Robustness Assessment of Biometric Authenticators

Romain Dagnas
Cybersecurity and Networks
IRT SystemX
Palaiseau, France
0000-0002-2994-8650

Anis Bkakria
Cybersecurity and Networks
IRT SystemX
Palaiseau, France
0000-0002-9758-4617

Reda Yaich
Cybersecurity and Networks
IRT SystemX
Palaiseau, France
0000-0001-7294-5909

***Abstract*—Biometric authenticators aim to provide a safe, secure, and accurate authentication process in restricted areas. Despite their advantages, biometric authenticators are vulnerable to cyber-attacks, such as spoofing attacks. Spoofing attacks enable malicious actors to masquerade as someone else to gain illegitimate access or privilege. To proceed, the attacker forges fake biometric data or duplicates existing ones. In such a context, the evaluation of the robustness of biometric authenticators is paramount to assessing their resilience potential and derive deployment strategies. Through this work, we propose a generic assessment method, based on a metric which quantifies the robustness of biometrics against cyber-attacks. Our methodology can be adapted to different families of cyber-attacks targeting biometric authentication techniques. We demonstrate our approach by considering spoofing-attacks. To achieve this objective, we present an extended state-of-the-art of biometrics (physiological and behavioural), including emerging biometric technologies. We also provide an overview of spoofing-attacks for each identified biometric mechanism in the literature. Based on this knowledge, we quantify and we combine the characteristics of such attacks into a quantitative robustness metric which can be applied to both a single and a combination of authenticators.**

***Index Terms*—biometrics, robustness assessment, robustness metric, authenticators combination**

I. Introduction

Nowadays, there is a real need to protect restricted areas and sensitive data with reliable and secure authentication mechanisms. Biometric authenticators are considered a safe way to guarantee the accuracy of an authentication process. This is mainly due to the common belief that biometric data are difficult to clone and/or steal, which is why such mechanisms are widely used. Despite their accuracy and advantages, biometric mechanisms could be vulnerable to adversarial attacks. In this paper, We focus on spoofing attacks targetting to biometric techniques. During spoofing attacks, an adversary uses fake, cloned, duplicated, or stolen biometric data belonging to an authorized person when interacting with a biometric authenticator. The objective of spoofing-adversary consists in impersonating the authorized user and being identified as the latter by the targeted authentication system. The literature has proven that without appropriate countermeasures, the security of biometric mechanisms can be bypassed by spoofing attacks [1]. Some vendor solutions incorporated into biometric technologies have been proposed, and these countermeasures can detect cloned biometric data that an adversary may attempt to use to fool biometrics. This includes, in the case of fingerprint authentication, the use of a pulse detector [1] to avoid using pictures or gelatin fingers by spoofing adversaries. However, depending on the attack, and depending on the biometric mechanism itself, spoofing attacks can not all be avoided. Many recent works highlight the vulnerabilities and the weaknesses of biometrics against spoofing attacks. The research community is continuously investigating to find innovative biometric mechanisms for ensuring safe, secure and accurate authentication processes. The actual surveys on biometrics do not include the emerging, and the less-known technologies such as Stylometry or Body Odor biometrics. There exists a large panel of biometrics, and each of these mechanisms can be subjected to attacks. Moreover, there is actually no works presenting the attacks applied to the existing biometric mechanisms. Actually, a generic robustness assessment method is missing in the literature. It is crucial to be able to quantify the robustness of single, or combinations of biometrics for choosing the best mechanisms combinations. In our opinion, a robustness assessment metric must take into consideration biometric mechanisms properties, as well as the properties of the attacks the biometrics are vulnerable to. This is why it is important to have an overview of the existing biometrics, and the known attacks they are vulnerable to. The approaches in the literature presenting robustness assessments of biometrics do not take this aspect into consideration. They only consider assessment methods based on the accuracy of biometric mechanisms. Furthermore, the proposed use-cases are based on metrics applied to specific authenticators for specific attacks. These approaches are not generic, and are not applicable to every biometrics. Our contributions are fourfold : (1) We extend the existing works presenting biometric mechanisms by incorporating emergent and new biometric technologies ; (2) We present the existing spoofing attacks applied to biometrics ; (3) We present a metric for the robustness assessment of biometric mechanisms ; (4) We investigate how to generalize our proposed metric to assess the robustness of existing combinations of biometrics against spoofing attacks. This work is organized as follows : We present a background on existing biometric authenticators (including emergent technologies), existing spoofing attack related to each biometric and related work in Section II ; Section III presents our robustness assessment method, which is based on a quantitative metric applied to single and combinations of authenticators regarding one or several

TABLE I
EXISTING BIOMETRIC AUTHENTICATORS.

Biometrics	Refs.	Family	
		Physiological	*Behavioral*
Body Odor	[3], [4]	✓	
Breath Recognition	[5]		✓
DNA (Deoxyribonucleic Acid)	[6]	✓	
Ear - Canal Echo	[7], [8]	✓	
Ear - Shape	[9]	✓	
ECG (Electrocardiogram)	[2]	✓	
Eye - Iris	[10]	✓	
Eye - Retina	[11]	✓	
Eye - Sclera Vein	[12]	✓	
Face	[2]	✓	
Finger - Contactless	[13]	✓	
Finger - Geometry	[14]	✓	
Finger - Print	[15]	✓	
Finger - Vein	[16]	✓	
Handwriting	[17]		✓
Hand - Geometry	[18]	✓	
Keystroke	[19]		✓
Lips Motion	[20]		✓
Palm - Print	[2]	✓	
Palm Vein	[21]	✓	
Skin Reflectivity	[22]	✓	
Stylometry	[23]		✓
Teeth Shape	[24], [25]	✓	
Thermography	[26]	✓	
Vocal Resonance	[27]		✓
Voice	[2]		✓
Walk	[28]		✓

attacks ; Section IV provides a discussion about the proposed contributions ; finally, Section V provides a general conclusion and future works.

II. BACKGROUND

A. Existing Biometric Authenticators

Nowadays, fingerprints, which has been the very first biometric technology to be used for authentication processes for centuries, are not anymore the only technology used for authentication purposes. Researchers are still investigating biometrics that guarantee accurate authentication processes, and difficult to duplicate or steal. Rui and Yan [2] have proposed a survey of biometrics that we propose to extend with emerging technologies such as the Body Odor, or the Skin Reflectivity mechanisms. There exist two families of biometrics presented in Table I with their relevant mechanisms. Physiological technologies refer to "biological" data, such as ECG signals, fingerprints, etc. Behavioral mechanisms include data such as keystroke dynamics, the way a person walks, etc. Through the next section, we present the identified spoofing attacks applied to the biometrics presented in Table I.

B. Existing Spoofing Attacks Against Biometrics

Biometric authenticators, as many connected components, are vulnerable to cyber-attacks. In our opinion, a robustness assessment of biometric technologies starts by identifying from which threat these biometrics need to be protected. The robustness assessment approach we build can be adapted to take into consideration a large panel of cyber-attacks. We choose the family of the spoofing attacks to demonstrate our approach because this family of attacks does not imply to exploit a vulnerability related to the system the authenticator is implemented in. Spoofing attacks only occur at the level of the sensor itself, and our approach puts the emphasis on how a single or a combination of biometric authentication solutions will withstand existing spoofing attacks. The Table II presents, for each identified biometric mechanism, the spoofing attacks in the literature they are subjected to. As shown in Table II, single biometrics as well as combinations of biometrics, are vulnerable to several attacks. A robustness assessment metric is therefore necessary, whether it is for the assessment of single biometrics, or for a combination assessment.

Remark 1: Some of the presented biometric mechanisms in the Table II are considered to not be subjected to spoofing attacks. This is the case for retina and Sclera Vein biometrics. Indeed, a Retina biometric uses the internal structure of a person's eye. Retinal images acquisition is done by the bias of ophthalmologic cameras, and such a biometric is very difficult to spoof [52]. A Sclera recognition system uses the vein schemes of an eye. This biometric mechanism, such as the Retina one, is internally located, and thus, considered as hard to spoof [53]. Actually, we have not identified spoofing attacks applied to Retina and Sclera Vein biometrics.

C. Related Work

1) Biometric Authenticators: Several works present a survey of biometric technologies, such as the work by Rui and Yan [2], but new technologies both on the physiological and behavioral aspects are not taken into consideration. Buciu and Gacsadi [54] also proposed a survey based on physiological biometrics, which are biometrics based on the capture of biological biometric data. However, they do not take into consideration the emerging technologies as well as the behavioral mechanisms. In Section II-A, dedicated to the existing biometric technologies, we present all the biometrics found in the literature, considering well-known technologies such as fingerprint, face authentication, etc, and also the emerging, or less-known technologies.

2) Spoofing Attacks against Biometrics: To the best of our knowledge, a work presenting spoofing attacks applied to the existing biometric technologies, has not been introduced yet. Several works present biometric mechanisms regarding spoofing attacks [1], [21], [44], [45]. However, the authors use some of the existing technologies, and an exhaustive view of the existing spoofing attacks is missing. In Section II-B, we present a mapping between the existing biometrics and the spoofing attacks they are vulnerable to.

3) Biometric authentication architecture and attack surface: The work by Stephen and Reddy [55] presents a general architecture of a biometric authentication system. Such an architecture is presented in the Fig 1.

Multiple attack points can be highlighted in such an architecture, as the work by Biggio et al [56] presents it. In the case of spoofing attacks, the attack surface is limited at the level of the biometric sensor itself.

TABLE II
BIOMETRICS WITH THE SPOOFING ATTACKS THEY ARE SUBJECTED TO.

		Biometric mechanisms																											
		Body Odor	Breath Recognition	DNA	Ear - Canal Echo	Ear - Shape	ECG	Eye - Iris	Eye - Retina	Eye - Sclera Vein	Face	Finger - Contactless	Finger - Geometry	Fingerprint	Finger - Vein	Handwriting	Hand - Geometry	Keystroke	Lips Motion	Palmprint	Palm - Vein	Skin Reflectivity	Stylometry	Teeth Shape	Thermography	Vocal Resonance	Voice	Walk
Spoofing Attacks	2-D print					[29]		[30]			[31]	[32]	[33]	[1]	[34]		[33]			[35]	[21]	[36]		[25]	[26]			
	2-D video							[30]			[31]		[33]				[33]					[36]		[25]				
	3-D model				[7]	[29]		[30]			[31]	[32]	[33]	[1]			[33]					[36]		[25]	[26]			
	Biological Samples			[37]																								
	Biological twin			[38]																								
	Contact Lens							[30]																				
	Plastic Film													[1]														
	Full-Fledge						[39]																					
	Impersonation		[40]													[17]		[19]	[41]			[36]	[42]			[43]	[44]	[45]
	Makeup										[46]																	
	Masking Sensors	[47]																										
	Replay		[40]				[48]												[41]							[43]	[49]	
	Stolen Clothes	[47]																										
	Spectral Conversion																										[50]	
	Synthesis																										[51]	

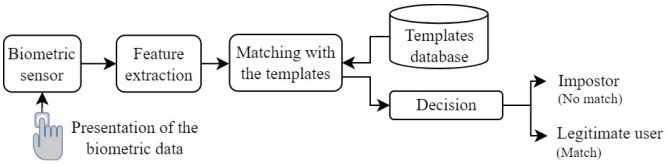

Fig. 1. Biometric authentication architecture.

4) Robustness Metric: To the best of our knowledge, quantitative robust metrics that take into consideration the properties of biometric technologies and the properties of the attacks they are subjected to, have not yet been introduced. The work by Gafurov et al [57] presents an impersonation attack against a gait authentication system with an active and a passive adversary, but the authors do not describe the properties of the attack they consider, neither a way to adapt their methodology to other families of attacks. The work by Rodrigues et al [58] presents two fusions schemes based on a fuzzy logic for enhancing the security of multimodal biometric systems, and a spoofing attack is taken as a use-case. However, this work does not specify that biometrics are all subjected to different kind of spoofing attacks, and a way to quantify the robustness of each biometrics facing each type of spoofing attack is not provided. The work by Akhtar et al [59] is dedicated to the robustness evaluation of multi-modal biometrics facing spoofing attacks. It is based on a quantification method of fake score distributions, and the authors used datasets to conduct their experiments. However, this work is only applied to a face recognition system, and a fingerprint system with the relevant datasets. The work by Hadid et al [60] presents spoofing attacks related to fingerprint and face recognition systems with an evaluation methodology based on the recognition rates of these biometrics. Our proposed methodology is different from the presented approaches. Indeed, we propose a generic and quantitative robust metric by investigating the properties of spoofing attacks and the properties of biometric mechanisms.

5) Robustness Assessment Authenticators Combinations: It is well-known that a single biometric may not be sufficient to guarantee the accuracy of an authentication process, and several works present combinations of several biometric mechanisms for more accurate and secure authentication processes [41], [61], [62]. Some evaluation methodologies applied to combinations of biometrics are also available in the literature such as the work by Wu et al [41]. In fact, this work presents a combination of Voice and Lips Motion biometrics that is, as claimed by the authors, "theoretically" robust against attacks such as recorded voice replaying without lips motion. However, such a biometric combination remains vulnerable facing an adversary who plays a recorded video of the voice of a legitimate person while imitating lips movements to match with the recorded voice. Indeed, the Lips Motion biometric technique is not capable of identifying the lips shapes, and this is why the previously stated attack can threaten the Voice and Lips Motion combination. This work also presents evaluation indicators such as True Positive Rate of the proposed authentication system. Another work, proposed by Stewart et al [62] is dedicated to a Keystroke-Stylometry combination to achieve a better robustness of the authentication process. The authors present an evaluation method based on the Equal Error Rate indicator, which is a percentage related to the accuracy of the authentication process conducted by the presented combination of biometrics. The previously stated two works do not present a generic robustness metric applied to biometric combinations, which takes into consideration the properties of the attacks and the biometric mechanisism properties. We address such a limitation in Section III.

III. Metric for Robustness Assessment

In this Section, we present a quantitative metric for a robustness assessment of the existing biometric techniques. We propose to build our own metric, that considers biometric mechanisms properties, such as the accuracy of biometric techniques, and also attacks properties, such as the maturity and the complexity of an attack. In a first time, qualitative values are attributed to these properties. The translation to quantitative values is made by following the strategy employed by the CVSS authors, which consist in assigning numerical values that follow linear distributions. The CVSS Scoring system [63] is an online calculator which provides three metrics for quantifying the severity of a vulnerability associated with a system. We start our investigation by presenting a robustness assessment method of single biometrics facing a single attack, and then, we generalize our methodology for a robustness assessment of biometrics facing several attacks. In a second time, we present a robustness assessment method for combinations of biometric mechanisms subjected to single and several attacks.

A. Single Authenticators Assessment

Our robustness assessment strategy makes abstraction of the environment the biometric mechanisms are implemented in. We consider the informations related to the biometric data and the properties of the attacks. Our choice to consider spoofing attacks is related to the fact that this family of attacks do not require the adversary to physically attack the biometric sensor. Thus, we consider that an authenticator is robust when facing a given attack if it is able to detect a fake presented biometric information. In the following content, we present the parameters used to build our assessment metric. These parameters can be classified into two groups, which are : Attack Efficiency Informations, and Biometric Data Informations. We define each of these parameters with their related qualitative values, and we propose a formula for a generic robustness assessment metric. The first parameters to be presented are related to the attack efficiency.

B. Attack Efficiency Informations

1) Attack Complexity: The Attack Complexity parameter quantifies the difficulty for an adversary to successfully exploit a vulnerability. For an attack α, we denote by $\mathcal{E}_{comp}(\alpha) \in [0,1]$ its Attack Complexity. This parameter is assumed to be "Low" if there is no specific conditions to exploit a vulnerability, and if it is easy for the adversary to perpetrate and repeat its attack ; "Medium" if the adversary needs to capture a behavioral data, which makes the attack more difficult to be perpetrated ; "High" if the adversary must prepare its attack and he needs specific resources, i.e., algorithms, physical material, etc., to successfully perpetrate it.

2) Attack Maturity: The Attack Maturity parameter quantifies the level of maturity of a given attack. For an attack α, we denote by $\mathcal{E}_{mat}(\alpha) \in [0,1]$ its Attack Maturity. This parameter is assumed to be "Unproven" when the attack implementation does not exist, or it is in a theoretical state ; "Proof-Of-Concept" if the implementation of the attack is not functional in all the situations and may need updates ; "Functional" if a functional way to implement the attack exists, and it works on most of the cases where the vulnerability exists ; "High" when a functional code, or a way to implement the attack is available with a full content related to the functional details.

3) Attack Remediation: The Attack Remediation parameter quantifies the state of countermeasures that exist to gap the vulnerability which is exploited by an attack. For an attack α, we denote by $\mathcal{E}_{rem}(\alpha) \in [0,1]$ its Attack Remediation. The possible could be "Unavailable" if there exist no countermeasures ; "Workaround" in the case where there is an unofficial solution available to avoid a given attack ; "Temporary Fix" if there exist an official and temporary fix solution for a given vulnerability ; "Officially Fix" if there is a complete vendor-solution available.

4) Attack Confidence: The Attack Confidence parameter quantifies the level of confidence in the success of an attack. For an attack α, we denote by $\mathcal{E}_{conf}(\alpha) \in [0,1]$ its Attack Confidence parameter. This parameter can be "Unknown" when there exist reports that highlight a vulnerability, but the cause of such a vulnerability is unknown, or there is no consensus on the cause of the vulnerability ; "Reasonable" if trusted and significant details have been published in the literature ; "Confirmed" if a detailed report is available.

Property 1: Let $\mathcal{E}(\alpha) \in [0,1]$ be the metric quantifying the efficiency of a spoofing attack α against a biometric authenticator. $\mathcal{E}(\alpha)$ is defined as follow :

$$\mathcal{E}(\alpha) = (\mathcal{E}_{mat}(\alpha) \times \mathcal{E}_{conf}(\alpha)) \times (1 - \mathcal{E}_{rem}(\alpha)) \times (1 - \mathcal{E}_{comp}(\alpha)) \quad (1)$$

The Equation 1 has been built by combining parameters that describe the power of an attack, such as $\mathcal{E}_{mat}$ and $\mathcal{E}_{conf}$. To these parameters, we combine $\mathcal{E}_{rem}$ and $\mathcal{E}_{comp}$ subtracted to one. Indeed, these two last parameters describe the properties that could make an attack difficult to be perpetrated.

An adversary who attempts to perpetrate an attack needs access to the biometric data to be spoofed. The following content is dedicated to the parameters used to quantify the complexity of getting a biometric data.

C. Biometric Data Information

1) Biometric Accuracy: The Biometric Accuracy parameter quantifies the reliability of a biometric mechanism during the authentication process. For a biometric β, we denote by $\mathcal{B}_{acc}(\beta)$ its Accuracy quantified as a percentage. For each biometric mechanism, we have investigated the literature to find surveys that evaluate their performance in terms of accuracy. For each biometric, we have filled the Table III with a range of accuracy, which corresponds to the minimum and the maximum values of accuracy found in the related surveys. We also provide a mean value of the accuracy for each biometric by considering all the performance estimations found in the surveys. This work has been done by considering

TABLE III
BIOMETRICS ACCURACY RANGE AND MEAN ACCURACY.

Biometrics	Refs.	Accuracy	
		Range (%)	*Mean (%)*
Body Odor	[3], [4]	$[85.00 - 88.00]$	86.5
Breath Recognition	[5]	$[91.56 - 92.21]$	91.85
DNA	[64]	X	99.9
Ear - Canal Echo	[7], [8]	$[93.04 - 97.57]$	95.31
Ear - Shape	[9]	$[52.00 - 100]$	89.34
ECG	[65]	$[73.00 - 100]$	95.3
Eye - Iris	[10]	$[93.60 - 99.40]$	96.45
Eye - Retina	[11]	$[90.21 - 100]$	98.57
Eye - Sclera Vein	[66]	$[92.65 - 99.07]$	96.75
Face	[67]	$[14.52 - 99.29]$	81.37
Finger - Contactless	[13]	$[91.67 - 98.93]$	95.56
Finger - Geometry	[68]	$[95.61 - 98.25]$	97.11
Finger - Print	[15]	$[75.35 - 98.60]$	90.6
Finger - Vein	[16]	$[79.00 - 100]$	96.3
Handwriting	[69]	$[76.00 - 97.00]$	87.23
Hand - Geometry	[18]	$[96.23 - 99.81]$	98.7
Keystroke	[70]	$[90.50 - 99.31]$	95.1
Lips Motion	[20]	$[53.00 - 100]$	90.65
Palm - Print	[71]	$[97.50 - 98.13]$	97.89
Palm - Vein	[72]	$[84.00 - 99.99]$	95.4
Skin Reflectivity	[22]	$[71.10 - 99.30]$	90.59
Stylometry	[23]	$[42.50 - 93.58]$	76.24
Teeth Shape	[24], [25]	$[55.00 - 99.74]$	81.34
Thermography	[73]	$[40.00 - 98.00]$	80.40
Vocal Resonance	[27]	$[94.20 - 96.10]$	95.15
Voice	[74]	$[61.40 - 100]$	87.54
Walk	[28]	$[57.80 - 99.90]$	86.48

the "Accuracy" and the "CRR" (Correct Recognition Rate) parameters evaluated in the surveys.

2) Victim Role: The Victim Role parameter quantifies the level of privileges required for an adversary to successfully interact with his victim in order to get a biometric data, and then perpetrate an attack. For a biometric β, we denote by $\mathcal{V}_{role}(\beta) \in [0,1]$ its Victim Role parameter. This parameter could refer to a "Low-Level" for Administration employees targeted by an adversary ; "Medium-Level" for Engineers employees targeted by an adversary ; "High-Level" for Head Departments employees targeted by an adversary.

Remark 2: The three presented role levels are generic, and can be adapted to other categories of employees. In our computation logic, the more complex a biometric is, the highest the role level is attributed. It means that an access to a restricted area of an organization, which requires complex biometrics, must only be owned by a person with a high role level in the organization.

3) Interaction with the victim: The Interaction with the victim parameter describes whether an interaction is required for an adversary with his victim, to get a biometric data and then, perpetrate an attack. For a biometric β, we denote by $\mathcal{V}_{interact}(\beta) \in [0,1]$ its Interaction with the victim parameter. We assume that this parameter could have a value "None" if the adversary does not need to interact with his victim to get a biometric data. In this case, the relevant biometric data can be found on the Internet, on Social Networks, etc. ; "Low" when the adversary needs to get a biometric data that is not publicly available and which needs low interactions, such as the capture of a fingerprint on an object ; "Medium" if the adversary needs to be physically close to his victim to get a biometric data such as a behavioral one, but he does not need to personally interact with his victim ; "High" for the case where the adversary needs to personally interact with his victim to get a biometric data.

4) Difficulty to Access the data: The Difficulty to Access the data parameter is the combination of the Victim Role and the Interaction with the victim parameters. For a biometric β, we denote by $\mathcal{B}_{DA}(\beta) \in [0,1]$ its Difficulty to Access parameter.

Property 2: The Difficulty to Access parameter $\mathcal{B}_{DA}(\beta)$ of a biometric β, is defined as follow :

$$\mathcal{B}_{DA}(\beta) = \mathcal{V}_{role}(\beta) \times \mathcal{V}_{interact}(\beta) \tag{2}$$

D. Translation to quantitative values

The previously introduced parameters are actually defined in a qualitative way. Our objective is to translate these qualitative values into quantitative ones for obtaining a numerical assessment with the robustness formula that we present in the next section. The CVSS Scoring System [63] uses a translation strategy from qualitative parameters to quantitative ones to provide a numerical criticality assessment associated with the vulnerabilities of a system. We follow the same strategy, and our investigations show that the numerical values used for the qualitative parameters of the CVSS follow linear distributions. According to this observation, we choose to assign the values as follows : Low=0.33 ; Medium=0.66 ; High=0.99 ; None=0.1. Due to the structure of our formula, it is not possible to choose a value equal to zero. We choose the value 0.1 for "None" as the closest value to zero. The same values are applied to the Victim Role parameter.

E. Robustness

In this section, we present our robustness formula which uses the previously introduced parameters.

Property 3: Let $\mathcal{R}(\beta,\alpha) \in [0,1]$ be the metric quantifying the robustness of a biometric authenticator β for a given attack α. The higher this indicator is, the more robust β is. $\mathcal{R}(\beta,\alpha)$ is defined as follow :

$$\mathcal{R}(\beta,\alpha) = (\mathcal{B}_{acc}(\beta) \times \mathcal{B}_{DA}(\beta)) \times (1 - \mathcal{E}(\alpha)) \tag{3}$$

With each numerical value of the defined parameters, we compute our robustness metric for single biometrics facing a single attack $\mathcal{R}(\beta,\alpha)$ and facing all the attacks they are subjected to $\mathcal{R}(\beta,\mathcal{A})$. The numerical results are presented in a Table available on GitHub [75]. We propose now to investigate the robustness assessment of biometric combinations.

F. Combination Assessment

A biometric authenticator considered as a single element used for an authentication process can be vulnerable to specific attacks. Depending on the biometric data the authenticator has been set up to identify, all the biometric authenticators do not have the same weaknesses, and they are not vulnerable to the same kind of attacks (spoofing or not). Several works

illustrate the combination of biometrics in order to provide a more secure authentication process. We can cite Lu, Huang, Deng and Alshamrani who have presented an authentication scheme which uses the Handwriting and the Hand Shape biometrics [61]. Wu et al have proposed an authentication method which uses the combination of the Voice and the Lips Motion biometrics [41]. Stewart et al have presented a work dedicated to an authentication strategy based on the use of the Stylometry and the Keystroke dynamics [62]. Other works presenting combinations of biometrics can be found in the literature, and we propose, as a contribution, to use our approach for a robustness quantification of such combinations of authenticators.

1) Combination of attacks: We have presented a metric for a robustness assessment of biometrics. Our investigations highlight that it is not possible for an adversary to combine several attacks in order to increase his power facing biometrics. Attacks perpetrated are, in a general way, able to bypass specific countermeasures implemented at the level of the biometric authentication techniques. However, there is no dependency between such attacks, and the observation made here is that an attack cannot improve another one.

We now generalize our metric for a robustness assessment of biometrics facing several attacks.

Property 4: Let us consider a biometric mechanism β, and $\mathcal{A} = \{\alpha_1, \ldots, \alpha_n\}$ the set of n attacks β is subjected to. The robustness of β becomes :

$$\mathcal{R}(\beta, \mathcal{A}) = \min_{\alpha \in \mathcal{A}} \mathcal{R}(\beta, \alpha) \tag{4}$$

Example 1: By applying the Properties 3 and 4 to the case of the Vocal Resonance mechanism, which is vulnerable to Impersonation and Replay attacks, we compute the robustness of $\beta = \mathit{Vocal\ Resonance}$ to $\mathcal{A} = \{\alpha_1, \alpha_2\}$ with $\alpha_1 = \mathit{Impersonation}$, and $\alpha_2 = \mathit{Replay}$. According to the Table [75], we have $\mathcal{R}(\beta, \mathcal{A}) = \min(0.3105, 0.8621) = 0.3105$.

As shown in Table [75], the robustness of several biometric technologies, such as the fingerprint mechanism, is low. Indeed, this can be explained by the fact that attacks could be able to bypass the security countermeasures of biometric technologies. In certain situations, the Attack Remediations are not sufficiently high and do not completely protect the biometric mechanism from an adversary. Thus, the adversary is able to get the biometric data, and to perpetrate an attack. This observation highlights the need to combine biometric mechanisms to have more accurate, secure and safer authentication processes [41], [61], [62]. This is why we propose to extend the application of our metric to combinations of biometric mechanisms. We address this subject in the following section.

2) Combination of biometric mechanisms: We have seen that biometrics are very diversified, and use different biological and behavioral data. However, these mechanisms can be dependent with other ones, and we propose to formalize this notion of dependency.

Definition 1 (Dependency): The dependency of a biometric data d_i with another biometric data d_j is assumed to be a numerical value in $[0, 1]$, rated $d_i \longrightarrow d_j$, i.e., it is the amount of informations of d_j obtained from d_i.

Property 5: Let us consider $\mathcal{M} = \{\beta_1, \beta_2\}$, as a set of 2 biometric mechanisms. Let d_i be the biometric data which is used for the authentication process to be conducted, with $i = \{1, 2\}$. The biometric mechanisms in $\mathcal{M}$ are data-dependent if the biometric data β_1 and β_2 are based on, are dependent.

Remark 3: The above definition provided is clearly related to the *Difficult to Access* parameter presented previously. In fact, the dependency between two biometrics makes it possible for an adversary to acquire a knowledge about a biometric data, from another one.

Example 2: Let us consider a combination of biometrics $\mathcal{M} = \{\beta_1, \beta_2\}$ with $\beta_1 = \mathit{Fingerprint}$ and $\beta_2 = \mathit{Palmprint}$. We can easily see that these two biometrics are dependent, and an adversary who has an access to a fingerprint data d_1 can perpetrate an attack against a fingerprint authenticator, and he can also acquire a knowledge about a palmprint data d_2 of a legitimate user. If the fingerprint data d_1 has a low *Difficult to Access* parameter DA_{d_1}, the *Difficult to Access* parameter DA_{d_2} of the palmprint biometric is going to decrease because of this dependency.

With these observations, we present the two following property which formalize the update procedure of the *Difficult to Access* parameter for both the cases where the biometric mechanisms are independant and dependant.

Property 6: Let us consider the *Difficult to Access* parameter of two biometric data d_i and d_j. If $d_i \longrightarrow d_j = 0$, i.e., there is no dependency between the biometric mechanisms β_i and β_j, we have :

$$DA_{d_j} = DA_{d_j} \tag{5}$$

If $d_i \longrightarrow d_j \neq 0$, i.e., there is a dependency between the biometric mechanisms β_i and β_j, we update the robustness value of the biometric mechanism β_j by setting-up its DA parameter as follow :

$$DA_{d_j} = \min(DA_{d_i} \times (d_i \longrightarrow d_j), DA_{d_j}) \tag{6}$$

Example 3: Let us consider the two biometric mechanisms $\beta_1 = \mathit{Fingerprint}$ and $\beta_2 = \mathit{Palmprint}$. We have $d_1 \longrightarrow d_2 = 0.1$ because a fingerprint can be assumed to be 10% of a palmprint data[1]. Thus, according to the Property 6 we have $DA_{d_2} = \min(0.1089 \times 0.1, 0.0979)$. DA_{d_2} is updated from 0.0979 to 0.0109.

This example shows that a dependency between two biometrics contributes to decrease the *Difficulty to Access* parameter of the biometric that include the data of the first one.

3) Robustness Assessment of Combinations: A robustness assessment of combinations of biometric mechanisms occurs in two different situations. In the first one, we consider the robustness of a combination facing a single attack.

[1]We assume that a palmprint is composed of 50% by the palm itself, and of $5 \times 10\%$ for each finger.

Property 7: Let us consider a combination of r biometric mechanisms $\mathcal{M}_C = \{\beta_i\}$, with $i = \{1, \ldots, r\}$. The robustness of $\mathcal{M}_C$ facing a spoofing attack α, rated $\mathcal{R}(\mathcal{M}_C, \alpha)$, is computed as follow :

$$\mathcal{R}(\mathcal{M}_C, \alpha) = \max_{\beta_i \in \mathcal{M}_C} \mathcal{R}(\beta_i, \alpha) \tag{7}$$

Example 4: Let us consider the case of the combination $\mathcal{M}_{C1}$ composed by the Fingerprint and the Palmprint biometrics, i.e., $\mathcal{M}_{C1} = \{\beta_1, \beta_2\}$ with $\beta_1 = \textit{Fingerprint}$ and $\beta_2 = \textit{Palmprint}$. $\mathcal{M}_{C1}$ could be vulnerable to 2-D print attacks. Thus, we have $\alpha = \textit{2D print}$. According to the Table [75], $\mathcal{R}(\beta_1, \alpha) = 0.0989$ and $\mathcal{R}(\beta_2, \alpha) = 0.0957$. Because $d_1 \longrightarrow d_2 = 0.1$, i.e., β_1 and β_2 are dependant, DA_{d_2}, i.e., the *Difficulty to Access* parameter of the palmprint biometric must be updated according to the Property 6. Due to this update, the robustness $\mathcal{R}(\beta, \alpha)$ of the palmprint biometric facing a 2-D print attack is updated from 0.0957 to 0.0107 with $DA_{d_2} = 0,0109$. Now, according to the Property 7 :

$$\begin{aligned} \mathcal{R}(\mathcal{M}_{C1}, \alpha) &= \max(\mathcal{R}(\beta_1, \alpha), \mathcal{R}(\beta_2, \alpha)) \\ &= \max(0.0989, 0.0107) = 0.0989 \end{aligned} \tag{8}$$

In the second case, we consider the robustness of a combination of authentication mechanisms facing several attacks.

Property 8: Let us consider a combination of s biometric mechanisms $\mathcal{M}_{C2} = \{\beta_j\}$, with $j = \{1, \ldots, s\}$. Let us also consider a set of t attacks $\mathcal{A} = \{\alpha_t\}$, with $t = \{1, \ldots, s\}$. The robustness of $\mathcal{M}_{C2}$ facing the attacks of $\mathcal{A}$, rated $\mathcal{R}(\mathcal{M}_{C2}, \mathcal{A})$, is computed as follow :

$$\mathcal{R}(\mathcal{M}_{C2}, \mathcal{A}) = \min(\max_{\beta_j \in \mathcal{M}_{C2}} \mathcal{R}(\beta_j, \mathcal{A})) \tag{9}$$

Remark 4: All the biometrics are not subjected to the same attacks. In a combination of biometrics $\mathcal{M} = \{\beta_1, \beta_2\}$, with $\mathcal{M}$ subjected to α, β_1 could be vulnerable to α but β_2 may not be exposed to α. In such a case, the Property 7 can still be applied by considering $\mathcal{R}(\beta_2, \alpha) = 1$. The same reasoning can be applied to the Property 8.

Example 5: Let us consider the case of the combination $\mathcal{M}_{C2}$ composed by the Voice and the Lips Motion, i.e., $\mathcal{M}_{C2} = \{\beta_1, \beta_2\}$ with $\beta_1 = \textit{Voice}$ and $\beta_2 = \textit{Lips Motion}$. $\mathcal{M}_{C2}$ could be vulnerable to Impersonation and Replay attacks. Thus, we have $\alpha_1 = \textit{Impersonation}$ and $\alpha_2 = \textit{Replay}$, and we have $\mathcal{A}_{C2} = \{\alpha_1, \alpha_2\}$. According to the Table [75], $\mathcal{R}(\beta_1, \alpha_1) = 0.3527$, $\mathcal{R}(\beta_1, \alpha_2) = 0.3801$, $\mathcal{R}(\beta_2, \alpha_1) = 0.1972$, and $\mathcal{R}(\beta_2, \alpha_2) = 0.2952$. We have $d_1 \longrightarrow d_2 = 0$, i.e., β_1 and β_2 are assumed to not be dependant. In fact, we consider an adversary perpetrating a replay attack, who acquired the voice biometric data on an audio recorder. According to the Property 8, we have :

$$\begin{aligned} \mathcal{R}(\mathcal{M}_{C2}, \mathcal{A}_{C2}) = \min(&\max(\mathcal{R}(\beta_1, \alpha_1), \mathcal{R}(\beta_2, \alpha_1)), \\ &\max(\mathcal{R}(\beta_1, \alpha_2), \mathcal{R}(\beta_2, \alpha_2))) \\ = \min(&\max(0.3527, 0.1972), \\ &\max(0.3801, 0.2952)) = 0.3527 \end{aligned} \tag{10}$$

Remark 5: In the previous example, we have assumed that the adversary has recorded the voice data on an audio recorder, and thus, there is no dependency between the Voice and Lips Motion biometrics. However, if the adversary would have recording the voice data with a camera focused on the mouth of the legitimate user, we would have had $d_1 \longrightarrow d_2 \neq 0$, i.e., there would have been a dependency between the two biometrics. In this case, the robustness of the Lips Motion biometric would have been impacted.

In the next section, we discuss the applications of our metrics.

IV. Discussion

The idea behind combining biometric authenticators is that a biometric can gap the weaknesses of another one, and the results provided in Table IV show that the considered combinations are more robust than the biometrics considered as single elements. Indeed, the less a biometric is subjected to attacks, the more robust it is. Combining two authenticators can avoid, or make more difficult the perpetration of attacks. From the combinations in the literature that we have presented in Section III-F, we notice that the mechanisms that constitute a combination generally trigger biometric data located in the same area of the human body. In fact, the biometrics of the combination Handwriting-Hand Shape are both located at the level of the hands. The Voice-Lips Motion biometrics are both located at the level of the mouth. This can be explained by the fact that it is easier and less expensive to implement a combination of biometrics targeting the same area of the body. For example, combining Palm Vein and Walk biometrics requires two different systems, one for reading physiological data, and the other one to read behavioral data. Such an authentication may be expensive and difficult to implement due to the material it requires. However, these two biometrics constitute a very safe authentication strategy, and here we have an example where two biometrics can be associated to make it extremely difficult for an adversary to perpetrate a "perfect" attack. Our proposed approach is not only related to a robustness assessment of already implemented biometric mechanisms. In fact, we propose to use it during the decision process for finding the better combinations to use, i.e., the more robust combinations from a set of several authenticators. The presented metrics can be used to make a comparison between combinations of biometrics, and help to choose the better ones in terms of robustness. The Table IV presents the robustness assessment of three biometric combinations from the literature, facing single and all the attacks each combination is exposed to, plus three additional combinations introduced as examples.

As shown in Table IV, we see that the only combination for which the two biometric mechanisms are dependent, i.e., the Voice-Lips Motion combination, has the lower degree of robustness facing all the attacks $\mathcal{R}(\mathcal{M}, \mathcal{A})$. Furthermore, we also see that combining physiological and behavioral biometrics, like Palm Vein-Walk biometrics, can provide a good level of robustness. However, we must highlight that

TABLE IV
BIOMETRIC COMBINATIONS WITH THEIR ROBUSTNESS ASSESSMENT.

		Spoofing Attack α	$\mathcal{R}(\mathcal{M},\alpha)$	$\mathcal{R}(\mathcal{M},\mathcal{A})$
$\mathcal{M}$ **in the literature**	Handwriting & Hand Shape [61]	2-D paper	1	1
		2-D video	1	
		3-D model	1	
		Impersonation	1	
	Voice & Lips Motion [41]	Impersonation	0.3527	0.3527
		Replay	0.3801	
		Synthesis	1	
		Spectral conversion	1	
	Stylometry & Keystroke [62]	Impersonation	0.4967	0.4967
$\mathcal{M}$ **examples**	Fingerprint & Palm Vein	2-D paper	0.6633	0.6633
		3-D model	1	
		Plastic film	1	
	Fingerprint & Walk	2-D paper	1	1
		3-D model	1	
		Plastic film	1	
		Impersonation	1	
	Palm Vein & Walk	2-D paper	1	1
		Impersonation	1	

the cost of the mechanisms needs to be taken into account. In fact, the biometrics with the better degree of robustness are generally the more complex and the more expensive ones. Even if all weaknesses can not be avoided, and the spoofing attacks a combination of biometrics is subjected to can not all also be avoided, a fine balance must be found between the biometrics combined and the corresponding attack surface. The more robust a combination is, the less the attack surface.

V. CONCLUSION AND FUTURE WORKS

We have presented an exhaustive overview of the biometric technologies by recensing the existing biometric mechanisms and the emerging ones. For each of these biometrics, we have recensed the spoofing attacks they are subjected to, and according to a quantitative metrics we build, we have proposed a robustness assessment of single biometrics and combinations of biometric mechanisms facing one and several attacks. Our approach is a generic assessment method, and we used the family of spoofing attacks to demonstrate our approach, but other families of cyber-attacks are compatible with our methodology. The next steps of our work consist in combining the properties established with new metrics for quantifying the usability of biometric mechanisms in a specific environment with specific constraints. Our objective is to extend such a robustness assessment by taking into consideration the environmental properties that may impact the lectures of biometrics.

ACKNOWLEDGMENT

This work has been supported by the French government under the "France 2030" program, as part of the SystemX Technological Research Institute within the PFS project.

REFERENCES

[1] C. Sousedik and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: a survey," *Iet Biometrics*, vol. 3, no. 4, pp. 219–233, 2014.

[2] Z. Rui and Z. Yan, "A survey on biometric authentication: Toward secure and privacy-preserving identification," *IEEE Access*, vol. 7, pp. 5994–6009, 2019.

[3] B. Yang and W. Lee, "Human body odor based authentication using machine learning," in *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2018, pp. 1707–1714.

[4] I. Traore, M. Alshahrani, and M. S. Obaidat, "State of the art and perspectives on traditional and emerging biometrics: A survey," *Security and Privacy*, vol. 1, no. 6, p. e44, 2018.

[5] J. Liu, Y. Chen, Y. Dong, Y. Wang, T. Zhao, and Y.-D. Yao, "Continuous user verification via respiratory biometrics," in *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications*, 2020, pp. 1–10.

[6] A. Z. Zahid, I. H. Mohammed Salih Al-Kharsan, H. A. Bakarman, M. F. Ghazi, H. A. Salman, and F. N. Hasoon, "Biometric authentication security system using human dna," in *2019 First International Conference of Intelligent Computing and Engineering (ICOICE)*, 2019, pp. 1–7.

[7] Y. Gao, W. Wang, V. V. Phoha, W. Sun, and Z. Jin, "Earecho: Using ear canal echo for wearable authentication," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 3, no. 3, sep 2019.

[8] Z. Wang, S. Tan, L. Zhang, Y. Ren, Z. Wang, and J. Yang, "Eardynamic: An ear canal deformation based continuous user authentication using in-ear wearables," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 5, no. 1, mar 2021.

[9] A. Abaza, A. Ross, C. Hebert, M. A. F. Harrison, and M. S. Nixon, "A survey on ear biometrics," *ACM Comput. Surv.*, vol. 45, no. 2, mar 2013.

[10] Y. W. Lee and K. R. Park, "Recent iris and ocular recognition methods in high- and low-resolution images: A survey," *Mathematics*, vol. 10, no. 12, 2022. [Online]. Available: https://www.mdpi.com/2227-7390/10/12/2063

[11] J. B. Mazumdar and S. Nirmala, "Retina based biometric authentication system : A review." *International Journal of Advanced Research in Computer Science*, vol. 9, no. 1, 2018.

[12] P. Rot, M. Vitek, K. Grm, Ž. Emeršič, P. Peer, and V. Štruc, "Deep sclera segmentation and recognition," in *Handbook of vascular biometrics*. Springer, Cham, 2020, pp. 395–432.

[13] X. Yin, Y. Zhu, and J. Hu, "Contactless fingerprint recognition based on global minutia topology and loose genetic algorithm," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 28–41, 2020.

[14] L. qing Zhu and S. yuan Zhang, "Multimodal biometric identification system based on finger geometry, knuckle print and palm print," *Pattern Recognition Letters*, vol. 31, no. 12, pp. 1641–1649, 2010, pattern Recognition of Non-Speech Audio.

[15] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, 2019.

[16] K. Syazana-Itqan, A. Syafeeza, N. Saad, N. A. Hamid, and W. Saad, "A review of finger-vein biometrics identification approaches," *Indian J. Sci. Technol*, vol. 9, no. 32, pp. 1–9, 2016.

[17] I. Griswold-Steiner, R. Matovu, and A. Serwadda, "Wearables-driven freeform handwriting authentication," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 1, no. 3, pp. 152–164, 2019.

[18] M. K. Ahuja and A. Singh, "A survey of hand geometry recognition," *International Journal*, vol. 3, no. 3, 2015.

[19] H. Khan, U. Hengartner, and D. Vogel, "Mimicry attacks on smartphone keystroke authentication," *ACM Trans. Priv. Secur.*, vol. 23, no. 1, feb 2020.

[20] D. P. Chowdhury, R. Kumari, S. Bakshi, M. N. Sahoo, and A. Das, "Lip as biometric and beyond: a survey," *Multimedia Tools and Applications*, vol. 81, no. 3, pp. 3831–3865, 2022.

[21] P. Tome and S. Marcel, "On the vulnerability of palm vein recognition to spoofing attacks," in *2015 International Conference on Biometrics (ICB)*, 2015, pp. 319–325.

[22] R. Munir and R. A. Khan, "An extensive review on spectral imaging in biometric systems: Challenges & advancements," *Journal of Visual Communication and Image Representation*, vol. 65, p. 102660, 2019.

[23] T. Neal, K. Sundararajan, A. Fatima, Y. Yan, Y. Xiang, and D. Woodard, "Surveying stylometry techniques and applications," *ACM Comput. Surv.*, vol. 50, no. 6, nov 2017.

[24] M. Banday and A. H. Mir, "Biometric identification system using panoramic dental radiograms based on car model," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, 2021, pp. 832–835.

[25] H. Jiang, H. Cao, D. Liu, J. Xiong, and Z. Cao, "Smileauth: Using dental edge biometrics for user authentication on smartphones," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 4, no. 3, sep 2020. [Online]. Available: https://doi.org/10.1145/3411806

[26] M. Kowalski, "A study on presentation attack detection in thermal infrared," *Sensors*, vol. 20, no. 14, 2020.

[27] R. Liu, C. Cornelius, R. Rawassizadeh, R. Peterson, and D. Kotz, "Vocal resonance: Using internal body voice for wearable authentication," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, no. 1, mar 2018.

[28] A. Sepas-Moghaddam and A. Etemad, "Deep gait recognition: A survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, pp. 1–1, 2022.

[29] î. Toprak and O. Toygar, "Detection of spoofing attacks for ear biometrics through image quality assessment and deep learning," *Expert Systems with Applications*, vol. 172, p. 114600, 2021.

[30] R. Agarwal and A. S. Jalal, "Presentation attack detection system for fake iris: a review," *Multimedia Tools and Applications*, vol. 80, no. 10, pp. 15 193–15 214, 2021.

[31] A. F. Ebihara, K. Sakurai, and H. Imaoka, "Efficient face spoofing detection with flash," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 4, pp. 535–549, 2021.

[32] S. Miller. (2017) Spoofing Countermeasures in Contactless Optical Fingerprint Acquisition. [Online]. Available: https://www.linkedin.com/pulse/spoofing-countermeasures-contactless-optical-seth-miller

[33] H. Chen, H. Valizadegan, C. Jackson, S. Soltysiak, and A. K. Jain, "Fake hands: spoofing hand geometry systems," *Biometric Consortium*, 2005.

[34] P. Tome, M. Vanoni, and S. Marcel, "On the vulnerability of finger vein recognition to spoofing," in *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 2014, pp. 1–10.

[35] M. Farmanbar and Ö. Toygar, "Spoof detection on face and palmprint biometrics," *Signal, Image and Video Processing*, vol. 11, no. 7, pp. 1253–1260, 2017.

[36] Y. Tian, K. Zhang, L. Wang, and Z. Sun, "Face anti-spoofing by learning polarization cues in a real-world scenario," in *2020 4th International Conference on Advances in Image Processing*, ser. ICAIP 2020. New York, NY, USA: Association for Computing Machinery, 2020, p. 129–137.

[37] T. Anderson, J. P. Ross, R. K. Roby, D. A. Lee, and M. M. Holland, "A validation study for the extraction and analysis of dna from human nail material and its application to forensic casework." *Journal of forensic sciences*, vol. 44 5, pp. 1053–6, 1999.

[38] K. M. Sudar, P. Deepalakshmi, K. Ponmozhi, and P. Nagaraj, "Analysis of security threats and countermeasures for various biometric techniques," in *2019 IEEE International Conference on Clean Energy and Energy Efficient Electronics Circuit for Sustainable Development (INCCES)*, 2019, pp. 1–6.

[39] N. Karimian, D. Woodard, and D. Forte, "Ecg biometric: Spoofing and countermeasures," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 2, no. 3, pp. 257–270, 2020.

[40] J. Chauhan, Y. Hu, S. Seneviratne, A. Misra, A. Seneviratne, and Y. Lee, "Breathprint: Breathing acoustics-based user authentication," in *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '17. New York, NY, USA: Association for Computing Machinery, 2017, p. 278–291.

[41] L. Wu, J. Yang, M. Zhou, Y. Chen, and Q. Wang, "Lvid: A multimodal biometrics authentication system on smartphones," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1572–1585, 2020.

[42] S. Duman, K. Kalkan-Cakmakci, M. Egele, W. Robertson, and E. Kirda, "Emailprofiler: Spearphishing filtering with header and stylometric features of emails," in *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1, 2016, pp. 408–416.

[43] H. Li, C. Xu, A. S. Rathore, Z. Li, H. Zhang, C. Song, K. Wang, L. Su, F. Lin, K. Ren, and W. Xu, "Vocalprint: A mmwave-based unmediated vocal sensing system for secure authentication," *IEEE Transactions on Mobile Computing*, pp. 1–1, 2021.

[44] Y. W. Lau, M. Wagner, and D. Tran, "Vulnerability of speaker verification to voice mimicking," in *Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004.*, 2004, pp. 145–148.

[45] D. Gafurov, E. Snekkenes, and P. Bours, "Spoof attacks on gait authentication system," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 491–502, 2007.

[46] K. Kotwal, Z. Mostaani, and S. Marcel, "Detection of age-induced makeup attacks on face recognition systems using multi-layer deep features," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 2, no. 1, pp. 15–25, 2020.

[47] M. D. Gibbs, "Biometrics: Body odor authentication perception and acceptance," *SIGCAS Comput. Soc.*, vol. 40, no. 4, p. 16–24, dec 2010.

[48] S. Eberz, N. Paoletti, M. Roeschlin, M. Kwiatkowska, I. Martinovic, and A. Patané, "Broken hearted: How to attack ecg biometrics," *Network and Distributed System Security Symposium*, 2017.

[49] Z. Wu and H. Li, "On the study of replay and voice conversion attacks to text-dependent speaker verification," *Multimedia Tools and Applications*, vol. 75, no. 9, pp. 5311–5327, 2016.

[50] A. Kassis and U. Hengartner, "Practical attacks on voice spoofing countermeasures," *arXiv preprint arXiv:2107.14642*, 2021.

[51] T. Toda, A. W. Black, and K. Tokuda, "Voice conversion based on maximum-likelihood estimation of spectral parameter trajectory," *IEEE Transactions on Audio, Speech, and Language Processing*, vol. 15, no. 8, pp. 2222–2235, 2007.

[52] M. F. Zibran, "Eye based authentication : Iris and retina recognition," 2011.

[53] K. D. Deshmukh and H. H. Kulkarni, "Effective segmentation of sclera region from eye image using contour," in *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, 2018, pp. 1–3.

[54] I. Buciu and A. Gacsadi, "Biometrics systems and technologies: A survey," *International Journal Of Computers Communications & Control*, vol. 11, no. 3, pp. 315–330, 2016.

[55] M. J. Stephen and P. P. Reddy, "Implementation of easy fingerprint image authentication with traditional euclidean and singular value decomposition algorithms," *Int. J. Advance. Soft Comput. Appl*, vol. 3, no. 2, 2011.

[56] B. Biggio, g. fumera, P. Russu, L. Didaci, and F. Roli, "Adversarial biometric recognition : A review on biometric system security from the adversarial machine-learning perspective," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 31–41, 2015.

[57] D. Gafurov, E. Snekkenes, and T. E. Buvarp, "Robustness of biometric gait authentication against impersonation attack," in *On the Move to Meaningful Internet Systems 2006: OTM 2006 Workshops*, R. Meersman, Z. Tari, and P. Herrero, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 479–488.

[58] R. N. Rodrigues, L. L. Ling, and V. Govindaraju, "Robustness of multimodal biometric fusion methods against spoof attacks," *Journal of Visual Languages & Computing*, vol. 20, no. 3, pp. 169–179, 2009.

[59] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Robustness evaluation of biometric systems under spoof attacks," in *Image Analysis and Processing – ICIAP 2011*, G. Maino and G. L. Foresti, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 159–168.

[60] A. Hadid, N. Evans, S. Marcel, and J. Fierrez, "Biometrics systems under spoofing attack: An evaluation methodology and lessons learned," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 20–30, 2015.

[61] D. Lu, D. Huang, Y. Deng, and A. Alshamrani, "Multifactor user authentication with in-air-handwriting and hand geometry," in *2018 International Conference on Biometrics (ICB)*, 2018, pp. 255–262.

[62] J. C. Stewart, J. V. Monaco, S.-H. Cha, and C. C. Tappert, "An investigation of keystroke and stylometry traits for authenticating online test takers," in *2011 International Joint Conference on Biometrics (IJCB)*, 2011, pp. 1–7.

[63] *Common Vulnerability Scoring System version 3.1 Specification Document - Revision 1*, FIRST, 6 2019, revision 1.

[64] DNAForce. (2015) The Accuracy of DNA Testing. [Online]. Available: https://dna-testing.ca/article/the-accuracy-of-dna-testing.html

[65] D. A. AlDuwaile and M. S. Islam, "Using convolutional neural network and a single heartbeat for ecg biometric recognition," *Entropy*, vol. 23, no. 6, 2021.

[66] S. Sharma and G. R. V, "Sclera segmentation techniques," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 9, no. 2, pp. 1072–1076, jul 2020.

[67] F. Liu, D. Chen, F. Wang, Z. Li, and F. Xu, "Deep learning based single sample face recognition: a survey," *Artificial Intelligence Review*, pp. 1–26, 2022.

[68] A. Bera and D. Bhattacharjee, "Human identification using selected features from finger geometric profiles," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 50, no. 3, pp. 747–761, 2020.

[69] R. K. Samsuryadi and F. S. Mohamad, "Automated handwriting analysis based on pattern recognition: A survey," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 22, no. 1, pp. 196–206, 2021.
[70] A. Tewari, "Keystroke dynamics based recognition systems using deep learning: A survey," 2022.
[71] M. Ali, V. H. Mahale, P. L. Yannawar, and A. T. Gaikwad, "A review: palmprint recognition process and techniques," *International Journal of Applied Engineering Research*, vol. 13, no. 10, pp. 7499–7507, 2018.
[72] W. Wu, S. J. Elliott, S. Lin, S. Sun, and Y. Tang, "Review of palm vein recognition," *IET Biometrics*, vol. 9, no. 1, pp. 1–10, 2020.
[73] R. Shoja Ghiass, O. Arandjelović, A. Bendada, and X. Maldague, "Infrared face recognition: A comprehensive review of methodologies and databases," *Pattern Recognition*, vol. 47, no. 9, pp. 2807–2824, 2014.
[74] N. H. Tandel, H. B. Prajapati, and V. K. Dabhi, "Voice recognition and voice comparison using machine learning techniques: A survey," in *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2020, pp. 459–465.
[75] "Robustness Assessment of Biometrics," https://github.com/IRT-SystemX/robustness_assessment_biometrics, gitHub repository, created: 2023-09-14.