Uniform LBP values account for the majority of encountered patterns on natural images [20, 1]. For example, in the case of eight sampling points, the patterns 00010000 and 11001111 are uniform since they have two bit-wise transitions. For eight sampling points, a total of 58 out of the 256 possible patterns are uniform.

To extract the LBP signature the input fingernail image is divided into 16 blocks using a 4×4 grid. Each image block is submitted multiple times to a Gaussian smoothing function, creating a Gaussian pyramid image set. This process generates a total of 48 smaller images from each input image. The final signature comes from the computation of uniform LBP values with a sample neighborhood of $(P,R) = (8,2)$ for each color channel. For each small image, 3 histograms of 59 bins are computed, 58 bins employed for the uniform patterns and the last bin for the non-uniform patterns. Thus, for each input image the signature is composed of 3×48 histograms of 59 bins. Although these histograms sum up to 8496 bins, the curse of dimensionality is avoided thanks to the matching technique.

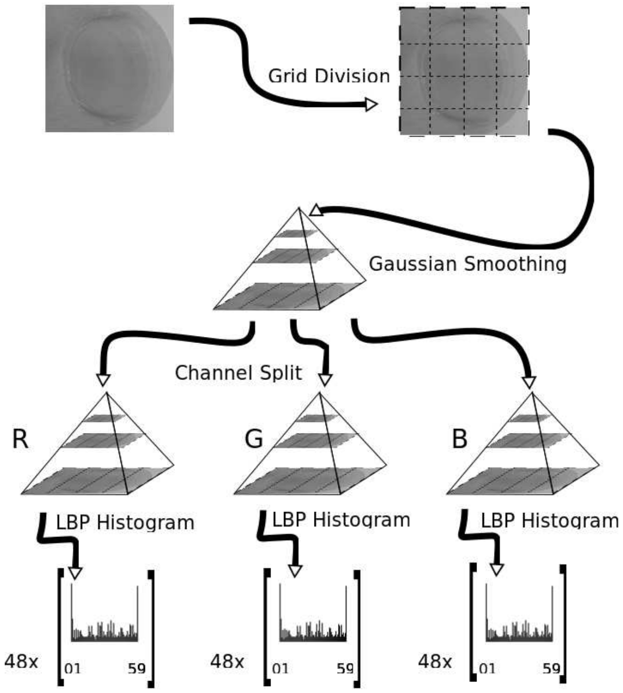


Fig. 3 LBP signature extraction. Each input image generates an LBP based signature comprised of 144 histograms, or 48 histograms per color channel.

3.2.2 Descriptor Based Signature

The first step of the descriptor based signature is to decompose the color image into three monochromatic images. Then keypoint detection is performed on each color channel. A keypoint detector that produces an output of low count is fundamental to any matching technique that relies on image descriptors. A low count of keypoints allows the solution to compare only significant points, speeding up the process and yielding a more robust and discriminative set of features. A multitude of different keypoint detectors have been proposed in computer vision while it is common for feature descriptors to propose their own keypoint detectors as for example in [14, 16].

Given that the image pre-processing presented in Sec. 3.1 already yields an image with a decent fingernail alignment and unique orientation, the use of keypoint detectors that are robust to such characteristics would be superfluous. A single fast and simple keypoint detector is shared across different descriptors. The selected keypoint detector is Good Features To Track (GFTT) [24] and represents a modification of the well known Harris corner detector [9]. Fig. 4 shows the result of this keypoint detector. The keypoints concentrate around the fingernail plate boundary as well as fingernail plate scratches and white spots, which are ideal to discriminate across subjects.

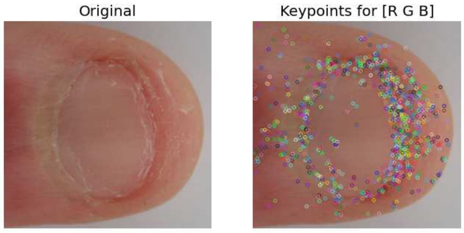


Fig. 4 Keypoints computed for the red, green and blue channels of a fingernail plate image. The keypoints concentrate around the fingernail plate border.

Having defined the keypoints, descriptors must next be computed on them. Two different keypoint descriptors are employed. The Scale Invariant Feature Transform - SIFT [16] was chosen for its success as a robust descriptor while the Binary Robust Invariant Scalable Keypoint - BRISK was selected for its efficiency [14]. Thus two biometric signatures are created for each input image, based on SIFT and BRISK respectively.

The total number of keypoints is reduced since both SIFT and BRISK prune down the keypoints by evaluating their stability (via contrast, distance to other keypoints, neighborhood noise, etc). Final monochromatic images have an average of 800 stable keypoints. Therefore, on average, a total of 2400 keypoints compose each of the two descriptor based signatures, one for SIFT and the other for BRISK.

3.3 Signature Matching

Signature matching defines the metrics used in order to compare different signatures. Ideally there is a small variation across signatures from the same subject, and large variation across signatures from different subjects. It is common to rely on machine learning techniques to discover patterns in signatures and then use such patters for signature matching. Previous work [2] even employed Bayesian classification and dimensionality reduction for signature matching.

Since the proposed approach intends to employ a direct methodology to transient biometrics, it avoids techniques that rely on training and cannot employ dimensionality reduction. Signature matching is thus done in stages; the three signature types are matched independently. This is also convenient for the exploration of different signatures fusion methodologies.

3.3.1 LBP Based Signature Matching

Matching LBP signatures fundamentally depends on obtaining a match score between two histograms, P and Q, with n bins. For this task, Cosine similarity as stated in Eq. 1, is employed:

$$\Phi(P,Q) = \frac{P \cdot Q}{\|P\|\|Q\|} = \frac{\sum_{b=1}^{n} P_b \times Q_b}{\sqrt{\sum_{b=1}^{n} (P_b)^2} \times \sqrt{\sum_{b=1}^{n} (Q_b)^2}} \tag{1}$$

A single LBP signature is composed of 144 histograms. Each histogram is derived from a small image region, and depends on the layer of a Gaussian pyramid and on the color channel. The final matching score is given as the mean score of matching corresponding histograms across different input images. Therefore, a histogram is only compared to its counterpart in another image, which deals with the curse of dimensionality while giving the signature the capability of describing texture and spatial relationships at the same time. If X_i represents the ith histogram of image X, then the LBP matching score L between images A and B is given by Eq. 2:

$$L(A,B) = \frac{1}{144} \sum_{i=1}^{144} \Phi(A_i, B_i) \tag{2}$$

3.3.2 Descriptor Based Signature Matching

A Fast Approximate Nearest Neighbor Search, proposed by [18], is first employed to evaluate the euclidean distance between keypoint combinations of the two images to be matched. The resulting matches are evaluated by a RANSAC [5] algorithm to remove bad matches and to detect a consensus set of plausible matches.

In order to create a unique signature matching score which can be combined with other scores, the RANSAC algorithm is executed multiple times. Each time it returns the percentage Υ of keypoints that are part of the consensus set. [2] The descriptor matching score D of images A and B is then computed as the average of the consensus keypoint percentage:

$$D(A,B) = \frac{1}{n} \sum_{i=1}^{n} |\Upsilon_i| \tag{3}$$

When matching is performed across multiple images using a distance measure, it is usual to normalize its output to yield a consistent matching score across images; however this normalization is only possible after all inter-image distances have been computed. Being an average percentage value, the proposed matching score of Eq. 3 does not require post-normalization and is thus suitable as a direct technique to compute the score between two images.

3.3.3 Signature Fusion

LBP describes the micro-texture that comprises the fingernail plates and their spatial relationships. In contrast to the descriptor based techniques LBP does not focus on discriminating white spots, marks or the border between fingernail plate and skin. A methodology for merging the different techniques is thus necessary. The idea of signature fusion is to generate a final matching score, which combines the properties of LBP, BRISK and SIFT.

The work of [21] shows different methodologies to similarity score fusion. Assuming that S_n is the nth similarity score, it proposes five fusion functions, as shown in (Eq. 4). S_A represents the arithmetic mean of the Manhattan (L_1) metric. S_E computes the root mean square of similarities and performs as a Euclidean (L_2) metric. S_G computes the product of similarities and works as geometric mean metric. S_{max} and S_{min} are simple rules to respectively select as final score the maximum or minimum similarity score:

$$S_A = \frac{1}{n} \sum_{f=1}^{n} S_f \tag{4}$$

$$S_E = \frac{1}{\sqrt{n}} \left(\sum_{f=1}^{n} {S_f}^2 \right)^{1/2} \tag{5}$$

$$S_G = \left(\prod_{f=1}^{n} S_f \right)^{1/n} \tag{6}$$

$$S_{max} = \max_{f=1}^{n} \left(S_f \right) \tag{7}$$

$$S_{min} = \min_{f=1}^{n} \left(S_f \right) \tag{8}$$

Since the proposed matching score functions of Eq. 2 and Eq. 3 have bounded outputs in the range $[0,1]$, all of the proposed methodologies of Eq. 4 could be employed as score fusion techniques. However most of them cannot handle the hidden issue of large variations in the skewing of the distribution scores.

In the case of the Cosine similarity used in the LBP matching technique (Eq. 2), the scores will have a propensity towards high values. While correct matches will present higher matching scores that wrong matches, given the derivation methodology and the fact that similarity is computed on a 59 dimension vector, wrong matches are also likely to give high matching scores.

The opposite is true in the case of descriptor matching where a natural bias towards low values occurs in the matching scores (Eq. 3). Given the low re-projection error accepted by the RANSAC algorithm when computing the

[2] Ransac is run multiple times to ensure change in the seed of the random number generator. Similar results are achieved if RANSAC is executed once for a longer time.

consensus set, the matching score technique will generally produce lower values; of course it is still true that correct matches are likely to yield higher results than wrong matches.

Given the aforementioned matching score value distributions, Eq. 4 and 5 would give a bigger weight to the LBP features, while Eq. 7 would ignore descriptor based features and Eq. 8 would ignore LBP based features. Such issues can be avoided with the normalization of the score distributions, but such a process is unacceptable in a direct approach.

The selected fusion technique is the geometric mean (Eq. 6). Thus the final matching score does not weigh differentially the LBP and descriptor based features. To explore different combinations of features a total of three signature fusions are computed. The first signature fusion F_{LS} relies on fusing LBP and SIFT features. This way the final signature will use the micro-texture capabilities of LBP combined with SIFT's capability of describing the fingernail border and fingernail plate white spots.

A second signature fusion F_{LB} is created using LBP and BRISK, in order to evaluate how the BRISK descriptor compares to the SIFT descriptor in this task. Finally a third signature F_{LBS} is defined, fusing LBP, BRISK and SIFT into a final matching score.

4 Experiments

This section describes the publicly available experimental dataset of fingernail plate images as well as the verification and identification performance of the proposed method on this dataset.

4.1 Publicly Available Dataset of Fingernail Plate Images

An extended version of an experimental dataset called Transient Biometrics Nails Dataset (TBND) was created[3]. TBND is composed of images of the right index finger. During acquisition the subject was instructed to lay their finger over a flat white surface and a simple point-and-shoot camera was used to acquire an image without the the use of a flash. No explicit instructions with respect to force applied were given and thus our results incorporate arbitrary force differences between users and capture sessions. Acquisition was thus done in a semi-controlled environment; apart from the white background and indirect lighting, the images present variation with respect to scale, focal plane and illumination. The dataset consists of three subsets, each one compromising the same 93 subjects, but varying on acquisition date.

The first subset **D01** consists of images acquired on the first acquisition day. The second subset **D02** is composed of images acquired one day later. The third subset **D30** was acquired one month after the first acquisition date. Given acquisition restrictions, the acquisitions of **D30** have up to two days' tolerance. This represents a massive expansion of the originally collected dataset [2], and will also be made available through NTNU Visual Computing lab's website [http://www.idi.ntnu.no/grupper/vis/TBND].

4.2 Verification Performance

To evaluate verification performance a simple direct classifier is used, which thresholds the matching score between two images to determine if they correspond. To asses the verification behavior across time and thus determine how transient the explored fingernail plate biometric really is, images from **D01** are matched against **D02** and **D30**. It is anticipated that the fingernail plate biometric information transforms as the fingernail grows. Therefore, higher verification rates should be expected for matches across a day interval (**D01**x**D02**) than for matches across a month interval (**D01**x**D30**). The difference in verification performance between these two cases will determine how transient the proposed biometric is.

Assuming that each subject represents a class, verification can be treated as a binary classification problem where the proposed solution verifies if a query image is from whom it is claimed to be. This implies that the classification output can yield four types of result: true positive, true negative, false negative and false positive. These outcomes are typically computed by comparing each image from the first dataset (called a query) against every image of the second dataset (called a target). A true positive is the case where the query is correctly classified as a match for the target while a true negative is the case where the query is correctly classified as a non-match for the target. A false negative is when the query is wrongly classified as a non-match for the target while a false positive is when the query is wrongly classified as a match.

Let TP, TN, FN and FP represent the cardinalities of the sets that represent the above four possible classification outcomes. By defining the False Positive Rate (FPR) as shown in Eq. 9 and the True Positive Rate (TPR) as shown in Eq. 10, it is possible to assess the verification performance with the Receiver Operator Characteristics (ROC) curve. This methodology evaluates how different thresholds on FPR (i.e. the risk of the system) impact on TPR (i.e. the convenience in the use of the system), by plotting FPR vs TPR:

$$FPR = \frac{FP}{FP+FN} \tag{9}$$

[3] Thanks to Cham Athwal of the School of Digital Media Technology, Birmingham City University

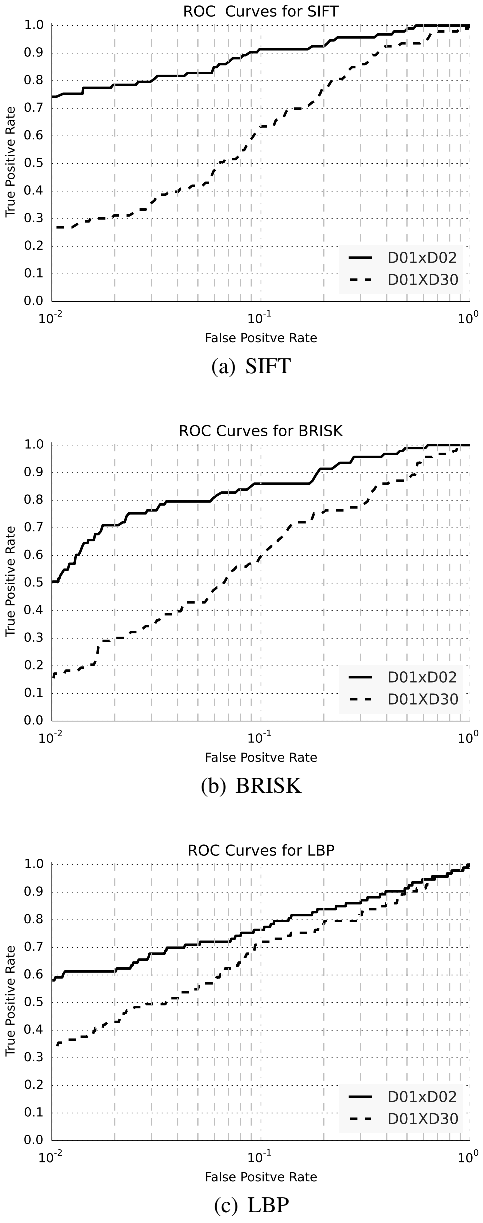
$$TPR = \frac{TP}{TP + FN} \tag{10}$$

Conventionally when a biometric methodology is evaluated with a ROC curve, the False Positive Rate ranges from 10^{-3} to 1. Given that our datasets compromise 93 subjects (being the first datasets of their kind), evaluating at $FPR = 10^{-3}$ would produce results of low statistical significance since the classification of a single subject would greatly alter the output values. This, in conjunction with the assumption that the proposed methodology is aimed at non-critical biometric applications, led us to compute the ROCs curves in the range 10^{-2} to 1.

We first compute the ROCs for each of the basic features used separately: SIFT, BRISK and LBP. We assess the verification rates for matches done with a day interval (**D01**x**D02**) against matches done with a month interval (**D01**x**D30**). The achieved results are shown in Fig. 5.

These ROC curves shows that all three features undergo an expected performance deterioration within the course of a month. This decay in performance shows that fingernail plate images are a *transient* biometric feature with a short lifetime.

We next present results on the fused signatures in Fig. 6. The ROC curve for F_{LS} shows verification performance for a signature based on the fusion of LBP and SIFT. In theory this signature fusion will have the capability to discriminate subjects' fingernails based on fingernail texture due to LBP, as well as due to fingernail border characteristics and fingernail white spots due to the SIFT descriptor. The computed ROCs are shown in Fig. 6 (a). The achieved results indicate that the proposed signature fusion technique of Eq. 6 on the fused signature F_{LS} outperforms the two best performing individual features shown in Fig 5 [(a) & (c)]. Therefore, the signature fusion technique was successful. This is further demonstrated in the fusion that results in the F_{LB} signature; in this case the LBP signature is combined with the efficient BRISK descriptor. The ROC curves for this fusion are shown in Fig. 6 (b). The final signature fusion F_{LBS} employs all three features, LBP, BRISK and SIFT. The idea is similar to before; use LBP to describe texture and SIFT/BRISK to describe fingernail borders and discriminating points. This time the fusion will also exploit any complementary information hidden in the combination of BRISK and SIFT. The results are shown in Fig. 6 (c).



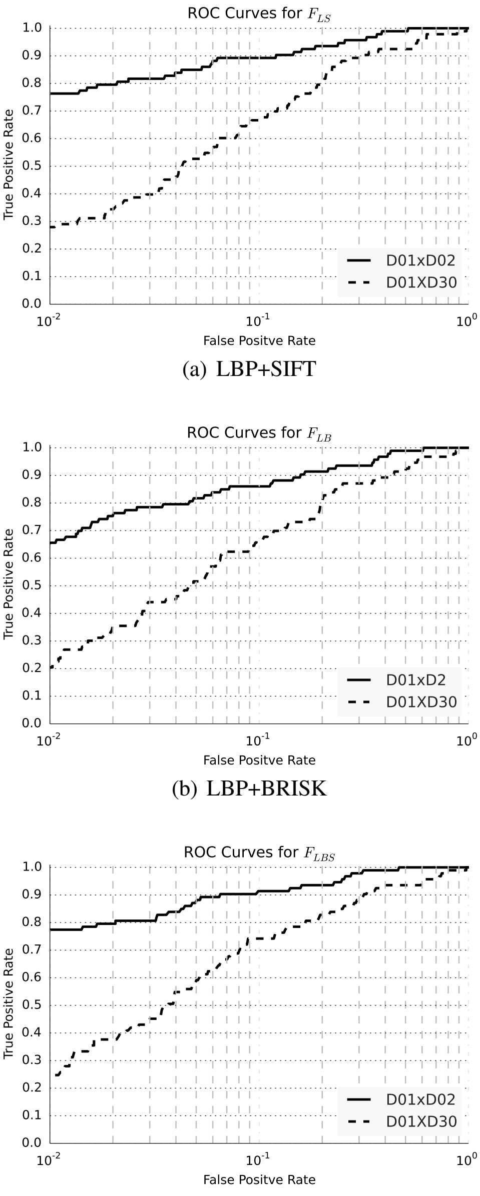
(a) SIFT

(b) BRISK

(c) LBP

Fig. 5 ROC curves for SIFT **(a)**, BRISK **(b)** and LBP **(c)**. Curves labeled **D01**x**D02** show the verification performance for matches done with a day interval, while curves labeled **D01**x**D30** show the verification performance across an interval of a month. The performance decay between the two intervals shows that fingernail plate images are a *transient* biometric feature.

Table 1 gives verification data for the proposed signatures. It shows the True Positive Rates achieved at an FPR of 0.01. The results indicate that the final signature fusion F_{LBS} for fingernail plate images is a transient biometric with a lifetime of less than 6 months. This is based on the assumption that the TPR of 0.247 after one month is already at an unacceptable level for practical recognition purposes (i.e. the biometric feature has been invalidated) and that the TPR value of 0.774 after one day is acceptable, at least for non-critical applications. We sextuple the invalidation period (from one to six months) to allow for possible future algorithmic improvements that could improve these figures and also taking into account physiological knowledge indicating that human fingernails totally outgrow within a period between 3 and 6 months [28].



(a) LBP+SIFT

(b) LBP+BRISK

(c) LBP+BRISK+SIFT

Fig. 6 ROC curves for combinations of [LBP+SIFT] F_{LS} **(a)**, [LBP+BRISK] F_{LB} **(b)** and [LBP+BRISK+SIFT] F_{LS} **(c)**. The performance improvement against the individual features of Fig. 5 indicates that a successful feature fusion methodology was found. Curves labeled **D01**x**D02** show the verification performance for matches done with a day interval, while curves labeled **D01**x**D30** show the performances for a month interval. The larger performance decay between the two intervals compared to single features, further supports the case that fingernail plate images are a *transient* biometric feature.

4.3 Identification Performance

Table 1 Verification data (TPR) at 0.01 FPR across datasets captured with a day interval (**D01**x**D02**) and a month interval (**D01**x**D30**).

True Positive Rate for different intervals

Signature	One day	One Month
SIFT	0.742	0.269
BRISK	0.505	0.151
LBP	0.581	0.333
F_{LS}	0.763	0.279
F_{LB}	0.656	0.204
F_{LBS}	0.774	0.247

The identification task is a multi class problem, where a query biometric signature is compared against a list of collected signatures (the target set) with the objective of finding if the query matches any of the collected signatures. To evaluate identification performance the cumulative match curve (*CMC*) will be used. *CMC* gauges the probability of a signature from a query dataset, in this case **D02** or **D30**, being correctly matched in the first *k* ranked subjects from the target set, in this case **D01**. The subjects of the target set are ranked using F_{LBS} (Fusion of LBP, BRISK and SIFT by Eq. 6). The abscissa in the CMC graph shows the rank while the ordinate shows the probability of a correct match up to that rank.

In the identification task, a simple threshold classifier plays no role on performance and the results show how reliable a computed matching score is for finding a correct match from an entire dataset. Figure 7 shows the CMC for F_{LBS} and gives another evaluation of the transient nature of the proposed biometric approach.

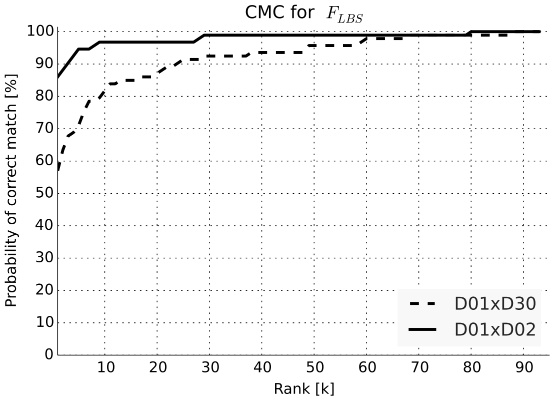


Fig. 7 Cumulative match curves for F_{LBS}. The scores are computed by comparing images from two query sets, respectively acquired within a day interval **D02** and within a month interval **D30**, against images of the target set **D01**. The decay in performance from **D02** to **D30** further supports the presumption that fingernail plate images constitute a transient biometric characteristic.

It is interesting to compare the identification results against our previous study which involved only 24 subjects [2]. Although the present method is significantly more robust, it achieves 86.022% Rank one identification on 93 subjects compared to 99.479% Rank one for the previous method on 24 subjects. [4]

4.4 Matching Score Distribution

In this section the results are analyzed using two charts showing matching score distributions. The score distribution charts give us an unbiased view of the behavior of a transient biometric across time that eliminates any bias introduced by classifier selection.

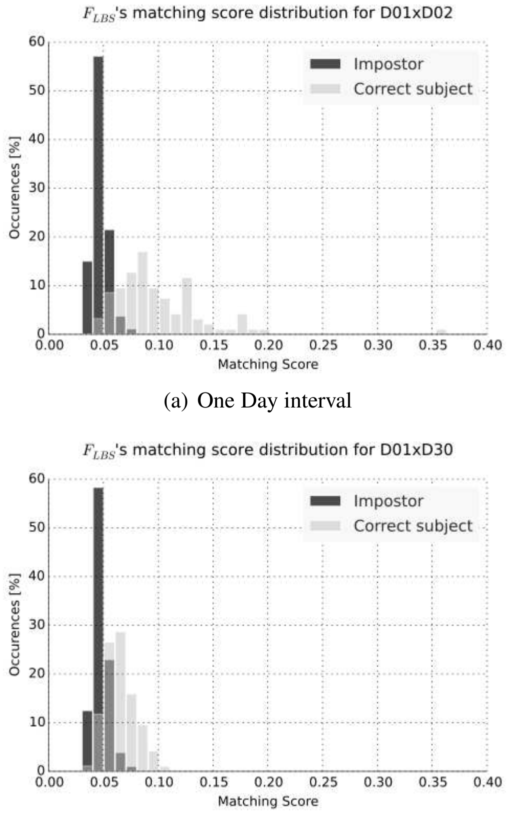
A histogram is used to approximate the probability density function (PDF) for matches done within a day interval (**D01**x**D02**) and within a month interval(**D01**x**D30**). In both scenarios the matching scores were divided into two different PDFs. The first PDF, called 'Impostor', accounts for the cases where the matching score is computed between a query subject and an impostor. The second PDF, named 'Correct Subject', accounts for the cases where the matching score is computed between a query subject and itself.

By separating the matching scores into these two categories, impostors and correct subjects, it is possible to observe the effect of time, and thus get an idea of the decay in recognition performance. These matching scores are computed using F_{LBS} (Fusion of LBP, BRISK and SIFT using Eq. 6). The abscissa represents matching score values while the ordinate represents frequency expressed as a percentage.

5 Conclusion

Transient biometrics are introduced as a plausible solution to the acceptability issue of biometric recognition systems. It presents a methodology which reduces the risk of misuse of biometric information; instead of relying on permanent biometric data it uses biometric data that changes within the short term and thus nullifies itself. Therefore, it is an engaging solution for collaborative individuals which are reluctant to volunteer hard biometric information (e.g. fingerprints, retina images) for non-critical biometric recognition tasks. Given the knowledge that the collected biometric data has an expiration date and becomes useless for recognition after this, individuals are more likely to volunteer such biometric data for day-to-day recognition tasks.

A transient biometric feature and methodology for verification and identification tasks was presented. This builds and completes previous work [2] and uses fingernail plate images. A new dataset is presented and will be made publicly available; it consists of a larger number of subjects, more realistic (and challenging) capture conditions as well as subjects with different skin tones.



(a) One Day interval

(b) One Month interval

Fig. 8 Probability Distribution Functions (PDF) for matches against impostors and correct subjects for a one day interval **(a)** and a month interval **(b)**. The change observed in the correct subject PDF from (a) to (b) further indicates that fingernail plate images are a plausible *transient* biometric. Notice that the score distribution for correct matches changes in such a way, that in case (b) it is hard to differentiate matching scores between correct subjects and impostors. This analysis eliminates any influence that may have been added from the choice of classifier. There is no post normalization after the matching score of Eq. 3; as this score comes from the percentage of RANSAC inliers, using a rather strict threshold, it is natural to have low matching scores.

The proposed methodology exploits both texture features and (descriptor based) information extracted from discriminant fingernail keypoints. No training or machine learning techniques are employed in the computation of the biometric signatures making this a direct approach.

Both verification and identification performance was high within a day interval but degrades considerably after a month, indicating that fingernail plate images are a valid *transient* biometric feature. Here we consider the performance of 80% to be high, given the novelty of the explored biometric trait. Nevertheless, some more traditional (non-transient) biometric technologies currently offer significantly higher recognition rates. It would therefore be important to explore improvements in the recognition rate, so that the proposed transient biometric could become commensurate with currently 'acceptable' recognition levels. One such improvement would

[4] Note that in the current study we compare day 1 to day 2 while in the previous study the comparison was across day 1 and day 8.

be the use multi-biometrics of the same class, by exploiting more than one fingernail per subject. In this case it is important to adopt a suitable fusion technique and to maintain the transient nature of the solution when extracting information from multiple fingernails, which could potentially be derived from a single image of the hand (that potentially also contains non-transient data). Another possibility for improving the recognition rate would be to use machine learning techniques instead of the current direct approach.

If one was willing to sacrifice the transient nature of the proposed approach, e.g. in order to create a multi-biometric solution using fingerprints and fingernails, the entire images of the fingers could be used. This would fit well with the works of [13], where finger knuckle images are used for biometric identification. A multi-biometric approach would also relate to the work of [12] where both fingernails and finger knuckles are used as biometrics.

The current size of the dataset does not allow for a realistic scalability study (e.g. it is not possible to compute a meaningful FPR of 10^{-3}). In further work, it would be interesting to expand the size of the dataset in order to allow for such a study.

Acknowledgements We would like to thank Cham Athwal of the School of Digital Media Technology, Birmingham City University, for co-acquiring the largest part of the fingernail datasets.

References

1. Ahonen, T., Hadid, A., Pietikäinen, M.: Face description with local binary patterns: application to face recognition. IEEE transactions on pattern analysis and machine intelligence **28**(12), 2037–41 (2006). DOI 10.1109/TPAMI.2006.244
2. Barbosa, I.B., Theoharis, T., Schellewald, C., Athwal, C.: Transient biometrics using finger nails. In: Biometrics: Theory, Applications and Systems (BTAS), 2013 IEEE Sixth International Conference on, pp. 1–6 (2013). DOI 10.1109/BTAS.2013.6712730
3. Bazzani, L., Cristani, M., Murino, V.: Symmetry-driven accumulation of local features for human characterization and re-identification. Comput. Vis. Image Underst. **117**(2), 130–144 (2013)
4. Chornenky, T.: United states patent us20030098774 (2001). URL https://www.google.no/patents/US20030098774
5. Fischler, M.A., Bolles, R.C.: Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography. Commun. ACM **24**(6), 381–395 (1981)
6. Fujishima, N., Hoshino, K.: Fingernail detection system using differences of the distribution of the nail-color pixels. JACIII **17**(5), 739–745 (2013)
7. Grieve, T., Lincoln, L., Sun, Y., Hollerbach, J., Mascaro, S.: 3d force prediction using fingernail imaging with automated calibration. In: Haptics Symposium, 2010 IEEE, pp. 113–120 (2010). DOI 10.1109/HAPTIC.2010.5444669
8. Hamdoun, O., Moutarde, F., Stanciulescu, B., Steux, B.: Person re-identification in multi-camera system by signature based on interest point descriptors collected on short video sequences. In: 2nd ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC-08). Stanford, Palo Alto, États-Unis (2008)
9. Harris, C., Stephens, M.: A combined corner and edge detector. In: Alvey vision conference, vol. 15, p. 50. Manchester, UK (1988)
10. Kale, K., Rode, Y., Kazi, M., Dabhade, S., Chavan, S.: Multimodal biometric system using fingernail and finger knuckle. In: Computational and Business Intelligence (ISCBI), 2013 International Symposium on, pp. 279–283 (2013). DOI 10.1109/ISCBI.2013.63
11. Krstic, R.: Human Microscopic Anatomy: An Atlas for Students of Medicine and Biology. Springer (1991)
12. Kumar, A., Garg, S., Hanmandlu, M.: Biometric authentication using finger nail plates. Expert Systems with Applications **41**(2), 373 – 386 (2014). DOI 10.1016/j.eswa.2013.07.057
13. Kumar, A., Ravikanth, C.: Personal authentication using finger knuckle surface. Information Forensics and Security, IEEE Transactions on **4**(1), 98–110 (2009). DOI 10.1109/TIFS.2008.2011089
14. Leutenegger, S., Chli, M., Siegwart, R.Y.: Brisk: Binary robust invariant scalable keypoints. Computer Vision, IEEE International Conference on **0**, 2548–2555 (2011). DOI http://doi.ieeecomputersociety.org/10.1109/ICCV.2011.6126542
15. Lienhart, R., Maydt, J.: An extended set of haar-like features for rapid object detection. In: Image Processing. 2002. Proceedings. 2002 International Conference on, vol. 1, pp. I–900–I–903 vol.1 (2002). DOI 10.1109/ICIP.2002.1038171
16. Lowe, D.: Distinctive image features from scale-invariant keypoints. International Journal of Computer Vision **60**(2), 91–110 (2004). DOI 10.1023/B:VISI.0000029664.99615.94
17. Mantelero, A.: The eu proposal for a general data protection regulation and the roots of the 'right to be forgotten'. Computer Law and Security Review **29**(3), 229 – 235 (2013)
18. Muja, M., Lowe, D.G.: Fast approximate nearest neighbors with automatic algorithm configuration. In: International Conference on Computer Vision Theory and Application VISSAPP'09), pp. 331–340. INSTICC Press (2009)
19. Ojala, T., Pietikäinen, M., Harwood, D.: A comparative study of texture measures with classification based on featured distributions. Pattern Recognition **29**(1), 51–59 (1996). DOI 10.1016/0031-3203(95)00067-4
20. Ojala, T., Pietikainen, M., Maenpaa, T.: Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Transactions on Pattern Analysis and Machine Intelligence **24**(7), 971–987 (2002)
21. Perakis, P., Theoharis, T., Kakadiaris, I.A.: Feature fusion for facial landmark detection. Pattern Recognition **47**(9), 2783 – 2793 (2014). DOI http://dx.doi.org/10.1016/j.patcog.2014.03.007
22. Ratha, N.K., Connell, J.H., Bolle, R.M.: Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal **40**(3), 614–634 (2001). DOI 10.1147/sj.403.0614
23. Rathgeb, C., Uhl, A.: A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security **2011**(1), 3 (2011). DOI 10.1186/1687-417X-2011-3
24. Shi, J., Tomasi, C.: Good features to track. In: Computer Vision and Pattern Recognition, 1994. Proceedings CVPR '94., 1994 IEEE Computer Society Conference on, pp. 593–600 (1994). DOI 10.1109/CVPR.1994.323794
25. Sun, Y., Hollerbach, J.M., Mascaro, S.A.: Measuring fingertip forces by imaging the fingernail. p. 20. IEEE Computer Society, Los Alamitos, CA, USA (2006). DOI http://doi.ieeecomputersociety.org/10.1109/VR.2006.97
26. Topping, A., Kuperschmidt, V., Gormley, A.: United States Patent US005751835A (1998)
27. Viola, P., Jones, M.: Rapid object detection using a boosted cascade of simple features. In: Computer Vision and Pattern Recognition, 2001. CVPR 2001. Proceedings of the 2001 IEEE Computer Society Conference on, vol. 1, pp. I–511–I–518 vol.1 (2001). DOI 10.1109/CVPR.2001.990517
28. Yaemsiri, S., Hou, N., Slining, M., He, K.: Growth rate of human fingernails and toenails in healthy american young adults. Journal of the European Academy of Dermatology and Venereology **24**(4), 420–423 (2010). DOI 10.1111/j.1468-3083.2009.03426.x