Comparison of Dynamic Biometric Security Characteristics against other Biometrics

Benoit Ducray*, Sheila Cobourne*, Keith Mayes* and Konstantinos Markantonakis*
*Smart Card Centre, Information Security Group (SCC-ISG)
Royal Holloway, University of London, Egham, Surrey, TW20 0EX
Email: {Benoit.Ducray.2013, Sheila.Cobourne.2008, Keith.Mayes, K.Markantonakis}@rhul.ac.uk

***Abstract*—Biometric data can be used as "something you are" in authentication systems, but if a biometric is compromised by a malicious entity, the genuine user can no longer use it because it cannot be easily changed. Dynamic biometrics may offer a practical alternative, as they capture both an inherence factor along with a changeable knowledge factor in a single step. This paper investigates dynamic biometrics and whether they offer useful security authentication properties compared to conventional biometrics. In particular the paper focuses on one type of dynamic biometry, authentication based on Gesture Recognition, and presents a proof of concept experiment. Security characteristics of examples from three classes of dynamic biometrics are compared to a selection of common physiological ("fixed") biometrics, leading to the conclusion that in addition to providing one-step, two factor authentication, dynamic biometry may provide privacy benefits in some circumstances.**

I. Introduction

Biometrics are often used in authentication solutions to provide "something you are". However, attackers may seek to compromise biometric authentication; possible attacks include compromise of stored biometric data, or copying/faking biometrics to fool data capture sensors. The compromise of a fixed user biometric is a fundamental disadvantage of this type of authentication, so the use of dynamic (changeable) biometrics may provide a practical alternative.

The availability of new types of sensors such as depth cameras, brainwave sensing headsets etc. has generated research interest into dynamic biometrics, as they can be used to capture inherent factors (physical/behavioral), simultaneously with a knowledge factor; for example Gesture Recognition (e.g.[1], [2], [3]). As the knowledge factor is easily changeable, a dynamic biometric can be changed yet still retain the advantages of biometric input. It will also provide a means for one step two factor authentication [4], where only one action is required to present two authenticating factors to a verifier. This paper investigates whether dynamic biometrics can provide security authentication and compares them to fixed biometrics. Several examples of dynamic biometry are presented, then one particular category, Gesture Recognition, is subjected to a more detailed analysis. As Gesture authentication is a relatively new research area, this paper also includes a proof of concept experiment, using a Leap Motion [5] depth camera as a sensor and feature extractor. This core example is then included in the subsequent security analysis. The security characteristics of several fixed/dynamic biometrics are determined based on criteria devised by Bonneau et al. [6]. The fixed biometrics included in the analysis are: *Fingerprints* as they are well proven and widely used biometric [7]; *Face Recognition* also widely used and accepted biometric [7]; *Retina* as it is seen as a highly reliable and accurate identifier [8].

This paper is structured as follows: Section II explains the background about dynamic biometrics and defines its different categories. Authentication based on Gesture Recognition, and a proof of concept experiment follow in Sections III and IV. Section V shows evaluation criteria and the security assessment of each biometric. The conclusion and future work appear in Section VI.

II. Background: Dynamic Biometrics

Our definition of dynamic biometrics is shown below (other papers have used slightly different definitions e.g. [9]):

A biometric is dynamic when physical/behavioural (inherent) biometric information is captured together with a knowledge factor from a user, such that it can be used as the basis of a one-step two factor authentication.

We introduce the following three dynamic biometric classes: text based, gesture based, and thought based.

- **Text based**: Keystroke, Speaker Recognition and touch screen patterns[1] on smart devices are good examples of this class [4], provided that the text /pattern used has been chosen by the user. Here, there is both biometric information (either the keystroke, sound emission or touch screen speed/ style/ pressure) and something the user has to know and can change easily, i.e. the text.
- **Gesture based**: This class can be divided into Gesture and Signature categories. *Gesture:* There are several ways to capture a gesture: for example, by using a depth camera (described later in this paper); or by using an electromyograph to capture electric impulses in the muscle [17]. The knowledge factor is the gesture itself. *Signature:* This refers to the capture of the direction, stroke, pressure, and shape of a signature, through touch sensitive technologies (such as PDAs or tablets). This

[1]Touchstroke dynamics is a behavioral biometric based on the style and rhythm that someone uses to interact with a touchscreen-equipped smartphone. This authentication method is analysed in [14] and [15], and enhanced in [16] e.g. by proposing how to handle typos.

Table I
COMPARISON OF GESTURE AUTHENTICATION. FP-BS: FALSE POSITIVE BRUTE FORCE, FP-AK: FALSE POSITIVE ATTACKER KNOWS

Papers	Sensor	Algorithm	TPR	FP-BF	FP-AK
Chahar et al. [10]	Leap Motion	Mix of Naive Bayes, Neural Network, Random Decision Forest	81%	1%	
Aslan et al. [11]	Leap Motion	DTW	88.29%		11.71%
Aumi et al. [2]	Short range depth sensor	DTW	96.6%	3.4%	5.3%
Ducray et al. [3]	Kinect™	DTW	93%	0%	1.7%
Wu et al. [12]	Kinect™	DTW	98.11%		1.89%
Tian et al. [13]	Kinect™	DTW	99%	1%	3%

only matches our definition of a dynamic biometric when the handwritten text can vary.

- **Thought based**: Authentication based on brainwave signals is now a realistic possibility. Several works have proposed the idea of a "passthought" and have shown than it is possible to authenticate a person via a specific thought [18], [19], [20]. Here the knowledge factor is the particular thought and the inherence factor is the uniqueness of the brain's wave emissions [18].

Dynamic biometrics have several advantages; they are easily changeable due to the knowledge factor, and they allow one-step two-factor authentication[2]. However, some categories of the dynamic biometrics family only use weak physical biometrics, such as gestures based on upper body geometry (shoulder length, arms length) which may be a disadvantage in some situations. Furthermore, any behavioural elements in the biometric may be observed/copied and knowledge factors may be forgotten.

The next two sections focus on one type of dynamic biometry, Gesture authentication, to provide a better understanding of its resistance to attacks by copying.

III. GESTURE AUTHENTICATION

Authentication based on Gesture Recognition requires the capture of the movement of a user. Different sensors can be used for this, but the amount of biometric data obtained varies by sensor type. For instance, gestures recorded using an accelerometer (e.g. in a mobile phone) do not capture the geometry of the hand performing the gesture. In this section, we focus on gestures recorded using depth cameras, as they provide more "two factor" aspects, i.e. the gesture plus some physical biometric data. Also, when discussing Gesture authentication we refer to a user that attempts to mimic the authentication gesture of another user, as an "attacker". Three different kinds of depth camera exist: Structured Light, Time of Flight and Stereo-Vision [22]. The user has to be in a position that will allow the sensor to see the user's movement. The gesture can be based on different parts of the body: depending on the system, we can use the full body [12], the upper body [3], or just the hand(s) [2]. The user is free to use any form of gesture, but some may prefer to use their signature [13], although the latter does not provide the required changeability. The Dynamic Time Warping (DTW) algorithm [23] is frequently used to do the comparison, but some systems may instead use a mix of Bayes, Neural Network or Random Decision Forest [10]. Depth cameras include the Kinect™, which is a depth camera with 20 3D skeleton tracking points. In [3] upper body parts recorded in the skeleton generated by the Kinect™were used for authentication based on Gesture Recognition: using 6 of the available 20 skeleton tracking points, gave a True Positive Rate (TPR) of 93%, with 0% False Positive Rate (FPR) if the attacker did not know the gesture and 1.7% of FPR once the attacker had seen the gesture. Other authors chose to use all 20 skeleton tracking points from the Kinect™ [12] which gave them a TPR of 98.11% for 1.89% of FPR. The Kinect™was used with the DTW algorithm for analysis and recognition of 3D signatures [13], giving 99% of TPR for 1% FPR when the signature is unknown to the attacker and 3% FPR when the attacker has full knowledge of the signature.

Furthermore, hand Gesture authentication, accuracy and attack resistance against shoulder surfing were explored in [2]. In this experiment, reference hand gestures were recorded using a depth camera, filmed, and shown to a group of attackers: they were then asked to copy the gestures [2]; here the FPR was 2.3%.

Table I compares several works on Gesture Recognition authentication. It shows that TPR varies between 88% to 99% depending on the method used. The table also shows results of brute force attacks against these systems (denoted FP-BS), where attackers attempted to guess a gesture: it can be seen that this type of attack is very unlikely to succeed. Additionally if the attacker knows the gesture (denoted FP-AK) the FPR results vary from 1.7% to 12%.

As Gesture authentication is a relatively new research area, the next section presents a proof of concept experiment using a Leap Motion device to capture hand gesture biometrics so that indicative results can inform the comparison of security criteria later in the paper.

IV. PRACTICAL EXPERIMENT

A. Methodology

We set up a Gesture Recognition experiment, which, by using the Leave One Out Cross Validation (LOOCV) comparison technique, produced 90,000 attacks and 10,000 attempts

[2]However the reverse is not true, all one-step two-factor authentications are not dynamic biometrics e.g. the Bionym wristband allows authentication via the cardiac rhythm it records plus ownership of the wristband itself [21].

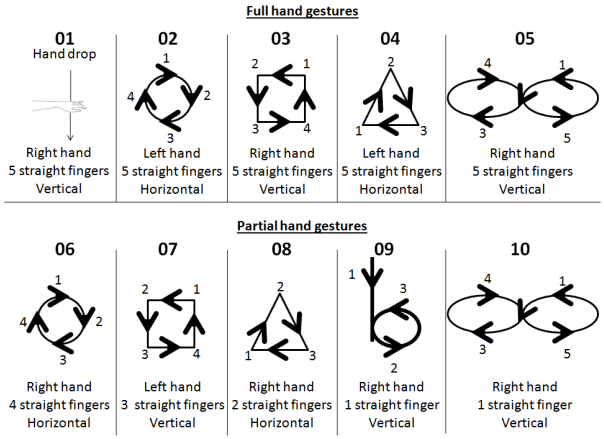

Figure 1. Model Gestures

at authentication by genuine users; section IV-C gives details of comparisons. We decided to use the Leap Motion sensor to monitor hand movements rather than the Kinect™ for full body gestures. This was a compromise between accuracy and practicality in common authentication scenarios. Gestures were captured by a Leap Motion device which tracks and records hand movements in Three Dimensions (For more technical information concerning the Leap Motion device please see [5]). We recorded the (x, y, z) positions of the palm centre and all five fingers tips and finger roots (i.e. eleven elements (E) for each frame). A group of 10 volunteers was asked to reproduce 10 pre-determined gestures ten times. It is important to note than this experiment was designed to simulate an attack, so all the participants knew all the gestures. We devised a set of 10 model gestures ranging from a simple hand drop, to more complex shapes e.g. drawing a symbol of infinity, and gave instructions about which hand to use and positioning of fingers (see Figure 1). Volunteers were given time to familiarise themselves with the equipment before the experiment started.

Five gestures were done with an open palm, as follows:

01: Let Right Hand (RH) drop vertically.

02: Make a circle on horizontal plane with Left Hand (LH).

03: Make a square on vertical plane with RH.

04: Make a triangle on horizontal plane with LH.

05: Draw a symbol of infinity on vertical plane with RH.

Another five gestures required variation of finger position, as follows:

06: Make a circle on horizontal plane with the RH and the index, middle, ring and little finger straight.

07: Make a square on vertical plane with LH and the index, middle, ring finger straight.

08: Make a triangle on horizontal plane with LH and the index, middle finger straight.

09: Draw a "b" on vertical plane with RH and the index finger straight.

10: Draw a symbol of infinity on vertical plane with RH and the index finger straight

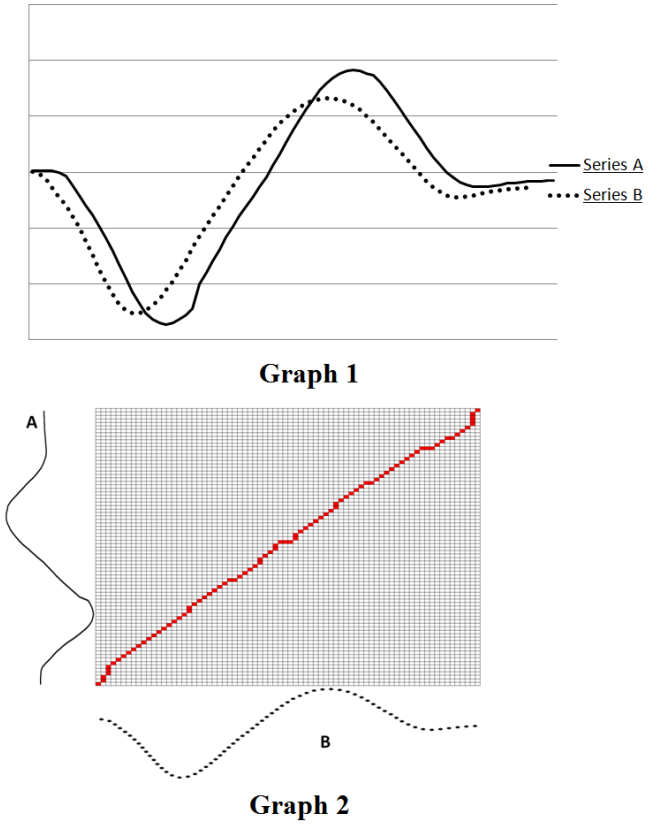

Figure 2. Graph 1 Two time series (A and B): Graph 2 The warping path between A and B obtained using the DTW algorithm

In order to accurately record when a gesture starts and stops, and to ensure that authentication attempts are synchronized with stored gesture templates, the software waits for an unmoving hand with five straight fingers before triggering or stopping the recording. More synchronisation is done automatically during the analysis with the DTW algorithm.

B. Dynamic Time Warping (DTW)

In order to compare two gestures, we chose to use the DTW algorithm, because it requires little training. DTW is reviewed in [23]. The following is a brief summary of DTW's properties.

DTW is used to find an optimal alignment between two time-bound sequences, independently of the variation of time or speed between both sequences. Originally, this algorithm was used in speech recognition [24] and its use has been enlarged to all domains in which data can be modeled in a linear representation e.g. computer animation, video, audio and graphics. The interested reader is referred to other works that have used this method [25]. The capability of finding an alignment for two sequences which are comparable but not aligned, is very important when comparing gesture patterns. In practice, the principle of DTW is to define a warping path with the minimal cost. This cost is given by the cost function (or distance function) which is the distance (or the error) between the two sequences, as shown in Figure 2. In other words, the

DTW algorithm gives us the alignment between the curve given by the reference model data, and the curve given by the user's captured data. which is given by:

$$\gamma\ (m,n) = d(m,n) + min(\gamma\ (m-1,n-1); \\ \gamma(m-1,n); \gamma(m,n-1)) \quad (1)$$

Where: $\gamma\ (m;n)$ is an $(M+1)\times(N+1)$ matrix; $\gamma\ (0;n)$ and $\gamma\ (m;0)$ are initialised with zero or a large number which represents infinity, depending on the application; $\gamma\ (0;0)$ with zero; $d(m;n)$ is the cost function.

C. The Analysis

We will use these definitions in the analysis:

Gesture set G will refer to the reference gesture and is composed of G=$(g_1, g_2, ..., g_{10})$ with $\#G$ representing here the number of elements in the set G i.e. 10.

User set U refers to the users and is composed of U=$(u_1, u_2, ..., u_{10})$ with $\#U$ representing here the number of elements in the set U 10.

Sample set S will refer to what a user produced for a specific gesture. It is composed of S=($s_{(g_i,u_j,1)}$, $s_{(g_i,u_j,2)}$, ..., $s_{(g_i,u_j,10)}$), where g_i is a specific element of G and u_j is a specific element of U, with $\#S_{(g_i,u_j)} = 10$.

At the end of the experiment, we used the LOOCV method, and obtained 100,000 comparisons, given by $\#G \times (\#S_{(g_i,u_j)} \times \#P)^2$.

Out of these 100,000 comparisons 10,000 were attempts at authentication from the genuine user ($\#G \times \#S^2_{(g_i,u_j)} \times \#U$) and 90,000 were attacks ($\#G \times \#S^2_{(g_i,u_j)} \times \#U \times (\#U-1)$), giving our FPR.

To assess TPR we focused our attention on a single user at a time; given a specific gesture, each user had 10 samples in the testing set for that gesture. The TPR is when the genuine owner of a gesture was authenticated correctly, for a fixed threshold θ. To assess FPR we look at many users at a time. Given a specific gesture, we isolated a sample from one user and compared all the other samples from all the other users and considered them as attackers. The FPR was when an attacker successfully authenticated for a fixed threshold θ. So TPR and FPR can be represented as:

$$TPR = \frac{N_U < \theta}{Total_U}, FPR = \frac{N_A < \theta}{Total_A} \quad (2)$$

Where N_U is the number of gestures from the genuine user below the threshold θ and N_A is the number of gestures from attackers below θ.

The next section discusses the experimental results.

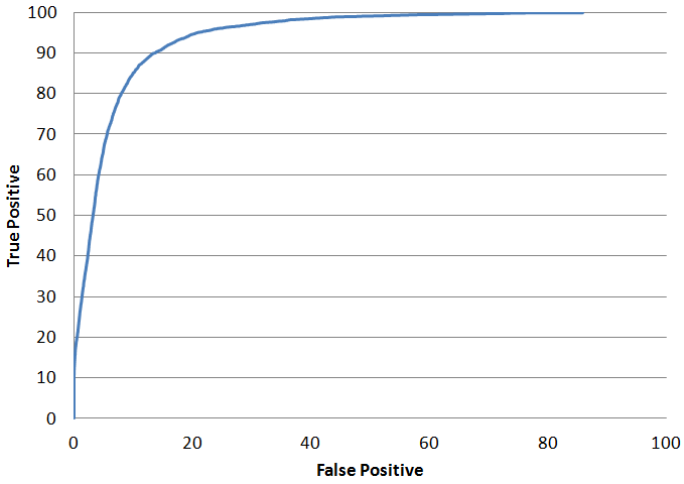

Figure 3. ROC curves of the Full Hand Gesture authentication.

D. Experimental Results

A Receiver Operating Characteristic (ROC) curve shows the performance of a biometric, by plotting TPR against FPR as the threshold is varied. The ROC curve we obtained is shown in Figure 3: It can be seen that for a TPR of 10 we have FPR of 0; that is due to the comparison of a user's gesture with itself which should always give us the minimal score i.e. 0. The asymptotic part takes a long time to reach the rate of 100, which means some of the samples are distant compared to other samples from the same user's gesture. This was possibly due to several users having difficulties using the Leap Motion for the first time. The users had not been given extensive training, as we chose DTW because we wished to minimise the training given and we were interested in how untrained users reacted to a relatively unfamiliar device. Figure 3 shows an EER of 11.88%. From the analysis of the ROC curve, we determined the optimal threshold, here we will continue to use the EER. With these respective thresholds, we find the global TPR= 88.12% and the FPR 11.88% for hand gestures. These results are not ideal, but referring to Table 1, it can be seen that they are closely comparable to prior art research using the Leap Motion sensor. More accurate results would have been expected from a Kinect™experiment.

Having explored Gesture authentication in detail, we now describe the evaluation criteria that will be used in assessing security characteristics of dynamic biometrics.

V. Evaluation Framework

The evaluation of dynamic biometrics will be based on security criteria outlined in the work of Bonneau et al. [6], along with additional security criteria that are particularly relevant to dynamic biometry. We have chosen to include in this comparison one example of each dynamic biometric class. We chose *Speaker Recognition* rather than keystroke recognition or touch screen because it is easily deployable over existing communications infrastructure (the telephone system) [29] and stable over various devices (Keystroke and

Table II
COMPARISON OF BIOMETRICS.

	Physical Biometrics			Dynamic Biometrics		
	Fingerprint Recognition	Face Recognition	Retina Recognition	Speaker Recognition	Passthought	Gesture Recognition
Resilient-to-Physical-Observation	High	Low	High	Low	High	Medium
Resilient-to-Targeted-Impersonation	Low [26]	Low [27]	High	Medium	Medium	Medium
Resilient-to-Unthrottled-Guessing	Low	Low	High	Low	Low	Low
Resilient-to-Theft	Medium [26]	High	High	High	High	High
Requiring-Explicit-Consent	Medium	Low [27]	High [28]	Medium	High	High
Unlinkable	Low	Low	Low	Medium	Medium	Medium [3]
One Step Two Factor	No	No	No	Yes	Yes	Yes
Changeable	No	No	No	Yes	Yes	Yes
False Positive Rate	0.2% [28]	0.1% [28]	0.0000001% [8]	2%-5% [28]	2% [19]	0%-3.4%
True Positive Rate	99.8% [28]	90% [28]	99.9999999% [8]	80-90% [28]	98% [19]	81%-99%

touch screen are not)[3]. We selected *Gesture Recognition* and *Passthought* as they are both relatively new research areas. Note that we expand our definition of 'attacker' here to refer to an individual who attempts to obtain biometrics information by any method (not just copying) in order to successfully authenticate instead of the genuine user.

A. Evaluation Criteria

- Resilient-to-Physical-Observation: if an attacker is present when the genuine user is authenticating, they should not be able to capture any useful information. We rate a biometric as High if no information can be captured, Medium if some information could be captured and Low if almost all the information can be captured.
- Resilient-to-Targeted-Impersonation: if an attacker has investigated background information about the genuine user, they should not be able to use this successfully in authentication. We rate a biometric as High if no information can be captured, Medium if some information could be captured and Low if almost all the information can be captured.
- Resilient-to-Unthrottled-Guessing: an attacker should not be authenticated if they are able to have an unlimited number of tries. We rate a biometric as High if the attacker would need more than 2^{20} attempts, Medium if they need more than 2^{10} attempts and Low they need less than 2^{10} attempts.
- Resilient-to-Theft: If the system uses a physical object for authentication (i.e. reader, keyboard, etc.), this object should not give any information to an attacker if they get access to it. We rate a biometric as High if it does not need any physical object or than the object does not keep any information, Medium if the biometric might require an object that an attacker could get information from, and Low if the biometric always needs an object that an attacker could potentially get information from.
- Requiring-Explicit-Consent: Here we rate a biometric High if it needs the full consent of the user to start an authentication process, Medium if the biometric can be used to authenticate without the consent of the user only by using subterfuge, and Low if the biometric can be used to authenticate without the consent of the user.
- Unlinkable: For privacy, it should not be possible for colluding verifiers to determine if the same user is authenticating to both their systems. We rate a biometric as High if there is no linkability, Medium if it is linkable in some circumstances and Low if it is totally linkable.
- One Step Two Factor: Does the biometric combine two factors in one step? (yes or no)
- Changeable: Can the biometric be changed and reused for authentication in the case of compromise? (yes or no)
- FPR/TPR: FPR - an attacker successfully authenticates; TPR - a genuine user successfully authenticates.

B. Evaluation of Biometrics

The following analysis has been summarised in Table II.

- Resilient-to-Physical-Observation: We rated Fingerprint and Retina as High, along with Passthought: for Passthought an observer cannot capture what the user is thinking as there is no device yet that can capture brain waves at a distance. Gesture Recognition is rated medium, as although an observer can see/observe/record a gesture, they cannot use a recording directly to get authenticated. Face and Speaker Recognition are rated Low.
- Resilient-to-Targeted-Impersonation: Retina is rated High as it is difficult for an attacker to find out the blood vessel pattern. Speaker Recognition, Passthought and Gesture are Medium because the attacker may be able to discover information relevant to the specific thought and gesture but that would not be enough to perform an attack. Fingerprint and Face Recognition are rated Low as it would be easy for an attacker to find a picture [27] and a latent Fingerprint [26] to impersonate a user.
- Resilient-to-Unthrottled-Guessing: Here we will use FPR data with the formula given in [30] to calculate the keyspace which is $1/FPR = keyspace$. We base our ratings on the following calculated keyspaces: Fingerprint $2^{8.97}$, Face Recognition $2^{6.7}$, Retina $2^{29.89}$, Speaker

[3]However, touch screen biometrics on smart phone devices exhibit many of the same characteristics as speaker recognition

Recognition goes from $2^{4.35}$ to $2^{5.65}$, Passthought $2^{5.65}$. Gesture[4] ranges from $2^{4.9}$ to $2^{6.65}$.

- Resilient-to-Theft: All the biometrics analysed here do not required any contact with an object or leave any information on it, with the exception of Fingerprint. This leaves some latent prints on the reader, which provides a way to attack it [26][5].
- Requiring-Explicit-Consent: Retina scanning requires the user to look into an eye-piece and focus on a specific spot [28]: we rate this High. Similarly, a High rating was given for Passthought and Gesture as it would be difficult for a attacker to authenticate without user consent. Fingerprint is rated Medium as an attacker could trick a genuine user into touching a reader to initiate an authentication. Speaker Recognition is rated Medium because an attacker could use a hidden microphone to authenticate as a genuine user without their consent. Face Recognition is rated Low as an attacker could authenticate using an easily obtained photo of the user taken without their consent [27].
- Unlinkable: By definition, biometrics are related to a particular user, so all 'fixed' biometrics are rated Low. However, some dynamic biometrics use weak inherent biometric factors: for example Gesture Recognition may involve some body measurements such as arm length or shoulder width [3] which are not sufficient for a unique identification of a user. This make them better for privacy. Also the inclusion of a knowledge factor in dynamic biometrics means that the same inherent factor to be used with different secrets at different verifiers. Consequently, all dynamic biometrics are rated Medium.
- One Step Two Factors: None of the physical biometrics can be used in a One Step Two Factor authentication, but by definition any dynamic biometric can.
- Changeable: Physical biometrics cannot be changed at the wish of the user. With dynamic biometrics the knowledge factor can be easily changed.
- FPR and TPR: For Fingerprint, Face, Speaker Recogniton we based this section on [28]. For Retina, the error rate is 0.0000001% [8] so we can assume than the FPR is the same and the TPR is 99.9999999%. Passthought [19] found a FPR of 2% and a TPR of 98%. For Gesture Recognition we used the range of values from Table I.

C. Security of Dynamic vs 'Fixed' Biometrics

The data shown in Table II highlights some important issues. There have always been concerns about privacy and linkability of biometrics, and that once compromised, a biometric credential becomes unusable by the genuine user. These are addressed by dynamic biometrics, and it can be seen from the table that this new family of biometrics outperforms some traditional biometrics in a number of respects. For example, our rating of Face Recognition is equal to or lower than all the dynamic biometrics assessed, for all security criteria identified. Also, Passthought could rival Retina Recognition in terms of security, being ranked lower in only two criteria, *resilient-to-targeted-impersonation* and *resilient-to-unthrottled-guessing*. All the dynamic biometry categories were ranked Medium in the *resilient-to-targeted-impersonation* criterion, better than Fingerprint and Face Recognition. Naturally, not all biometrics are suitable for all authentication situations: conventional biometric techniques are typically used for applications with higher security requirements than dynamic biometrics. For example, as Gesture authentication is vulnerable to 'shoulder-surfing' (copying) attacks it would not be suitable for use in busy public environments but would be a plausible option for video games. Passthought currently requires fairly intrusive use of hardware so may not be a good option for day-to-day use. Dynamic biometrics are by definition capable of providing One-step Two Factor Authentication, and the use of a secret knowledge factor brings some privacy benefits in comparison to 'fixed' biometrics: additionally the use of weak inherent biometric data in gestures will also improve unlinkability.

[4]An FPR of 0% was found in [3], i.e. a very high keyspace, but we feel that this value needs to be confirmed by further experiments.

[5]This is also a disadvantage in touch screen biometrics.

VI. Conclusion

A major security issue with 'fixed' biometrics occurs if biometric data is compromised so the use of a changeable, dynamic biometric may provide a practical alternative. This paper investigated how the security of dynamic biometrics compares to conventional biometrics. Several examples of dynamic biometry were presented, and one category, Gesture Recognition was analysed in more detail. As Gesture authentication is a relatively new research area, a proof of concept experiment was described, which used a Leap Motion [5] depth camera as a sensor and feature extractor. An attacker mimicking a known gesture had 11.88% likelihood of a successful attack, whilst a genuine user had a 88.12% chance to be correctly authenticated. These initial results were a little disappointing, however they were comparable to prior-art research using the Leap Motion sensor. Evaluation criteria devised by Bonneau et al. [6] were then used as a basis to assess the security of several fixed/dynamic biometrics. The inclusion of a knowledge factor in a dynamic biometric brings some privacy benefits in comparison to 'fixed' biometrics, in addition to making the biometric changeable. Unlinkability improves a) because the same physical characteristic can be used at different verifiers with different secret knowledge, and b) by using weak inherent biometric data in some dynamic biometrics (e.g. in Gesture Recognition). In future work, we intend to extend the proof of concept experiment using a larger sample of volunteers, and implement a secure system using authentication based on Gesture Recognition.

References

[1] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan, "UWave: Accelerometer-based personalized gesture recognition and its applications," *Pervasive and Mobile Computing*, vol. 5, no. 6, pp. 657–675, 2009.

[2] M. T. I. Aumi and S. Kratz, "Airauth: evaluating in-air hand gestures for authentication," in *Proceedings of the 16th international conference on Human-computer interaction with mobile devices & services*. ACM, 2014, pp. 309–318.

[3] B. Ducray, S. Cobourne, K. Mayes, and K. Markantonakis, "Authentication based on a changeable biometric using gesture recognition with the Kinect," in *Biometrics (ICB), 2015 International Conference on*. IEEE, 2015, pp. 38–45.

[4] J. Chuang, "One-step two-factor authentication with wearable biosensors."

[5] "Leap Motion," https://developer.leapmotion.com/getting-started/javascript/developer-guide, 2016, [Online; accessed 25 February 2016].

[6] J. Bonneau, C. Herley, P. C. Van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012, pp. 553–567.

[7] R. Heyer, "Biometrics technology review 2008." 2008.

[8] P. Cofta, S. Furnell, and H. Lacohee, *Understanding Public Perceptions: Trust and engagement in ICT-mediated services*. Intl. Engineering Consortiu, 2008.

[9] S. J. Simske, "Dynamic biometrics: The case for a real-time solution to the problem of access control, privacy and security," in *2009 First IEEE International Conference on Biometrics, Identity and Security (BIdS)*. IEEE, 2009, pp. 1–10.

[10] A. Chahar, S. Yadav, I. Nigam, R. Singh, and M. Vatsa, "A leap password based verification system," in *Biometrics Theory, Applications and Systems (BTAS), 2015 IEEE 7th International Conference on*. IEEE, 2015, pp. 1–6.

[11] I. Aslan, A. Uhl, A. Meschtscherjakov, and M. Tscheligi, "Mid-air authentication gestures: an exploration of authentication based on palm and finger motions," in *Proceedings of the 16th International Conference on Multimodal Interaction*. ACM, 2014, pp. 311–318.

[12] J. Wu, J. Konrad, and P. Ishwar, "Dynamic Time Warping for gesture-based user identification and authentication with Kinect," in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*. IEEE, 2013, pp. 2371–2375.

[13] J. Tian, C. Qu, W. Xu, and S. Wang, "Kinwrite: Handwriting-based authentication using Kinect." in *NDSS*, 2013.

[14] D. Damopoulos, G. Kambourakis, and S. Gritzalis, "From keyloggers to touchloggers: Take the rough with the smooth," *Computers & security*, vol. 32, pp. 102–114, 2013.

[15] G. Kambourakis, D. Damopoulos, D. Papamartzivanos, and E. Pavlidakis, "Introducing touchstroke: keystroke-based authentication system for smartphones," *Security and Communication Networks*, 2014.

[16] F. Alshanketi, I. Traore, and A. A. Ahmed, "Improving performance and usability in mobile keystroke dynamic biometric authentication," in *Security and Privacy Workshops (SPW), 2016 IEEE*. IEEE, 2016, pp. 66–73.

[17] M. S. Holi, "Electromyography analysis for person identification," *International Journal of Biometrics and Bioinformatics (IJBB)*, vol. 5, no. 3, p. 172, 2011.

[18] J. Thorpe, P. C. van Oorschot, and A. Somayaji, "Pass-thoughts: authenticating with our minds," in *Proceedings of the 2005 workshop on New security paradigms*. ACM, 2005, pp. 45–56.

[19] B. Johnson, T. Maillart, and J. Chuang, "My thoughts are not your thoughts," in *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*. ACM, 2014, pp. 1329–1338.

[20] J. Chuang, H. Nguyen, C. Wang, and B. Johnson, "I think, therefore I am: Usability and security of authentication using brainwaves," in *International Conference on Financial Cryptography and Data Security*. Springer, 2013, pp. 1–16.

[21] "Bionym nymi," http://www.bionym.com/, 2016, [Online; accessed 23 May 2016].

[22] F. Weichert, D. Bachmann, B. Rudak, and D. Fisseler, "Analysis of the accuracy and robustness of the Leap Motion controller," *Sensors*, vol. 13, no. 5, pp. 6380–6393, 2013.

[23] E. Keogh and C. A. Ratanamahatana, "Exact indexing of Dynamic Time Warping," *Knowledge and information systems*, vol. 7, no. 3, pp. 358–386, 2005.

[24] V. Velichko and N. Zagoruyko, "Automatic recognition of 200 words," *International Journal of Man-Machine Studies*, vol. 2, no. 3, pp. 223–234, 1970.

[25] D. Gavrila and L. Davis, "Towards 3-d model-based tracking and recognition of human movement: a multi-view approach," in *International workshop on automatic face-and gesture-recognition*. Citeseer, 1995, pp. 272–277.

[26] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys (CSUR)*, vol. 47, no. 2, p. 28, 2015.

[27] R. Tronci, D. Muntoni, G. Fadda, M. Pili, N. Sirena, G. Murgia, M. Ristori, S. Ricerche, and F. Roli, "Fusion of multiple clues for photo-attack detection in face recognition systems," in *Biometrics (IJCB), 2011 International Joint Conference on*. IEEE, 2011, pp. 1–6.

[28] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4–20, 2004.

[29] T. O. Majekodunmi and F. E. Idachaba, "A review of the fingerprint, speaker recognition, face recognition and iris recognition based biometric identification technologies," 2011.

[30] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.