Técnicas de Anonimización para Datos Biométricos Conductuales: Un Estudio

Dr. Simon Hanisch[1]
Prof. Patricia Arias Cabarcos[2]
Dr. Javier Parra Arnau[3]
Prof. Thorsten Strufe[1]

Agencia Española de Protección de Datos
Premio de Investigación en Protección de Datos Personales "Emilio Aced"

[1] Karlsruher Institut für Technologie, Alemania
[2] Universität Paderborn, Alemania
[3] Universitat Politècnica de Catalunya, España

Barcelona, 30 de enero de 2026

Contenido

1 Introducción

La actual transformación digital está conduciendo a una recopilación de datos cada vez más exhaustiva sobre los ciudadanos. La mejora constante de dispositivos electrónicos periféricos como las gafas de realidad aumentada (RA)/realidad virtual (RV), trajes y guantes de captura de movimiento, relojes inteligentes y otros dispositivos *wearables*, aumentan drásticamente la cobertura y la resolución a la que nuestros datos biométricos y de comportamiento pasan a estar disponibles para su procesado.

Una gran cantidad de estos datos se comparte de forma consciente: cuando publicamos fotos, vídeos u opiniones sobre productos o temas de actualidad, compartimos nuestra ubicación en redes sociales, participamos en foros o blogs, o valoramos servicios y establecimientos, entre muchos otros ejemplos. Una cantidad aún mayor se recopila de manera inadvertida, ya sea cuando navegamos por la Web, utilizamos servicios de geolocalización en aplicaciones de navegación o recomendación, o simplemente al entrar en espacios inteligentes equipados con asistentes de voz y cámaras.

Los correspondientes datos conductuales o de comportamiento son altamente descriptivos del individuo y pueden revelar una multitud de atributos personales. Contienen fuertes indicadores de rutinas, hábitos y también información médica, manías y tics. Las correlaciones conocidas entre características fisiológicas y condiciones médicas incluyen la detección de depresión [60] en fotografías faciales, la detección de insuficiencias orgánicas debido a la coloración de los ojos (hepatitis) o la piel (abuso de alcohol [58], estado físico general [219], y otros). Los datos conductuales también pueden utilizarse para identificar a individuos de forma única. Ejemplos destacados en todo el espectro incluyen la identificación de rasgos y características personales a partir de los "feeds" de redes sociales [144], la identificación de usuarios por sus patrones de movilidad [61] y su comportamiento de navegación web [68]. La marcha se ha utilizado de forma muy destacada para identificar a individuos [288, 313], y obviamente tiene el potencial de revelar atributos individuales como la edad, el género y las condiciones fisiológicas [280].

Preservar la privacidad —y, en última instancia, la dignidad— de las personas que entran en el alcance de estos sensores y cuyos comportamientos son captados requiere enfoques mucho más sofisticados que la simple eliminación de identificadores directos (p. ej., dirección IP, número de la seguridad social, difuminado del rostro) o de cuasi-identificadores intuitivos (como género, edad o etnia) en las bases de datos. Cabe señalar que los datos de comportamiento humanos presentan tanto dependencias temporales —derivadas de su naturaleza secuencial— como dependencias fisiológicas, impuestas por las restricciones biológicas y físicas propias del organismo humano. Estas interdependencias estructurales entre observaciones ponen en entredicho la eficacia de las técnicas de anonimización basadas en aleatorización o perturbación, ya que pueden ofrecer vías para reconstruir información identificativa que tales técnicas pretenden eliminar. Además, la presencia de información contextual y de patrones conductuales estables (que a menudo se manifiestan como señales de gran intensidad) añade una capa adicional de complejidad, dificultando una anonimización verdaderamente robusta.

Un creciente número de estudios está abordando el reto de anonimizar los datos de comportamiento. Se centran en una variedad de rasgos humanos diferentes, que van desde la voz, pasando por la marcha, hasta ejemplos menos destacados como los gestos o el ritmo cardíaco. Consideramos necesaria una revisión sistemática de todas estas soluciones, que permita identificar las similitudes conceptuales y metodológicas que comparten, y establecer puentes entre ellas. Asimismo, buscamos destacar las diferencias entre los distintos enfoques, esclarecer sus propiedades conceptuales y señalar las oportunidades de investigación que se abren a futuro.

En este décima edición de los *Premios a la Protección de Datos de Carácter Personal*, presentamos un estudio sistemático y crítico del estado del arte de técnicas de protección para datos biométricos

conductuales. Nuestro trabajo profundiza en las tecnologías de mejora de la privacidad aplicables a escenarios en los que los datos de comportamiento son recopilados por terceros o compartidos con ellos para llevar a cabo una operación específica o prestar un servicio.

El estudio se centra en la privacidad de los datos más que en su confidencialidad: no abordamos soluciones en las que una entidad cifra sus propios datos para impedir el acceso por parte de terceros. En su lugar, analizamos aquellas propuestas diseñadas para evitar la revelación no intencionada de la información contenida en los datos [51]. Por este motivo, enfoques como la computación confidencial, el procesamiento basado en criptografía homomórfica o técnicas afines —en los que el propietario de los datos es la única entidad que puede inferir información a partir de ellos— quedan fuera del alcance de nuestro análisis.

Para nuestro estudio seguimos las directrices de Kitchenham [140] para identificar y examinar de manera sistemática el estado actual de la técnica. El proceso nos llevó a analizar 142 estudios distintos, seleccionados a partir de un corpus inicial de 364 trabajos.

Identificamos las aplicaciones más comunes que procesan datos de comportamiento, con el fin de extraer métricas de utilidad relevantes, así como las amenazas típicas a la privacidad y los correspondientes modelos de adversario. Asimismo, definimos dos taxonomías de anonimización específicas para este tipo de datos: la primera clasifica las técnicas en función de cómo transforman los datos, mientras que la segunda se centra en el objetivo de anonimización que buscan garantizar.

A continuación, presentamos un resumen detallado de las diferentes soluciones de anonimización, organizadas según el rasgo que pretenden proteger. Para cada propuesta, proporcionamos información sobre las aplicaciones que determinan la utilidad, las amenazas a la privacidad consideradas, los objetivos de privacidad perseguidos, los conceptos de anonimización aplicados y la evaluación realizada por los autores, incluyendo los conjuntos de datos empleados.

En este contexto, nuestro estudio contribuye a una mejor comprensión de los riesgos asociados al uso de tecnologías emergentes que operan sobre datos especialmente sensibles y potencialmente de alto impacto social. Al profundizar en estos riesgos y en las medidas de mitigación disponibles, nuestro trabajo ofrece elementos clave para promover un uso responsable y seguro de estas tecnologías.

Este trabajo se ha desarrollado en el marco de un proyecto internacional llevado a cabo por investigadores del Karlsruher Institut für Technologie (Alemania), la Universität Paderborn (Alemania) y la Universitat Politècnica de Catalunya. Los resultados han sido publicados en la prestigiosa revista *ACM Computing Surveys*, que cuenta con un factor de impacto de 23.8 y ocupa la primera posición en la categoría de revistas internacionales en el ámbito de la *informática, teoría y métodos*. Desde su publicación en línea en junio de 2025 ha recibido un total de 32 citas (Google Scholar). La referencia bibliográfica completa se muestra debajo.

Simon Hanisch, Patricia Arias-Cabarcos, Javier Parra-Arnau, and Thorsten Strufe, "Anonymization Techniques for Behavioral Biometric Data: A Survey". ACM Computing Surveys, vol. 57, no. 11, Article 272 (November 2025), 54 pages. IF: 23.8; 1/144, D1 (computer science, theory & methods). DOI: https://dl.acm.org/doi/10.1145/3729418.

2 Antecedentes

En esta sección, primero revisamos la terminología relevante utilizada a lo largo de este trabajo y las revisiones existentes sobre técnicas de anonimización. A continuación, presentamos la metodología que utilizamos para realizar la revisión sistemática de la literatura.

2.1 Terminología

Nuestro uso del término **mejora de la privacidad** o **protección** se referirá a la ofuscación de información frente a cualquier observador adversario, incluido el proveedor de servicios , independientemente de si esta ofuscación consiste en control de acceso a datos, cifrado, minimización de los datos revelados, o modificación de datos, perturbación, parcial o total, de cualquier manera. En el sentido más abstracto, la información de comportamiento a proteger puede estar compuesta por varios elementos, incluyendo enlaces o relaciones entre varios fragmentos de información. Tenga en cuenta que más adelante nos centraremos en técnicas que controlan la divulgación en procesos donde partes no confiables obtienen acceso a *algunos* datos interpretables, en lugar de procesos en los que partes no confiables obtienen acceso únicamente a datos cifrados.

Un tipo importante de información a ofuscar es la **identidad** explícita de un usuario. La estrecha relación entre los dispositivos personales (como teléfonos inteligentes o dispositivos vestibles) y sus usuarios hace que las características distintivas (p. ej., huellas digitales del dispositivo) en dichos dispositivos sean identificadores potencialmente únicos. Nos adherimos a la convención de que el **anonimato** es el caso particular de la privacidad en el que los datos no pueden vincularse al individuo al que se refieren los datos. Esto se refiere no solo a los identificadores directos[1] sino también a los identificadores indirectos.

En el campo del control de revelación estadística (SDC) [292], el objetivo es proteger un conjunto de microdatos, asegurando al mismo tiempo que estos datos sigan siendo útiles para los investigadores. Un conjunto de microdatos es una base de datos cuyos registros contienen información al nivel de encuestados individuales. En este campo, los conceptos de **divulgación de identidad y atributos** se refieren al objetivo de un atacante de averiguar o la identidad de un individuo en el conjunto de microdatos o el/los atributo/s confidencial/es del mismo.

Emplearemos el término **utilidad** para cuantificar el grado de funcionalidad mantenido con respecto a un servicio para el cual están destinados los datos biométricos de comportamiento. La utilidad se mantiene a pesar de la implementación de un mecanismo de privacidad que puede ocultar o perturbar parte de los datos, lo que puede degradar la calidad del servicio. Recalcamos que la utilidad en este contexto no se refiere al diseño de la interfaz de usuario.

Como se señaló anteriormente en la introducción, cualquier PET plantea un **compromiso entre privacidad y funcionalidad**. La optimización del compromiso privacidad-funcionalidad (o privacidad-utilidad) se referirá al diseño y ajuste de las PET para maximizar la privacidad para una funcionalidad deseada, o viceversa.

2.2 Estudios relacionados

La mayoría de las revisiones sobre datos de comportamiento se centran en analizar la unicidad y la idoneidad de los rasgos de comportamiento para identificar a las personas, comparando la precisión de diferentes enfoques y su aplicabilidad. En esta línea de investigación, encontramos revisiones que cubren una gama de biometrías de comportamiento existentes para la autenticación de usuarios [13, 153, 164, 181], y otras que se centran en la revisión de rasgos específicos, como el reconocimiento de la marcha [288], las pulsaciones de teclas [19, 271], la mirada [135], o la biometría de ondas cerebrales [98]. Sin embargo, el tratamiento de las cuestiones de privacidad se limita a mencionar que existe el potencial de inferencias sensibles o filtraciones de identidad, pero no hay una discusión en profundidad sobre las contramedidas de privacidad.

[1] Los identificadores directos permiten identificar inequívocamente a los individuos. Por ejemplo, sería el caso de los números de la seguridad social (SSN) o nombres completos. En un proceso de anonimización de datos, los identificadores directos siempre se eliminan en la primera fase.

Existe una importante corriente de investigación sobre posibles ataques a la privacidad de los datos de comportamiento centrada en la **inferencia de atributos** [18, 34, 123], o que trata la desidentificación de usuarios (es decir, intentar identificar a una persona por sus datos de comportamiento) [75, 77, 107, 310]. Dantcheva et al. [53] proporcionan una visión general extensa de qué atributos sensibles, la llamada biometría suave (género, edad, etnia, peso, etc.), pueden inferirse a partir de la biometría primaria extraída de datos de imagen y vídeo. Ciriani et al. [48] realizaron una revisión sobre k-anonimidad, que puede utilizarse para proteger contra la identificación de biometría suave en datos tabulares. Laishram et al. [148] realizaron un estudio sobre los avances recientes en la construcción de sistemas de reconocimiento facial que preservan la privacidad. Además, algunas revisiones recientes se centran en las implicaciones para la privacidad de los grandes modelos de lenguaje (LLM) [54] y el aprendizaje automático generativo [94, 290].

Si bien la literatura actual sobre datos de comportamiento subraya la necesidad de defensas de privacidad, el trabajo en esta área es todavía emergente y disperso. Hasta ahora no se ha realizado una visión integral del problema, las soluciones existentes y los desafíos. Ribaric et al. [244] revisan técnicas para proteger los datos visuales y multimedia del usuario de inferencias de atributos y reidentificación. Aunque incluyen una sección sobre protección de datos de comportamiento, solo cubre un número limitado de rasgos (voz, marcha y gestos) y técnicas de anonimización que se aplican cuando estos datos se han capturado como vídeo, audio o imágenes. No se consideran otros sensores. También estrechamente relacionado, Nhat Tran et al. [279] examinan las técnicas de protección de plantillas biométricas, pero lo hacen de forma general sin entrar en detalles sobre las necesidades de anonimización de la biometría de comportamiento. Meden et al. [179] revisan las PET que se aplican a los rostros, observando diferentes aspectos como las garantías de privacidad que ofrecen y qué enfoques conceptuales se eligen. Shopon et al. [255] analizan una variedad más amplia de rasgos biométricos, incluyendo la marcha y el estilo de escritura. Su taxonomía se centra en si las anonimizaciones ocultan tanto la identidad como los atributos de la persona o retienen algunas características biométricas suaves.

Las revisiones actuales de la anonimización biométrica conductual consideran solo un rasgo específico o revisan solo unas pocas técnicas de anonimización. Lo que falta es una revisión que examine en profundidad un conjunto exhaustivo de tipos tradicionales y modernos de rasgos conductuales para los que se han propuesto soluciones, teniendo en cuenta diferentes tipos de sensores de recolección y casos de uso. Además, no se ha realizado una comparación de los enfoques de evaluación a través de las biometrías conductuales. Al comparar un gran conjunto de biometrías conductuales, las similitudes y diferencias entre los enfoques de anonimización se hacen evidentes y se pueden identificar preguntas de investigación abiertas. Para abordar estas deficiencias del trabajo relacionado, realizamos un estudio de las anonimizaciones para rasgos biométricos conductuales, comparamos las anonimizaciones entre rasgos y también comparamos sus evaluaciones de privacidad.

2.3 Metodología

Realizamos una revisión sistemática de la literatura siguiendo las directrices de Kitchenham [140] para identificar estudios relevantes sobre técnicas de privacidad para datos de comportamiento, como se muestra en la Figura 1.

Nuestra pregunta de investigación principal es: **¿qué técnicas son aplicables para proteger la privacidad de los datos de comportamiento?** Desde este punto de partida, el objetivo es comprender cómo funcionan estas técnicas, cuál es el nivel de protección proporcionado y cuáles son las limitaciones y los desafíos todavía por resolver. Para responder a estas preguntas, primero exploramos la literatura sobre biometría [5, 13, 53, 97, 164, 181, 220, 301] para determinar qué tipo de rasgos de comportamiento pueden utilizarse para identificar a una persona. La lista completa

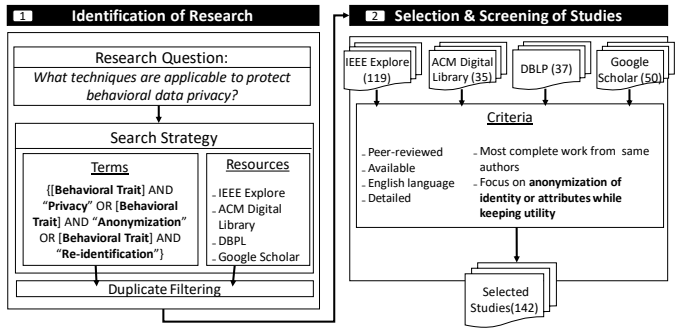


Fig. 1. Resumen del procedimiento para identificar y seleccionar estudios relevantes sobre técnicas de privacidad de datos de comportamiento. Primero analizamos la literatura sobre biometría para determinar los rasgos de comportamiento para la identificación de personas. Luego utilizamos estos rasgos como términos clave para buscar publicaciones relacionadas con la privacidad, siguiendo las directrices de Kitchenham para revisiones sistemáticas de la literatura [140]. La lista completa de rasgos de comportamiento que buscamos incluye: actividad cerebral, mirada, expresión facial, marcha, gestos, escritura a mano, háptica, ritmo cardíaco, pulsaciones de teclas, labios, movimiento, ratón, térmica, tacto y voz.

de rasgos de comportamiento que buscamos incluye: actividad cerebral (también referida como biometría cognitiva), mirada, expresión facial, marcha, gestos, escritura a mano, háptica, ritmo cardíaco, pulsaciones de teclas, labios, movimiento, ratón, térmica, tacto y voz. A continuación, utilizamos esta lista de rasgos combinada con la palabra clave **privacy** (privacidad) y los términos semánticamente similares **anonymization** (anonimización) y **de-identification** (deidentificación), como cadenas de búsqueda en las principales bases de datos académicas de informática. Basándonos en estos términos de búsqueda, recopilamos trabajos sin restricciones de fecha de publicación, obteniendo un conjunto de 364 artículos que abarcan desde 2007 hasta octubre de 2024, tras filtrar los duplicados. Durante la preselección, construimos una taxonomía de soluciones de privacidad y decidimos reducir el alcance del estudio a las técnicas de anonimización centradas en proteger la publicación de datos de comportamiento frente a ataques de divulgación de identidad y atributos. Consideramos enfoques que asumen la recopilación, higienización y posterior publicación de datos, los cuales deben ser anonimizados pero también mantener un nivel de utilidad para proporcionar servicios impulsados por datos de comportamiento. En consecuencia, la selección final de estudios primarios a analizar en este estudio consideró los siguientes criterios. Los documentos se excluyeron si:

(1) El formato de publicación era distinto a una revista académica revisada por pares o un artículo de conferencia.
(2) El artículo no pudo recuperarse utilizando IEEE Explore, ACM Digital Library, DBLP o Google Scholar.
(3) El idioma de publicación no era el inglés.
(4) Otro artículo de los mismos autores reemplazaba el trabajo, en cuyo caso se consideró el trabajo más completo.
(5) La técnica de protección de la privacidad era distinta a la anonimización de identidad o atributos con utilidad de datos.
(6) El enfoque de anonimización se describía a alto nivel y no se proporcionaban suficientes detalles para abordar adecuadamente nuestra pregunta de investigación principal.

El protocolo de búsqueda y selección arrojó un corpus final de 142 trabajos revisados por pares sobre anonimización de datos de comportamiento, que agrupamos según el rasgo de comportamiento protegido: marcha, actividad cerebral[2], ritmo cardíaco,mirada, voz y movimientos de la mano (escritura a mano, pulsaciones de teclas, movimientos del ratón y gestos de la mano). No encontramos artículos sobre expresión facial, labios, tacto y rasgos hápticos que cumplan con nuestros criterios.

3 Aplicaciones de datos de comportamiento y riesgos de privacidad

Los datos de comportamiento pueden aprovecharse para proporcionar servicios valiosos tanto para los usuarios como para las empresas. En esta sección, resumimos el modelo de aplicación, los usos principales de los datos de comportamiento y las cuestiones de privacidad emergentes relacionadas, que motivan la necesidad de nuestro estudio.

3.1 Datos biométricos conductuales

Los datos biométricos de comportamiento son una subclase de datos biométricos que abarca todo el comportamiento humano. Mientras que en SDC las columnas de un conjunto de microdatos que deben protegerse (p. ej., nombre o dirección) son explícitas, para la biometría de comportamiento no es evidente qué parte de los datos es sensible a la privacidad. Dado que los datos biométricos de comportamiento se capturan de un humano, contienen muchas dependencias implícitas entre puntos de datos individuales y entre rasgos. Por ejemplo, el movimiento de un pie es altamente dependiente del movimiento de la pierna correspondiente. Puede implicar inmediatamente que una persona se ha lesionado, ya que el comportamiento muestra patrones típicos de cojera, aunque este atributo no se haya hecho explícito en un campo del registro. Otra dependencia a considerar es la dependencia temporal entre puntos de datos, ya que la biometría de comportamiento generalmente se captura como una serie temporal de estados consecuentes. Estas dependencias hacen que la anonimización de los datos biométricos de comportamiento sea un desafío, ya que un atacante puede utilizarlas para reconstruir los datos originales y extraer información implícita de los datos anonimizados.

3.2 Escenario

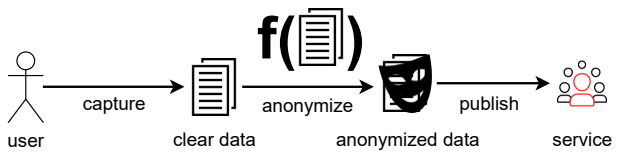


Fig. 2. Escenario de publicación de datos del estudio.

En este estudio, asumimos un escenario de publicación de datos (véase la Figura 2) en el que los datos se transforman primero de manera protectora de la privacidad y luego se publican, o son procesados por, o compartidos con un servicio o aplicación. Esto también incluye la publicación involuntaria, que por ejemplo puede ocurrir cuando se filtran las plantillas biométricas de un sistema de autenticación o se venden los datos de un rastreador de actividad física. Asumimos que la utilidad de los datos protegidos y modificados se preserva hasta el punto de que el servicio

[2]Las señales de ondas cerebrales son una manifestación tanto de su estructura fisiológica como de la forma conductual en que procesa la información, por ejemplo, en reacción a estímulos. En el contexto de este estudio, nos referimos a los EEG como datos de comportamiento, dado que este es nuestro principal foco de estudio, pero reconocemos que existen componentes fisiológicos presentes.

recibido (p. ej., una recomendación personalizada o un juego de realidad virtual jugado) sigue siendo significativo.

3.3 Aplicaciones

En general, todo el campo de la **interacción persona-ordenador** captura y procesa datos biométricos de comportamiento, ya que cada entrada a lo largo del tiempo también comprende un comportamiento. Los patrones de pulsación de teclas y el movimiento del ratón son nuestra principal modalidad de entrada para los sistemas informáticos hoy en día, sin embargo, nuevas modalidades de entrada como el tacto, la voz y los gestos están en auge y probablemente serán más relevantes en los próximos años. Importante a este respecto será la realidad mixta, ya que combina muchas de estas modalidades de entrada y requiere una monitorización constante de sus usuarios.

Otra área donde los datos de comportamiento son útiles es la **atención sanitaria** y el **yo cuantificado**. Los avances en sensores y técnicas de aprendizaje automático permitieron el desarrollo de aplicaciones para el reconocimiento de actividades, detección de caídas y monitorización remota de la salud que facilitan el cuidado de personas mayores, enfermas o discapacitadas y facilita el diagnóstico [59, 211, 225]. Los datos recopilados típicos son información de la marcha y el movimiento proveniente de acelerómetros y giroscopios integrados en dispositivos de usuario, y bioseñales como el ritmo cardíaco o la actividad cerebral. Estos datos también pueden procesarse para dar retroalimentación relacionada con la salud a los usuarios, por ejemplo, para guiarlos a través de la relajación o para detectar y señalar estados cognitivos, como estar estresado, para que el usuario pueda actuar en consecuencia.

Una de las áreas de aplicación más importantes y mejor investigadas de los datos de comportamiento es el **reconocimiento biométrico** [13, 114, 164, 181]. El comportamiento de una persona, como la forma de caminar o escribir en un teclado, contiene patrones inherentes únicos que permiten verificar la identidad de esa persona. Dado que estos patrones pueden detectarse implícitamente mientras la persona interactúa, usa o lleva un dispositivo, la biometría de comportamiento generalmente se considera más utilizable que otras biometrías tradicionales como las huellas dactilares[29, 30], y por lo tanto una buena alternativa o complemento a la autenticación basada en contraseñas. La investigación académica ha demostrado la viabilidad de numerosos rasgos de comportamiento para la autenticación de usuarios, por nombrar algunos: patrones de pulsación de teclas [271], marcha [288], tacto [272], movimiento del ratón [322], actividad cerebral [98], o incluso patrones de respiración [41, 42]. Y algunos de ellos ya están desarrollados en soluciones comerciales, especialmente en el sector financiero para prevenir el fraude mediante la detección de anomalías de comportamiento [22, 204, 281, 287].

Además del reconocimiento biométrico y la atención sanitaria, una gran cantidad de aplicaciones impulsadas por datos de comportamiento se centran en la **personalización**. En esta categoría, encontramos interfaces y servicios adaptativos que cambian su contenido o apariencia según las preferencias previstas del usuario basadas en su comportamiento. Además, la personalización se puede aplicar en muchas áreas. Para dar algunos ejemplos, los datos de comportamiento se utilizan para personalizar juegos en línea adaptándose al perfil del jugador para una experiencia más satisfactoria (p. ej., ajustando el nivel de dificultad) [326], en sistemas de recomendación para sugerir contenido en línea o anuncios [240], o en educación para adaptar la experiencia de aprendizaje al estado mental del estudiante (nivel de atención, estrés, etc.) [129].

3.4 Utilidad

Dependiendo de cada aplicación, los datos biométricos de comportamiento se utilizan para una variedad de propósitos. Por ejemplo, en una aplicación para autenticación biométrica, una medida evidente de utilidad es la capacidad de verificar la identidad de un individuo. Del mismo modo, en una

aplicación basada en la interacción persona-ordenador, podemos requerir que el comportamiento siga funcionando como una modalidad de entrada fiable para los sistemas informáticos. En una aplicación de atención sanitaria, podemos estar interesados en detectar patrones de comportamiento anormales, y monitorizar aspectos específicos del comportamiento como contar pasos o inferir las preferencias de un usuario para la personalización. La utilidad del servicio proporcionado puede evaluarse como el rendimiento en la realización de esas tareas.

3.5 Riesgos de privacidad

También existen implicaciones de privacidad preocupantes derivadas de la cantidad significativa de información personal recopilada implícitamente en aplicaciones impulsadas por datos de comportamiento. Como hemos visto, los datos de comportamiento pueden usarse como biometría porque son ricos en información individualizadora. La contrapartida es que cualquier entidad que recopile datos de comportamiento podría usarlos para identificar a las personas, incluso si ese no es el propósito principal del servicio que brindan. Lo que agrava este problema es que las personas pueden no ser conscientes de que están siendo medidas, ya sea por la falta de transparencia y marcos de consentimiento adecuados, o porque la vigilancia está destinada a ser encubierta. Pero además de la identidad, los datos de comportamiento conllevan una riqueza de información potencialmente sensible que también puede ser abusada. Por ejemplo, rasgos de comportamiento como nuestra voz, mirada, marcha o respuestas cerebrales, están correlacionados con diferentes enfermedades [59, 302], estados mentales y emociones [269, 299], y reacciones involuntarias específicas (como la dilatación de la pupila) pueden señalar nuestros intereses [146].

Técnicamente, el proceso general para inferir la identidad u otra información sobre un individuo a partir de sus datos de comportamiento sigue cuatro pasos, representados en la Figura 3. Primero, hay un paso de adquisición de datos en el que los datos de comportamiento se graban y digitalizan. Luego se extrae una representación de características que es adecuada para la inferencia posterior a partir de los datos brutos. Esta representación de características se reduce habitualmente para disminuir el número de dimensiones y reducir su complejidad. En el último paso, la representación reducida de características se utiliza para realizar la inferencia de la identidad o de atributos específicos. Así, se aplican técnicas de aprendizaje automático para clasificar los datos del usuario como pertenecientes a un perfil de usuario existente o no, o como pertenecientes a una clase de atributo específica (hombre, mujer). También se pueden aplicar modelos de regresión para asignar al individuo objetivo una medida (p. ej., grado de depresión en una escala continua). Basándose en este flujo de trabajo general, un servicio que utiliza un asistente personal controlado por voz podría aplicar el proceso para clasificar al usuario que ordena abrir una aplicación de correo electrónico como el propietario de la cuenta (autenticación). Pero también podría explotar las características de la voz para clasificar el estado de ánimo del usuario y ofrecerle anuncios altamente dirigidos, una práctica que puede conllevar discriminación y amenazar la autonomía del usuario.

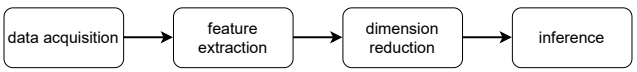


Fig. 3. Proceso general de inferencia basado en el comportamiento.

Si bien las grandes empresas ya recopilan una enorme cantidad de datos de comportamiento, la llegada de dispositivos vestibles de consumo asequibles con numerosos sensores (p. ej., dispositivos de RV/RA con seguimiento ocular, detección de postura de la cabeza y sensores de electroencefalografía (EEG)) exacerba el problema. Una vez recopilados los datos, incluso si es para una funcionalidad legítima y consentida por el usuario, como la detección de fraudes basada en

anomalías de comportamiento, estos datos pueden explotarse para conocer información privada. Por lo tanto, la necesidad de técnicas para proteger los datos de comportamiento es apremiante. Para establecer un mapa de la investigación actual sobre el tema, categorizamos y analizamos los enfoques de protección existentes para prevenir la revelación de identidad y atributos.

3.6 Modelo de atacante

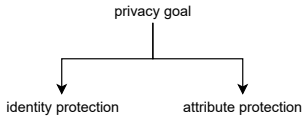
Nuestro adversario ha obtenido acceso a los datos biométricos de comportamiento de uno o varios usuarios y ahora desea inferir información privada sobre ellos. El adversario ha obtenido este acceso ya sea porque es el proveedor de servicios que los usuarios han utilizado, es un usuario del servicio y ha obtenido los datos (p. ej., imágenes faciales descargadas de redes sociales), o porque ha habido una filtración de los datos biométricos. Dado que el adversario tiene acceso completo a los datos biométricos de comportamiento, puede seleccionar libremente una técnica de inferencia para realizar inferencias de privacidad. Además, también podría tener acceso a conocimiento previo adicional sobre el usuario, como plantillas biométricas o biometría suave.

4 Una taxonomía de soluciones para la privacidad de los datos de comportamiento

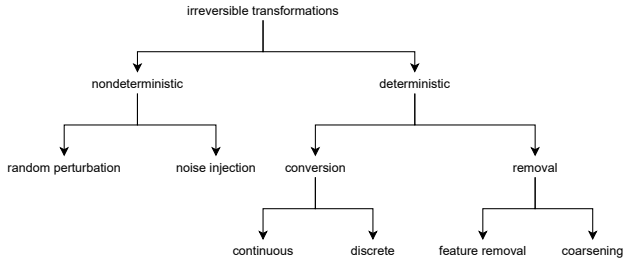
Basándonos en nuestro análisis de la literatura, identificamos dos **amenazas a la privacidad** principales que se aplican a los datos de comportamiento recopilados/procesados por un tercero y pueden explicarse en términos del modelo de atacante relacionado:

- **Revelación de identidad.** El objetivo del atacante es utilizar los datos de comportamiento para identificar al usuario. En esta amenaza, asumimos que el atacante es capaz de vincular los datos de comportamiento del objetivo con la identidad del objetivo y ahora quiere identificarlo en otro escenario. Por ejemplo, vinculando la cuenta de usuario y los datos en una aplicación relacionada con el trabajo a su cuenta en una aplicación de entretenimiento. Esta vinculación permitiría al atacante conocer más sobre la actividad del usuario. Un ejemplo de este tipo de atacante, como se presenta en [264], podría ser un usuario de visor de RV entrando en un Metaverso federado que ofrece varios servicios (p. ej., juegos, contenido para adultos, aplicaciones de formación profesional). Incluso si el usuario intenta usar un seudónimo al entrar en un servidor ajeno, el servidor y otros usuarios pueden usar los datos de comportamiento transmitidos (p. ej., movimientos del controlador/visor, seguimiento ocular) para identificar al usuario a través de diferentes seudónimos. Además, no es raro que los datos de comportamiento se vendan a terceros o se filtren involuntariamente a través de una brecha o ciberataque[3].
- **Revelación de atributos.** En esta amenaza, el objetivo del atacante no es reidentificar al usuario entre cuentas, sino derivar atributos sensibles incluidos dentro de los datos de comportamiento disponibles que el usuario no tenía la intención de revelar, como el sexo, condiciones médicas o intereses personales. El atacante podría haber tenido acceso previo o podría haber recopilado un conjunto de datos en el cual entrenar el modelo de aprendizaje automático para una inferencia dirigida. Por ejemplo, basándose en conjuntos de datos de electroencefalogramas disponibles públicamente de personas alcohólicas y no alcohólicas [133, 202], podría ser posible construir un clasificador que determine si los datos recién recopilados de una aplicación de entretenimiento que utiliza una interfaz cerebro-computador (BCI) pertenecían a un usuario con un problema de alcohol.

[3] https://www.zdnet.com/article/over-60-million-records-exposed-in-wearable-fitness-tracking-data-breach-via-unsecured-database/



(a) Taxonomía de técnicas de anonimización para la protección de datos de comportamiento según el objetivo de privacidad.



(b) Taxonomía de técnicas de anonimización para la protección de datos de comportamiento según el tipo de transformación de datos aplicada.

Fig. 4. Vistas generales de la taxonomía

A partir de las amenazas a la privacidad, podemos derivar los dos **objetivos de anonimización** con los que se pueden categorizar las técnicas, es decir, centradas en proteger la **identidad** del usuario y centradas en proteger **atributos** específicos, como se representa en la Figura 4a.

- **Protección de identidad**. El proceso de transformar los datos biométricos de comportamiento de una persona de tal manera que su identidad ya no pueda vincularse a los datos. La **seudonimización** reemplaza el identificador de una persona por uno nuevo y la **anonimización** impide la identificación por completo.
- **Protección de atributos**. El proceso de transformar los datos biométricos de comportamiento de una persona de tal manera que atributos privados específicos de la persona ya no puedan inferirse de los datos. Esto abarca tanto atributos de larga duración como la edad o el género y atributos de corta duración como el estado mental o condiciones de salud temporales. Una versión extrema de la protección de atributos es la protección de plantillas. Para la **protección de plantillas**, la verificación de identidad de la persona, en el contexto de un sistema de autenticación, debería ser todavía posible mientras todos los atributos están protegidos.

Basándonos en el estudio de los métodos de protección del estado del arte, hemos realizado una clasificación de métodos que, como es de esperar, no es totalmente exclusiva del campo de la privacidad de datos de comportamiento, ya que comparte similitudes con otras clasificaciones en campos de privacidad más maduros, como el SDC (Control de Revelación Estadística). En esta sección, profundizamos en esta clasificación y establecemos correspondencias con técnicas de anonimización ampliamente estudiadas en SDC.

Nuestra taxonomía de soluciones de anonimización para datos biométricos de comportamiento, que mostramos en la Figura 4b, se basa en el **tipo de transformación** aplicada a los datos originales, para derivar datos anonimizados y protegidos. Incluimos solo conceptos fundamentales, algunas de las técnicas de anonimización combinan múltiples de ellos. La característica básica y compartida de todos los métodos de anonimización es que tienen como objetivo proporcionar transformaciones irreversibles, es decir, es imposible transformar los datos de vuelta a los datos originales.

La primera distinción de nuestra taxonomía es si son técnicas deterministas o aleatorizadas. Los **métodos no deterministas** dependen de la aleatoriedad en su transformación, lo que puede producir resultados diferentes para la misma entrada, y los **métodos deterministas** siempre dan el mismo resultado para la idéntica entrada. Existen varios métodos bajo estos dos enfoques, como detallamos a continuación.

- **Métodos no deterministas.**
  - **Perturbaciones aleatorias.** Una transformación aleatoria a un dominio diferente.
  - **Inyección de ruido.** Métodos que añaden ruido aleatorio a los puntos de datos. Encontramos que el método correspondiente en la literatura de SDC se conoce como *enmascaramiento de ruido aditivo* [121], una técnica perturbativa que permite la publicación de un conjunto completo de microdatos, donde se publican los valores modificados en lugar de los valores exactos. Nos gustaría enfatizar que el enmascaramiento de ruido aditivo se combina típicamente en este campo con transformaciones deterministas, ya sean lineales o no lineales.
- **Los métodos deterministas** se dividen a su vez en **eliminación** y **conversión**. El método de eliminación suprime puntos de datos de los datos de tal manera que los puntos de datos no tienen influencia en el resultado anonimizado. Los métodos de conversión transforman los puntos de datos en una nueva representación, que típicamente depende del dominio original.
  - **La eliminación** puede realizarse de dos maneras: **coarsening** y **feature removal**. El *coarsening* (generalización) se refiere a eliminar partes de cada punto de datos o hacer los datos más dispersos. La eliminación de características se refiere a eliminar puntos de datos pertenecientes a una característica específica por completo. Esta técnica de eliminación se llama *supresión* [121] en el campo de SDC. Allí, cuando un conjunto de microdatos contiene muy pocos registros que comparten una combinación de valores cuasi-identificadores, se denomina una "combinación insegura" debido al riesgo de reidentificación potencial. Para abordar esta preocupación, se suprimen deliberadamente valores específicos de variables individuales, y efectivamente se reemplazan con valores perdidos. Esta estrategia de supresión tiene como objetivo ampliar el número de registros que se ajustan a cada combinación de valores clave, eliminando así las combinaciones inseguras y mejorando la protección de la privacidad.
  - **La conversión** puede ser **discreta** o **continua**, dependiendo de si el resultado de la conversión es un valor discreto o continuo. Como se mencionó anteriormente en la técnica de inyección de ruido, el SDC también emplea transformaciones de este tipo.

5 Técnicas de anonimización

Organizamos las técnicas examinadas según el rasgo biométrico de comportamiento que buscan proteger. Empezamos por la voz, ya que destaca como el rasgo más significativo basado en la literatura disponible, y luego pasamos a la marcha, los movimientos de la mano, el ritmo cardíaco,la mirada y la actividad cerebral. Para cada uno de los rasgos, analizamos su utilidad, el espacio de amenazas, las técnicas de anonimización y la metodología de evaluación.

5.1 Voz

El procesamiento y análisis de voz [35] se han realizado durante mucho tiempo y, por lo tanto, existe un amplio conjunto de terminología específica para describirlos. El sonido de la voz humana es creado por la laringe y luego viaja a través del tracto vocal, que transforma y filtra el sonido antes de que salga de la boca. Debido a su forma de tubo aproximada, el tracto vocal produce resonancias del sonido que dependen de la longitud del tracto vocal. Un fonema es la unidad de sonido más pequeña que distingue una palabra de otra y una proferencia (utterance) es una unidad de habla entre dos pausas claras. El espectro logarítmico es una representación importante del sonido, ya que se aproxima más a la percepción humana. Al utilizar una transformación de dominio (transformada rápida de Fourier (FFT) o coseno) en el espectro logarítmico, obtenemos el cepstrum (ver Figura 5). El cepstrum es útil porque permite estimar fácilmente la frecuencia fundamental

(f0) de la señal. La frecuencia fundamental percibida por los humanos se conoce como tono (pitch). Una escala ampliamente utilizada para transformar la frecuencia fundamental al tono es la escala Mel. Utilizando la escala Mel, el cepstrum se puede muestrear a frecuencias con la misma distancia percibida utilizando sumas ponderadas. Aplicando una FFT a esas sumas se obtienen los coeficientes cepstrales de frecuencia Mel (MFCC). Los MFCC son una cuantificación aproximada del espectro de la señal que se centra en la macroestructura de la señal.

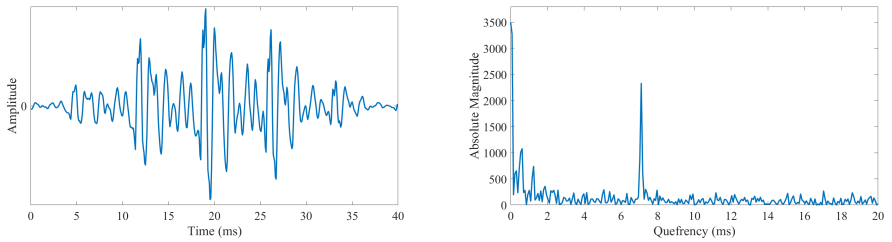


Fig. 5. Un segmento de habla en ventana (izquierda) y su correspondiente Cepstrum (derecha). Fuente: https://wiki.aalto.fi/display/ITSP/Cepstrum+and+MFCC.

A continuación se ofrece una breve descripción general del campo del reconocimiento de locutores (es decir, identificación) que tiene como objetivo establecer la identidad de un hablante. Los modelos de mezcla gaussiana [242] (GMM) representan a los locutores como la distribución de sus vectores de características. Los vectores de características se extraen del habla (la mayoría de las veces representados como MFCC) del locutor y luego se modelan como densidad de mezcla gaussiana. Un GMM asume que los puntos de datos son generados por un número finito de distribuciones gaussianas con parámetros desconocidos. Cada vector de características se representa como una combinación lineal de densidades gaussianas. Un modelo de fondo universal (UBM) es un GMM que modela una amplia variedad de locutores no objetivo, representando posibles impostores. Las medias del UBM se ajustan luego al locutor objetivo utilizando una adaptación maximum a posteriori [243] que resulta en un GMM para el locutor objetivo. El beneficio de este enfoque es que las gaussianas utilizadas para modelar al locutor objetivo son las mismas que en el UBM. Para la clasificación de un locutor, se compara la log-verosimilitud del GMM del locutor objetivo con la del UBM para determinar si el locutor debe ser aceptado. Una alternativa al enfoque de log-verosimilitud es obtener un GMM para cada grabación de locutor a través de una adaptación de probabilidad maximum a posteriori (MAP) del UBM y luego mapear estos GMM a un nuevo vector de características, llamado Supervector [36]. Los supervectores se pueden clasificar utilizando métodos tradicionales como máquinas de vectores de soporte (SVM). Una extensión de los supervectores es el enfoque de variabilidad total (TV) [64]. Esto asigna los supervectores a un espacio de baja dimensión que modela tanto al locutor como la variabilidad del canal. El vector resultante se llama i-vector y es el estado del arte de facto en la identificación de locutores. Una alternativa a los i-vectores son los x-vectores [259], que se extraen para cada proferencia a través de una red neuronal profunda (DNN).

5.1.1 Utilidad. El uso principal de las grabaciones de voz es la transmisión de información entre humanos; sin embargo, en los últimos años la voz también se ha convertido en una importante modalidad de entrada para los sistemas informáticos [230]. En ambos casos, es importante que el contenido del habla sea inteligible para los oyentes previstos. Pero también la mera detección del habla en muestras de audio puede ser útil, por ejemplo, para la detección de multitudes [49].

Además, las voces identifican de manera única a su hablante, haciéndolas adecuadas tanto para fines de autenticación como de reconocimiento [246].

5.1.2 Espacio de Amenazas. Las amenazas a la privacidad de las voces humanas van desde la identificación de individuos, pasando por la inferencia de atributos privados, hasta el robo de identidad a través de grabaciones falsas. La identificación de individuos a través de su voz ha sido evidente para los humanos durante mucho tiempo. Pero las voces transmiten más información que solo la identidad; también nos permiten inferir atributos como el género [78], o el estado emocional [299]. Además, los métodos modernos de síntesis de voz permiten la creación de grabaciones de voz falsas para un locutor objetivo, lo que permite el robo de identidad o la elusión de los sistemas de autenticación de locutores. A diferencia de otros rasgos biométricos de comportamiento, la voz y su habla resultante también pueden conllevar un significado semántico, que puede ser sensible para la privacidad.

5.1.3 Objetivo de Privacidad Adicional. La voz tiene el difuminado del habla como un objetivo de privacidad adicional, que apunta a destruir la inteligibilidad del habla para proteger su contenido semántico de oyentes no intencionados.

5.1.4 Técnicas de Anonimización. Ahora presentamos las técnicas de anonimización examinadas que tratan de proteger las voces humanas.

Perturbación Aleatoria. Parthasarathi et al. [213] extienden sus métodos de eliminación de características [212] barajando adicionalmente los bloques de voz para añadir aleatoriedad. Mtibaa et al. [192] proponen un esquema de protección de plantillas que se basa en barajar el vector de características de un sistema de identificación de locutores GMM-UBM.

Inyección de Ruido. Tamesue et al. [270] proponen un método muy simple para hacer que el habla sea ininteligible simplemente reproduciendo ruido rosa entre 180 y 5630 Hz con varios dB. Ma et al. [162] también intentan hacer que el habla sea ininteligible, pero se centran en las grabaciones de teléfonos inteligentes. Su dispositivo crea dos ondas de ultrasonido cuya interacción crea ondas aleatorias de baja frecuencia que generan ruido en el micrófono de un teléfono inteligente pero que los humanos no pueden oír. En su evaluación, encontraron que pueden bloquear las grabaciones de teléfonos inteligentes hasta 5 metros, dependiendo del tipo de teléfono inteligente. Hashimoto et al. [106] proponen un sistema para preservar la privacidad del locutor en espacios físicos. La idea central es agregar ruido blanco para evitar que las grabaciones de los locutores sean utilizadas para el robo de identidad. Concluyen que prevenir la identificación del locutor es posible (tasa de error igual (EER) del 2

Ohshio et al. [207] entrenan múltiples máscaras de balbuceo (babble maskers) a partir de locutores pregrabados segmentando el habla y luego promediando los segmentos. Cuando un locutor debe ser desidentificado, la máscara de balbuceo se selecciona en función de la frecuencia fundamental y el tono de la persona. Vaidya et al. [283] proponen añadir ruido aleatorio a cuatro características: tono, tempo, pausa y MFCC. Encontramos que las descripciones de su enfoque son bastante breves. Sharma et al. [253] utilizan un combinador de canales de autoatención para añadir ruido a las señales de voz.

Se han propuesto dos métodos que se basan en la privacidad diferencial para la inyección de ruido. Hamm et al. [102] proponen un filtro min-max diferencialmente privado. El filtro min-max minimiza el riesgo de privacidad mientras maximiza el riesgo de utilidad con una utilidad y tarea privada dadas. La privacidad diferencial se logra añadiendo ruido antes o después del filtro. Han et al. [103] se basan en X-vectores como representación del locutor y definen formalmente la indistinguibilidad de voz como una métrica de privacidad utilizando privacidad diferencial. Como medida de similitud

entre x-vectores, se utiliza la distancia angular y el esquema general proporciona un límite superior de esta distancia hasta el cual dos x-vectores no pueden distinguirse.

Supresión. Parthasarathi et al. [214] proponen tres métodos de eliminación de características para la detección de cambio de locutor consciente de la privacidad. El filtrado adaptativo asume que la fuente de excitación es independiente de la respuesta del tracto vocal. Realizan un análisis de predicción lineal a corto plazo para estimar un modelo de todos polos [154] (que representa el tracto vocal), un residuo (que representa la fuente de excitación) y la ganancia. Luego, el residuo se utiliza para estimar su cepstrum real. Su segundo método consiste en eliminar todas las subbandas excepto la de 1,5 kHz a 2,5 kHz y de 3,5 kHz a 4,5 kHz. Representan las dos subbandas como coeficientes MFCC y log-energía de un solo filtro. Su último método solo utiliza la pendiente espectral del locutor representada como coeficientes cepstrales. En otro trabajo [212], Parthasarathi et al. también proponen métodos similares de eliminación de características para la diarización de locutores utilizando el cepstrum real y MFCC como características. Su análisis encuentra que MFCC funciona mejor que el cepstrum real. Agarwal et al. [7] proponen un esquema similar. Primero transforman las señales de habla segmentadas al dominio de la frecuencia, luego seleccionan los n picos más importantes e interpolan una nueva señal antes de transformarla de nuevo al dominio del habla.

Wyatt et al. [295] proponen un método de eliminación de características para la segmentación de locutores y la detección de conversaciones. Dividen el audio en segmentos y guardan para cada uno el pico máximo de autocorrelación no inicial, el número total de picos de autocorrelación, la entropía espectral relativa y la energía del marco. Zhang et al. [320] utilizan las mismas características propuestas por Wyatt et al. excepto la energía del marco y luego utilizan un HMM para realizar la detección de conversaciones. Falta una evaluación de la privacidad en ambos trabajos.

Ditthapron et al. [69] han investigado cómo se puede eliminar el habla de locutores no objetivo en un escenario de evaluación del habla. Para separar a los locutores, primero extraen representaciones del locutor a partir de los MFCC del habla a través de un codificador. La representación del locutor se concatena luego con los MFCC originales antes de filtrar a todos menos a los locutores objetivo en la red de coincidencia de locutores. Echamos en falta una evaluación convincente de la privacidad.

Nelus et al. [200] proponen entrenar una DNN a través del aprendizaje adversario para extraer características de un locutor que permitan el reconocimiento de género pero no la identificación del locutor. Su evaluación muestra una caída en la identificación del 61

Conversión Discreta. Para la conversión discreta, encontramos múltiples esquemas de protección de plantillas.

Pathak et al. [216] presentan un algoritmo de hash para proteger los datos de voz con fines de autenticación. El supervector de un locutor se obtiene realizando la adaptación MAP de un modelo de fondo universal para cada proferencia del locutor y concatenando las medias del modelo adaptado. El hashing sensible a la localidad se realiza entonces con el supervector, lo que lo transforma en un espacio de baja dimensión, que se conoce como cubo (bucket). Esta operación es una aproximación del algoritmo de vecinos más cercanos que permite la comparación de cubos para autenticar al individuo.

Portelo et al. [228, 229] proponen un esquema de protección de plantillas basado en incrustaciones binarias seguras. Los autores utilizan un sistema de identificación de locutores que utiliza supervectores e i-vectores para representar las características de la voz de un locutor. Los vectores de características se codifican luego con incrustaciones binarias seguras que tienen la propiedad de que si la distancia euclidiana de los dos vectores está por debajo de un cierto umbral, entonces la distancia de Hamming de los hashes resultantes es proporcional a la distancia euclidiana. Esto

permite la comparación de los vectores codificados utilizando una máquina de vectores de soporte (SVM) con un núcleo basado en la distancia de Hamming.

Billeb et al. [27] proponen un esquema de protección de plantillas que se basa en el compromiso difuso (fuzzy commitment). Primero extraen el espectro de frecuencia a través de una FFT y luego extraen características del espectro de magnitud. Luego se aplica la adaptación MAP de un sistema de identificación de locutores GMM-UBM y se extraen estadísticas adicionales. La plantilla se almacena entonces como una combinación de código de corrección de errores y algoritmo de hash.

Conversión Continua. La mayoría de las técnicas de anonimización de voz caen en la categoría de conversión continua, ya que intentan crear una grabación de habla anonimizada. Hemos encontrado las siguientes técnicas.

La **transformación de locutor** es el proceso de manipular las características de voz de un locutor (no las características lingüísticas) para hacer que la voz suene como un locutor objetivo. Un locutor objetivo puede ser un locutor natural específico o un locutor sintético. Para el locutor sintético, se utiliza un locutor existente o se genera uno nuevo, por ejemplo, promediando múltiples locutores en uno. El enfoque general de la transformación de locutor es que las características de voz del locutor fuente se extraen y luego se transforman para que coincidan con el locutor objetivo. En el último paso, se sintetiza el nuevo locutor. Los siguientes métodos realizan la transformación de locutor.

Jin et al. [128] evalúan cuatro métodos para la transformación de locutor para la protección de la identidad. Su método base utiliza un sistema de transformación de locutor basado en mapeo GMM para transferir locutores a una voz sintética objetivo llamada kal-diphone. Además, prueban la transformación de duración en la que la longitud de las proferencias del locutor fuente se escala para que coincida con las del locutor objetivo.

5.2 Marcha

La marcha humana es el patrón en el que los humanos mueven sus extremidades durante la locomoción; existen múltiples formas de marcha, como trotar, caminar o correr. La marcha se puede dividir en ciclos de marcha individuales [267] (ver Figura 6)que es la tarea repetitiva más corta durante la marcha. El ciclo de marcha abarca desde un evento de marcha específico de un pie hasta que el mismo pie alcanza el mismo evento de marcha. Consta de una fase de apoyo, en la que el pie está en el suelo, y una fase de oscilación, en la que el pie está en el aire. Las dos fases se alternan para cada pie. Debido a su utilidad como rasgo biométrico de comportamiento para identificar a individuos, la marcha ha sido durante mucho tiempo un interés de investigación tanto de la informática como de la psicología. Por ejemplo, Yovel et al. [313] encuentran que juega un papel importante para que los humanos identifiquen a las personas a distancia, y Pollick et al. [226] muestran que es posible para los humanos inferir el género de un caminante, incluso cuando el caminante solo se muestra como un conjunto de puntos, como la llamada visualización de puntos de luz (point-light-display). La siguiente sección trata sobre la anonimización de los patrones de marcha.

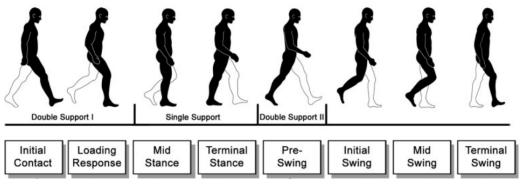


Fig. 6. Fases del ciclo de marcha. Fuente [267].

Los métodos de reconocimiento de la marcha han sido un tema de investigación activo en el pasado, por lo que existe un gran conjunto de métodos diferentes para varios métodos de captura. Wan et al. [288] realizaron un estudio reciente sobre el tema y enumeran métodos de reconocimiento para cámaras, acelerómetros, sensores de suelo y radares. La mayor parte de los trabajos se centran en el reconocimiento de la marcha basado en cámaras, que Wan et al. clasifican como basado en modelos o libre de modelos. Los métodos basados en modelos utilizan un modelo específico del caminante, por ejemplo, un modelo de péndulo de las piernas, para luego hacer coincidir al caminante con él. Los métodos libres de modelos, sin embargo, no tienen un modelo explícito, sino que utilizan la captura completa de la marcha para realizar el reconocimiento, por ejemplo, promediando la silueta del caminante a lo largo del tiempo como una imagen de energía de marcha. Los sistemas basados en acelerómetros también promedian la marcha en una representación de características, ya sea segmentando la marcha en sus ciclos de marcha o utilizando tramas con un tamaño fijo.

5.2.1 Utilidad. Las grabaciones de la marcha son importantes para el diagnóstico médico de anomalías de la marcha [139]. Otro ejemplo más casual sería la grabación del patrón de marcha para contar los pasos que una persona ha realizado durante un día [260]. Además, los patrones de marcha a menudo se graban en videos; para no degradar la calidad del video, la marcha debe parecer natural y convincente para sus espectadores [124].

5.2.2 Espacio de Amenazas. Debido a su omnipresencia en la vida cotidiana, la marcha humana es fácil de capturar, especialmente porque la mayoría de los métodos de captura no son intrusivos y no requieren la participación de la víctima. Además, se ha demostrado que el reconocimiento de la marcha es muy robusto a la calidad del video y a la ofuscación, lo que lo hace muy adecuado para sistemas de vigilancia [288]. Además de identificar a los humanos, también se ha demostrado que la marcha se puede utilizar para inferir atributos privados como el género [226]. Teniendo en cuenta todo esto, la amenaza para la biometría de la marcha ya es grande. Es más, con los recientes desarrollos en métodos de captura más ricos como LiDAR [86] o trajes de captura de movimiento baratos, es de esperar que el espacio de amenazas para la marcha aumente aún más en los próximos años.

5.2.3 Técnicas de Anonimización. A continuación, presentamos los métodos de anonimización de la marcha encontrados en la literatura, ordenados por nuestra taxonomía.

Perturbación Aleatoria. Hoang et al. [112] proponen un esquema de compromiso difuso basado en códigos Bose–Chaudhuri–Hocquenghem (BCH) para almacenar plantillas de marcha de acelerómetro. Después de la extracción de características y la binarización de los datos del acelerómetro, se extraen los bits fiables. Estos bits luego se someten a una operación XOR con la clave secreta codificada en BCH para obtener el seguro. Además del , se almacenan el hash de la clave secreta y algunos datos auxiliares. Durante la fase de autenticación, los bits fiables extraídos se someten a una operación XOR con el seguro y luego se decodifican con BCH. El resultado se puede hashear y comparar con el hash de la clave secreta. Si bien la tasa de falsos positivos (false accept rate) es prometedora, la tasa de falsos negativos (false reject rate) de este esquema debe mejorarse para ser más amigable con el usuario.

Inyección de Ruido. La influencia de la inyección de ruido en el rendimiento de los sistemas de autenticación de acelerómetro/giroscopio fue estudiada por Matovu et al. [174]. Para su enfoque, generan una serie temporal de valores de ruido extraídos de una distribución uniforme y luego fusionan la serie temporal original con la generada.

Un enfoque de inyección de ruido para la marcha en videos fue desarrollado por Tieu et al. [275]. Utilizan una red neuronal convolucional (CNN) para mezclar la marcha de una segunda persona (marcha de ruido) en la marcha original. En el primer paso, la silueta tanto de la marcha original como de la de ruido se extrae de una representación en blanco y negro de los videos de entrada. La marcha de ruido se selecciona aquí para que tenga el mismo tamaño y ángulo de visión que la marcha original para lograr un resultado más natural. Las siluetas se introducen luego en la CNN, que utiliza redes de pesos compartidos para abstraerlas y luego fusiona las representaciones abstraídas a través de una tercera red. En un paso de posprocesamiento, la marcha original se reemplaza por la marcha recién fusionada. Dependiendo del ángulo de visión, logran tasas de identificación entre el 20

Los autores mejoran aún más su método en un artículo de seguimiento [276]. Aquí, la marcha de ruido se genera a través de una red generativa antagónica (GAN) que toma ruido gaussiano como entrada y emite una silueta de ruido. En lugar de usar una CNN, luego usan una GAN de autopoda y crecimiento (SP-GAN) para fusionar el ruido y la marcha original. Aquí la precisión de identificación estuvo entre el 30

Generalización. Nair et al. [197] experimentan con el coarsening (generalización) de la velocidad de fotogramas, la precisión posicional y la dimensionalidad de los datos de movimiento de RV. Encuentran que, si bien estas técnicas pueden reducir las tasas de identificación para secuencias de movimiento individuales, no permiten una anonimización efectiva por sesión y, por lo tanto, no son efectivas para anonimizar datos de movimiento.

Supresión. Un enfoque de eliminación de características para el reconocimiento de actividades que preserva la privacidad a través de acelerómetros es propuesto por Jourdan et al. [130]. Extraen varias características temporales y de frecuencia de los datos del acelerómetro, como la media, la correlación, la energía o la entropía. A través de experimentos, luego determinan la influencia de cada característica para el reconocimiento de actividad e identidad. Encuentran que las características temporales contribuyen más al reconocimiento de identidad y las características de frecuencia más al reconocimiento de actividad, por lo tanto, eliminan las características temporales. Sus resultados muestran un buen compromiso entre el reconocimiento de actividad (96

5.3 Movimiento de Manos y Gestos

Usamos el término movimientos de la mano como un paraguas para todos los factores biométricos relacionados con el movimiento de la mano, incluyendo la escritura a mano, pulsaciones de teclas, movimientos del ratón y gestos manuales. Estos rasgos difieren principalmente en cómo se registran y qué tipo de movimientos de la mano se realizan. La escritura a mano puede capturarse offline (fuera de línea) u online (en línea), dependiendo de si se utiliza solo el texto escrito resultante o una captura en tiempo real de la mano mientras se escribe. Para este estudio, solo consideramos la singularidad de un estilo de escritura y no el estilo lingüístico (Estilometría) del texto escrito. En la vida moderna, la escritura a mano ha sido reemplazada en su mayoría por la escritura en teclados, que también es un factor biométrico importante ya que los individuos pueden ser identificados por los tiempos de sus pulsaciones de teclas. Además de los teclados, el uso de ratones de ordenador crea patrones únicos, ya que sus trayectorias y clics son nuevamente un factor biométrico. Por último, los movimientos de la mano pueden capturarse directamente utilizando técnicas de seguimiento óptico o acelerómetro.

El reconocimiento de movimientos de la mano abarca múltiples técnicas de reconocimiento para diferentes modalidades de captura; aquí damos una visión general de la escritura a mano, los movimientos del ratón, las pulsaciones de teclas y los gestos. Para el reconocimiento de movimientos de la mano basado en la escritura a mano, la secuencia de escritura de entrada a menudo se ajusta a

su línea base, se escala a un estilo de escritura normal y se segmenta para cumplir con las demandas del clasificador [222]. La escritura a mano depende además de si fue capturada mientras la persona escribía (escritura online), por ejemplo, con un bolígrafo digital, o si solo se captura la escritura en sí después de que la persona ha terminado (escritura offline). El reconocimiento de movimientos del ratón se basa en la trayectoria, la velocidad y los clics simples y dobles realizados con un ratón como características. El reconocimiento de movimientos de la mano basado en pulsaciones de teclas se basa principalmente en las diferencias de tiempo entre los eventos de tecla arriba (key up), abajo (key down) y mantener (hold). Además de los eventos individuales, las diferencias entre dos eventos sucesivos o incluso tres eventos sucesivos también se utilizan como características [325]. El reconocimiento de movimientos de la mano a través de gestos se puede dividir en gestos 2D que se realizan en una superficie plana (por ejemplo, en un teléfono inteligente) y gestos 3D que se realizan en el aire. Sherman et al. [254] utilizan las trayectorias de cada dedo y primero las remuestrean usando una interpolación de spline cúbica para obtener una tasa de muestreo más baja, eliminando la fluctuación no deseada. Para calcular la distancia entre dos gestos, se emplea la deformación temporal dinámica (dynamic time warping) con varias métricas de distancia.

5.3.1 Utilidad. El rango de utilidad para los movimientos de la mano es grande y diverso. Para la escritura a mano, el texto resultante debe ser legible tanto por humanos como por ordenadores, el estilo de escritura particular generalmente no es importante. Esto es diferente para las firmas, ya que su propósito principal es facilitar la identificación y verificación de la identidad del firmante, por lo tanto, su estilo particular es importante, mientras que la legibilidad del nombre es menos importante. Dado que los otros movimientos de la mano sirven principalmente como modalidades de entrada para sistemas informáticos, su utilidad como modalidad de entrada [318] debe mantenerse precisa y oportuna para mantener su utilidad. Para los gestos manuales [249], existe además su utilidad para la comunicación no verbal.

5.3.2 Espacio de Amenazas. El espacio de amenazas para el movimiento de la mano es diverso, ya que el uso de nuestras manos es inevitable en la mayoría de las tareas cotidianas y, como a menudo usamos dispositivos digitales, el registro de los movimientos de la mano ocurre la mayor parte del tiempo sin que nos demos cuenta. Como han demostrado muchos estudios, los movimientos de la mano se pueden usar para identificar a las personas por su escritura a mano [222], dinámica de pulsaciones de teclas [12], movimientos del ratón [241] y gestos [303]. Además de la identificación, nuestros movimientos de la mano también suelen transmitir significado, como cuando escribimos un texto en un teclado; la semántica de los movimientos de la mano también puede ser sensible, como cuando ingresamos contraseñas o escribimos mensajes privados. Condiciones médicas específicas se manifiestan en los movimientos de la mano, como los temblores de manos en pacientes con Parkinson [127]. Además, los movimientos de la mano transmiten información sobre nuestro estado emocional [263].

5.3.3 Técnicas de Anonimización. A continuación, presentamos los métodos adecuados para la anonimización de movimientos de la mano, con la excepción de los movimientos del ratón, ya que no encontramos ningún artículo adecuado para ello.

Perturbación Aleatoria. Maiorana et al. [166] proponen un método de protección de plantillas para la escritura a mano online que divide una secuencia de escritura a mano en segmentos y luego mezcla aleatoriamente los segmentos antes de convolucionarlos. El mismo enfoque de barajado es tomado por Maiti et al. [167] para prevenir ataques de inferencia de pulsaciones de teclas a través de acelerómetros llevados en la muñeca; sin embargo, no convolucionan los segmentos. El enfoque solo se evaluó con 4 participantes. Otro estudio que investiga la permutación de pulsaciones de teclas es realizado por Vassallo et al. [286]; en su evaluación solo investigan la reducción de la

utilidad. Goubaru et al. [96] proponen un esquema de protección de plantillas para plantillas de escritura a mano online. Extraen el ID de patrón para un usuario utilizando una plantilla común. El ID de patrón luego se somete a una operación XOR con un secreto que fue codificado por un código de corrección de errores. El resultado se almacena como la plantilla. Para la verificación, el ID de patrón se extrae nuevamente y luego se somete a una operación XOR con la plantilla.

Inyección de Ruido. Migdal et al. [187] añaden retrasos a los tiempos de pulsación de teclas. Shahid et al. [251] proponen utilizar el mecanismo de Laplace en las coordenadas 2D del texto manuscrito para lograr privacidad diferencial local.

Generalización. Vassallo et al. [286] exploran la supresión de pulsaciones de teclas para preservar el contenido del texto escrito en un escenario de autenticación continua. Maiti et al. [167] también se centran en la privacidad de las pulsaciones de teclas y proponen dos métodos de coarsening (generalización) para prevenir ataques de inferencia de pulsaciones de teclas a través de acelerómetros llevados en la muñeca. En su primer enfoque, simplemente detectan si un usuario está escribiendo a través de varias características y luego bloquean el acceso a los datos del acelerómetro para prevenir ataques. Su segundo método reduce la tasa de muestreo del acelerómetro.

Conversión Discreta. Para la conversión discreta encontramos las siguientes técnicas destinadas a la protección de plantillas. Un esquema de protección de plantillas de escritura a mano online es propuesto por Sae-Bae et al. [247] que descompone las firmas en histogramas sobre los cuales se realiza la autenticación. Utilizan histogramas unidimensionales para capturar la distribución de características individuales e histogramas bidimensionales para capturar la dependencia entre dos características. Migdal et al. [188] proponen un esquema de protección de plantillas para múltiples modalidades, incluidas las pulsaciones de teclas. Su esquema combina múltiples piezas de información, como direcciones IP, con la información de pulsación de teclas y luego calcula un biohash sobre ella. Leinonen et al. [150] investigan la anonimización de datos de tiempo de pulsación de teclas utilizando dos enfoques de redondeo que clasifican efectivamente los tiempos en cubos. Su enfoque parece ser efectivo ya que la identificación cae de cerca del 100Vassallo et al. [286] exploran la sustitución de teclas con una tecla cercana aleatoria para preservar el contenido del texto escrito en un escenario de autenticación continua.

Figueiredo et al. [84] han desarrollado un lenguaje de modelado que se puede utilizar para diseñar nuevos gestos para aplicaciones. Los gestos pueden reconocerse luego en el hardware de grabación, eliminando la necesidad de dar a la aplicación acceso a los datos en claro. No se realizó ninguna evaluación de privacidad. Para el reconocimiento de gestos respetuoso con la privacidad, Mukojima et al. [193] diseñaron un sistema que ilumina la mano con un patrón de píxeles aleatorio y captura la luz restante en el lado opuesto de la mano con un detector. A partir de esta recopilación de datos reducida, la forma de la mano se reconstruye mediante aprendizaje automático. Los autores no evaluaron la protección de la privacidad de su enfoque.

Conversión Continua. Maiorana et al. [166] proponen dos conversiones continuas para plantillas de escritura a mano online: una conversión de línea base que primero divide una secuencia de escritura a mano en múltiples segmentos basados en una clave secreta y luego convoluciona los segmentos. Y una transformación de desplazamiento que aplica un desplazamiento a la secuencia inicial. La coincidencia de plantillas se realiza sobre la plantilla protegida. Para la anonimización de gestos que han sido capturados a través de sensores de unidad de medición de inercia (IMU), Malekzadeh et al. [170] proponen dos autocodificadores separados. Se supone que el primer autocodificador reemplaza las secuencias en los datos que han sido clasificadas como sensibles con una secuencia neutral generada. Mientras que el segundo debería minimizar la información mutua entre los datos y la identidad del usuario. Su enfoque reduce la identificación del 96Fan et al. [80]

también proponen usar dos codificadores, usan uno para la codificación de tareas y uno para la codificación de identidad y luego alimentan ambas codificaciones en el decodificador. Este sistema se entrena en un enfoque adversario para reducir el reconocimiento de identidad y aumentar el reconocimiento de acciones utilizando un pequeño conjunto de datos sEMG.

Otro enfoque basado en autocodificadores es propuesto por Saunder et al. [249] en el que los movimientos del lenguaje de señas de una persona se transfieren a otra. Su técnica es doble: primero extraen la pose del video fuente y la codifican en un conjunto de características de pose. En segundo lugar, codifican el estilo de la apariencia objetivo utilizando una distribución de apariencia. La pose y el estilo codificados se combinan luego para generar una nueva imagen. No se evaluó si las personas pueden ser identificadas solo por sus movimientos de manos. Un segundo enfoque para realizar la anonimización del lenguaje de señas fue propuesto por Xia et al. [296]. Utilizan una estimación de las regiones de movimiento y luego usan flujo óptico en combinación con un mapa de confianza para codificar los movimientos del video fuente y del video conductor. Luego, el video anonimizado se genera a través de un autocodificador a partir del video fuente, el flujo óptico y el mapa de confianza. Para mantener alta la utilidad del lenguaje de señas, utilizan una función de pérdida que se centra especialmente en la diferencia entre el movimiento de la mano y la cara del video conductor y el anonimizado. Nuevamente, no se realizó ninguna evaluación de si las personas pueden ser identificadas por sus movimientos de manos.

5.3.4 Evaluación. La anonimización de los movimientos de la mano se evalúa principalmente en el contexto de la autenticación y, como tal, la tasa de falsos positivos (FPR), la tasa de falsos negativos (FNR) y la tasa de error igual (EER) son métricas importantes para evaluar el rendimiento. Pero también existe el uso de enfoques de reconocimiento para la evaluación que utiliza la precisión de la inferencia de identidad, edad, género y destreza manual. Un enfoque de evaluación único que encontramos fue utilizado por Goubaru et al. [96], quienes utilizaron la aleatoriedad de los bits de la plantilla a través de ocurrencias y autocorrelación para evaluar su enfoque. Nuevamente encontramos que son posibles enfoques de evaluación más críticos, ya que el EER probablemente sobreestimará el rendimiento de la anonimización ya que intenta lograr una tasa baja de falsos positivos.

5.4 Mirada

La mirada ocular implica dos tipos de movimientos: **fijaciones** y **sacadas**. Nuestros ojos alternan entre ellos durante tareas visuales, como la lectura (ver Figura 7). Las fijaciones se refieren al foco visual mantenido en un solo estímulo, mientras que las sacadas son movimientos oculares rápidos entre fijaciones para reorientar nuestra mirada. Además, incluso durante las fijaciones, nuestros ojos no están completamente quietos, sino que producen constantemente micro movimientos involuntarios (cientos por segundo) conocidos como microsacadas [4].

Las tecnologías de seguimiento ocular están cada vez más disponibles en el mercado de consumo y de investigación. El tipo más común de tecnología de seguimiento funciona iluminando el ojo con una matriz de fuentes de luz no visibles que generan un reflejo corneal. Estos reflejos se detectan y analizan para extraer la rotación ocular de los cambios en los reflejos. Existe una amplia gama de configuraciones de hardware para el seguimiento ocular, incluidas cámaras integradas en ordenadores, teléfonos inteligentes y visores de realidad virtual, hardware externo dedicado o gafas móviles (eye-wear). Estos sensores permiten extraer mediciones no solo con respecto a los datos de movimiento relacionados con las fijaciones y sacadas (velocidad, ángulo de la mirada, puntos de atención, ruta de escaneo), sino también características adicionales, como variaciones del tamaño de la pupila y comportamiento del parpadeo. Las combinaciones de estas características proporcionan información valiosa para implementar aplicaciones impulsadas por la mirada.

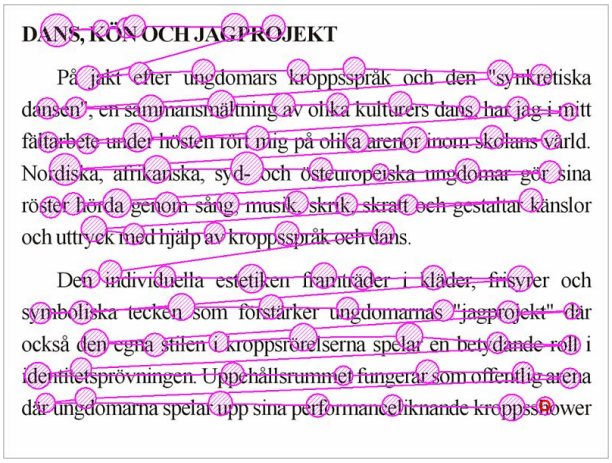


Fig. 7. Fijación y sacadas durante la lectura, de un estudio de lectura rápida realizado por Humanistlaboratoriet, Universidad de Lund, en 2005. Fuente:http://en.wikipedia.org/wiki/File:Rea.

5.4.1 Utilidad. Los movimientos oculares se han estudiado, analizado y utilizado durante más de un siglo en diferentes dominios de investigación. En el campo médico, la mirada proporciona información útil sobre nuestro procesamiento cognitivo y visual [16, 105], que se puede utilizar para diagnosticar diferentes enfermedades. En informática, la mirada se utiliza como una forma de interacción humano-computadora para mejorar la accesibilidad, la experiencia del usuario y para adaptar el comportamiento del sistema [50, 168, 227]. Más recientemente, los investigadores de seguridad y privacidad se han centrado en analizar características únicas estables del movimiento ocular para construir sistemas de autenticación biométrica [135]. La biometría ocular conductual ha sido objeto de una intensa investigación en la última década, mostrando EER tan bajos como 1.8

5.4.2 Espacio de Amenazas. Los datos de movimiento ocular son ricos en información que puede ser explotada por entidades maliciosas o proveedores de servicios curiosos para descubrir atributos sensibles del usuario más allá de los revelados intencionalmente y requeridos para el propósito del servicio o para identificar directamente a una persona. Además de la información biométrica que conllevan los datos de movimiento ocular, la investigación también ha documentado su correlación con múltiples trastornos y condiciones mentales, como Alzheimer [122], esquizofrenia [115, 151], Parkinson [147], trastorno bipolar [88], deterioro cognitivo leve [302], esclerosis múltiple [67], autismo [31, 289], o psicosis [79], por nombrar algunos. Además, se sabe que el tamaño de la pupila es un indicador del interés de una persona en una escena [108] y un indicador para detectar la carga cognitiva [145, 175]. Otros trabajos recientes demostraron que los datos oculares se pueden utilizar para inferir el género y la edad, o incluso rasgos de personalidad [24, 146]. Dada la riqueza de los datos oculares y la mayor disponibilidad de dispositivos de seguimiento de consumo y la llegada de aplicaciones impulsadas por la mirada, existe un potencial de amenaza a la privacidad significativo e inminente [6]. Las amenazas a la privacidad de las tecnologías de seguimiento ocular también han sido reconocidas por fabricantes de hardware como Apple, que prohíben el uso de información de seguimiento ocular para aplicaciones de terceros en su visor Vision Pro.

Las dos amenazas principales que ponen en peligro la privacidad ocular son la reidentificación y la inferencia de atributos.

5.4.3 Técnicas de Anonimización. Encontramos múltiples propuestas recientes para proteger la privacidad de los datos de movimiento ocular, muchas de ellas utilizando inyección de ruido para lograr privacidad diferencial (DP).

Perturbación Aleatoria. David-John et al. [55] adaptan el modelo marginal basado en tareas para la mirada, en el cual para cada dimensión del vector de características se construye una distribución de los valores para luego muestrear aleatoriamente nuevos datos sintéticos de estas distribuciones. La precisión de identificación de los datos sintéticos generados está cerca del nivel de azar.

Inyección de Ruido. Steil et al. [264] proponen una técnica basada en DP para proteger los datos de movimiento ocular recopilados mientras los usuarios leen diferentes tipos de documentos (cómic, periódico, libro de texto) en un entorno de RV. El objetivo de utilidad es predecir con precisión el tipo de documento para proporcionar funciones mejoradas en la aplicación de lectura. Además, los objetivos de privacidad son evitar inferencias de género a partir de los datos de movimiento ocular y proteger contra la reidentificación cuando el atacante tiene conocimiento previo de un conjunto de datos que incluye los datos oculares y la identidad del usuario objetivo. Para lograr estos objetivos, el mecanismo exponencial [74] se aplica a una base de datos de características oculares de los usuarios por un conservador de confianza antes de su publicación. Esta base de datos higienizada se puede utilizar luego para entrenar clasificadores para proporcionar la funcionalidad de lectura mejorada. Los experimentos que prueban varios niveles de ruido muestran que la utilidad con respecto a la clasificación de documentos se puede preservar en parte (55-70%) mientras se reduce la precisión de la inferencia de género al nivel de conjeturas aleatorias (50%).

Basándose en el conjunto de datos de Steil et al., Bozkir et al. [33] evalúan dos tipos de perturbaciones basadas en DP, el algoritmo de perturbación Laplaciana estándar (LPA) [73] y el algoritmo de perturbación de Fourier (FPA) [238]. También proponen una modificación del algoritmo FPA que divide los datos oculares en fragmentos antes de añadir ruido, con el fin de reducir las correlaciones temporales, que es una fuente de utilidad reducida ya que se requiere más ruido para proteger la privacidad. Con esta modificación, obtienen resultados de clasificación de tipo de documento similares a los utilizados por Steil et al. [264] para el caso del 50

Liu et al. [155] presentan una solución basada en DP para anonimizar datos de seguimiento ocular agregados como un mapa de calor. Un mapa de calor, o paisaje atencional, es un método popular para visualizar datos de movimiento ocular que representa fijaciones agregadas [72]. Esto significa que la intensidad de cada píxel se ajusta en relación con el número de fijaciones sobre esa región. El objetivo de privacidad en este caso es proteger los mapas de mirada individuales mientras se preserva la utilidad del mapa de calor agregado. Sus experimentos con selección aleatoria y ruido aditivo (Gaussiano, Laplaciano) muestran que el ruido Gaussiano es la mejor opción para obtener buenas garantías de privacidad para los mapas de mirada de los individuos sin distorsionar visualmente los puntos calientes en el mapa de calor agregado, es decir, manteniendo una cierta utilidad.

David-John et al. [57] trabajaron en la protección de datos de seguimiento ocular registrados en visores de RV/RA. Proponen dos modelos de interfaz diferentes para cómo se pueden compartir los datos con un tercero y proponen tres técnicas de anonimización: inyección de ruido Gaussiano, submuestreo temporal y submuestreo espacial para uno de los modelos de interfaz. Se descubrió que el enfoque de inyección de ruido era el más efectivo, ya que reducía al máximo la tasa de identificación de los sujetos con valores de varianza altos para la distribución Gaussiana. Wilson et al. [293] también propusieron añadir ruido Gaussiano a los datos de seguimiento ocular, mostrando resultados similares.

Hu et al. [118] propusieron un mecanismo local diferencialmente privado para generar trayectorias de movimiento ocular sintéticas llamado Otus. Su técnica primero separa el campo de visión

en teselas y luego construye un grafo que codifica la duración de la mirada de cada tesela y la probabilidad de transición entre las teselas. El grafo se perturba luego usando el mecanismo Laplaciano antes de ser enviado al servidor. El servidor luego promedia los grafos de todos los usuarios y usa caminatas aleatorias en el grafo para generar nuevas trayectorias de movimiento ocular.

Li et al. [152] propusieron Kaleido, un sistema plugin que permite anonimizar trayectorias de mirada con garantías de privacidad diferencial. Los autores extienden la geo-indistinguibilidad [14] y la privacidad de eventos w [136] para tener en cuenta el área de interés con radio r que un usuario está mirando. La intuición de su garantía es que todas las posiciones de la mirada dentro del área son indistinguibles. Señalan que solo protegen contra la información espacial y no la temporal. Además, definen un algoritmo adaptativo para asignar el presupuesto de privacidad de un usuario dependiendo del presupuesto de privacidad total de cada ventana de tiempo. Sus resultados muestran una reducción de la identificación de los usuarios a un nivel cercano al azar; sin embargo, la utilidad de los datos también está cerca del nivel de azar.

Generalización. Las técnicas de submuestreo temporal y espacial propuestas por David-John et al. [57] son ambas técnicas basadas en coarsening (generalización). Para el submuestreo temporal solo se puede registrar una reducción muy pequeña en la precisión de identificación, mientras que el submuestreo espacial tiene un efecto mayor pero debe escalarse muy alto para hacerlo. Wilson et al. [293] propusieron un enfoque de submuestreo espacial para el ángulo de la mirada. Primero mapean los 180° a 2160 puntos y luego generalizan (coarsen) el ángulo de la mirada a estos puntos. En su evaluación, el submuestreo espacial parece ser más efectivo que el submuestreo temporal.

Conversión Continua. Wilson et al. [293] proponen suavizar la mirada utilizando un enfoque de ventana deslizante. Muestran que usar una ventana lo suficientemente grande reduce la tasa de identificación.

David-John et al. [55] aplicaron k-anonimidad a los movimientos oculares agrupando las trayectorias de los usuarios y luego promediándolas. Pudieron demostrar que incluso con números pequeños de k la precisión de identificación cae significativamente. Debido a que procesan los vectores de características de cada tarea por separado, su alta utilidad reportada es cuestionable. En un artículo posterior, David-John et al. [56] proponen dos enfoques de generación de datos sintéticos para la mirada. Su enfoque k-same synth aplica k-anonimidad a los parámetros ajustados de un modelo de mezcla Gaussiana antes de usarlo para generar fijaciones y sacadas. Su enfoque event-synth-PD utiliza un autocodificador variacional condicional para generar nuevos datos con características dadas. Muestran que su enfoque event-synth-PD logra una negación plausible. Comparan ambos métodos con Kaleido y logran resultados comparables en privacidad y utilidad.

Fuhl et al. [85] realizan la anonimización de la mirada utilizando un autocodificador en combinación con aprendizaje por refuerzo. El autocodificador se entrena en las trayectorias de la mirada para aprender una representación latente de los datos. Luego, un agente de manipulación modifica el vector latente de las trayectorias para evitar, por ejemplo, la clasificación de género. Después de la decodificación del vector latente, un clasificador prueba qué tan buena fue la manipulación y su resultado se usa como pérdida para el entrenamiento del agente de manipulación.

5.4.4 Evaluación. Las propuestas de Steil et al. [264] y Bozkir et al. [33], miden la calidad de sus técnicas de anonimización para la protección contra inferencia de atributos utilizando la métrica de precisión de clasificación para la tarea principal y la tarea de inferencia de atributos. Para el caso de protección contra reidentificación, se asume que el atacante tiene conocimiento previo de una base de datos de datos oculares de los usuarios y sus identidades. Para simular este conocimiento, entrenan los clasificadores en los datos limpios y los prueban en los datos anonimizados, utilizando también la métrica de precisión para informar sobre la protección de la privacidad. Además, estos

trabajos también informan el llamado parámetro de pérdida de privacidad ε de la teoría de DP, que cuantifica la diferencia máxima entre los puntos de datos de dos individuos en el conjunto de datos.

Liu et al. [155] analizaron el compromiso privacidad-utilidad de los mapas de calor anonimizados utilizando el coeficiente de correlación (CC) y el error cuadrático medio (MSE) de los mapas de calor ruidosos bajo diferentes niveles de privacidad (diferentes valores de ε). El CC y el MSE dan una idea de la similitud entre los mapas de calor originales y los anonimizados, y la ε proporciona información sobre la garantía de privacidad (cuanto menor, mejor privacidad). Estas métricas van acompañadas de la representación visual del mapa de calor ruidoso, con el fin de ayudar a las partes interesadas relevantes a decidir qué nivel de ruido es aceptable para una aplicación dada.

Con respecto a los conjuntos de datos, el conjunto de datos más grande disponible es GazeBaseVR [159], que capturó a 407 participantes realizando 5 tareas con hasta 6 sesiones. Como dispositivo de grabación utilizaron un visor de RV. Steil et al. [264] recopilan datos de 20 participantes (10 hombres, 10 mujeres, de 21 a 45 años) mientras leen documentos usando un visor de RV. Cada grabación se divide en tres sesiones (leyendo un cómic, periódico o libro de texto), con una duración total de 30 minutos. Extraen 52 características de movimiento ocular relacionadas con fijaciones, sacadas, parpadeos y diámetro de la pupila. El conjunto de datos ha sido publicado públicamente[4] por los autores y Bozkir et al. [33] lo utilizan como base para evaluar su propuesta.

El conjunto de datos Ehtask [119] contiene las grabaciones de 30 personas realizando 4 tareas diferentes de mirada ocular usando un visor de RV. Otro conjunto de datos de visor de RV es DGaze [71], que captura a 43 personas en 5 escenas diferentes. En el estudio de anonimización de mapas de calor, Liu et al. utilizan un conjunto de datos simulado sintético para ilustrar su análisis de privacidad. Además del análisis técnico de privacidad, Steil et al. [264] es uno de los pocos trabajos que consideran las preocupaciones de privacidad de los usuarios con respecto a la recopilación de datos de comportamiento. Realizan una encuesta de usuarios a gran escala (con N=164 participantes) para explorar con quién, para qué servicios y en qué medida los usuarios están dispuestos a compartir sus datos de mirada. Su informe muestra que las personas se sienten incómodas con las inferencias (género, raza, orientación sexual) y se opondrían a compartir sus datos si estos atributos pueden filtrarse. Los resultados también muestran que las personas generalmente aceptan compartir sus datos de seguimiento ocular con una agencia gubernamental de salud o para fines de investigación, pero se opondrían a hacerlo si los propietarios de los datos son empresas. Estas ideas son un primer paso hacia la comprensión de la conciencia de privacidad del usuario y las necesidades de privacidad, pero se requiere más trabajo en este campo para guiar el diseño de técnicas de protección de la privacidad centradas en el usuario para los datos de comportamiento.

5.5 Ritmo Cardíaco

Un electrocardiograma (ECG) es un gráfico de voltaje a lo largo del tiempo que captura las actividades eléctricas de despolarización del músculo cardíaco seguidas de la repolarización durante cada latido. Como se muestra en la Figura 8, el gráfico ECG de un latido normal se compone de una secuencia de ondas: una onda P que refleja el proceso de despolarización auricular, un complejo QRS que representa el proceso de despolarización ventricular y una onda T que denota la repolarización ventricular. Otras partes de la señal ECG abarcan los intervalos PR, ST y QT [321].

Al igual que otros sistemas biométricos aplicados a tareas de identificación, los ECG generalmente se convierten en representaciones abstractas y comprimidas, generalmente denominadas plantillas biométricas, antes de que se lleve a cabo la tarea. Los métodos de plantilla biométrica se pueden clasificar según las características explotadas de los datos de ECG. Los más populares son los

[4]https://www.mpi-inf.mpg.de/departments/computer-vision-and-machine-learning/research/visual-privacy/privacy-aware-eye-tracking-using-differential-privacy

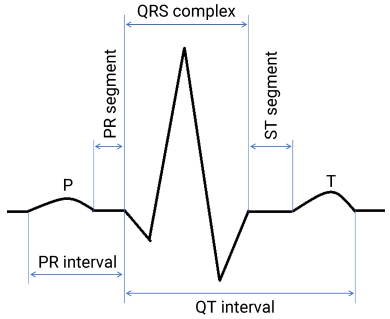


Fig. 8. Forma de onda de una señal ECG con ciclo cardíaco normal. Fuente: https://www.nottingham.ac.uk/nursing/practice/resources/cardiology/function/normal_duration.php.

métodos basados en fiduciarios, los no basados en fiduciarios y los métodos híbridos [206]. Por un lado, las técnicas basadas en fiduciarios utilizan puntos característicos en la señal ECG para extraer características temporales, de amplitud, envolvente, pendiente y área. Los puntos característicos son las ubicaciones que corresponden a los picos y límites de las ondas P, QRS y T de la señal ECG. Por otro lado, los métodos no basados en fiduciarios no dependen de los puntos característicos del ECG, y los ejemplos incluyen coeficientes de autocorrelación, transformadas de Fourier y wavelet. Los métodos híbridos combinan características tanto basadas en fiduciarios como no basadas en fiduciarios.

5.5.1 Utilidad. Los datos de ECG encuentran aplicación en sistemas de atención médica y biométricos, estos últimos destinados a la identificación y autenticación [282]. En la atención médica, los ECG se utilizan para el diagnóstico de enfermedades cardíacas [157]. Por lo general, existe un servicio independiente o un sistema completo de salud electrónica donde el proveedor de servicios, además de ofrecer un repositorio de datos médicos personales, puede permitir procesar dichos datos de forma remota. En cualquier caso, el objetivo es proporcionar información en tiempo real a pacientes y hospitales, ya sea como advertencia de una emergencia médica inminente o como ayuda de monitoreo durante los ejercicios físicos.

5.5.2 Espacio de Amenazas. Independientemente de la aplicación (es decir, identificación, autenticación o atención médica), los ECG son datos de salud y, como tales, las regulaciones de protección de datos los consideran sensibles y deben protegerse. Considere el caso, por ejemplo, de un usuario que podría ver aumentada su prima de seguro o sufrir discriminación durante una solicitud de empleo debido a una condición médica inferida de sus ECG.

Aunque es bien sabido que los datos de ECG pueden ayudar a diagnosticar la condición fisiológica o patológica de un paciente, otras inferencias probablemente menos conocidas incluyen el consumo de cocaína [117] y el estrés [223], que pueden ser sensibles para el paciente y obviamente deberían mantenerse en privado. El hecho de que los mismos datos de series temporales permitan extraer tanto inferencias deseables (es decir, para la atención médica) como inferencias sensibles (que deben protegerse) plantea un dilema de gran relevancia práctica.

5.5.3 Técnicas de Anonimización. A continuación, examinamos las técnicas de protección de la privacidad más relevantes para los datos de ECG.

Otro enfoque basado en la detección comprimida (CS) [38] es propuesto por Djelouat et al en [70]. CS es una técnica de procesamiento de señales que combina el muestreo y la compresión a través de proyecciones aleatorias. Basándose en esta técnica, los autores proponen comprimir la señal

ECG muestreándola en el momento de la detección. Esto reduce la necesidad de almacenar los datos confidenciales de ECG en el dispositivo portátil, proporcionando así protección contra esa entidad. Las propiedades teóricas de esta técnica de compresión aseguran que, bajo ciertas suposiciones sobre la proyección aleatoria, se puede obtener una buena reconstrucción de la señal ECG original en el lado del proveedor.

Supresión. Kalai et al. [315] presentan un esquema de protección de plantilla para datos de ECG. En una primera fase, los autores proponen calcular la transformada de coseno discreta (DCT) de los coeficientes de autocorrelación de la señal ECG y luego eliminar aquellos coeficientes DCT con la energía más baja. Los coeficientes DCT restantes constituyen la plantilla biométrica. En una segunda fase, se obtienen dos claves de la plantilla. Una se transmite a la aplicación de destino que el usuario desea autenticar. La otra funciona como una clave privada, que se deriva de la DCT completa ya almacenada en el servidor. Un enfoque similar es presentado por Zaghouani et al. [316] que utiliza un paso de cuantificación una vez que se obtiene la plantilla DCT. Este último enfoque se evalúa en el conjunto de datos PTB pero no se realiza una comparación experimental entre las dos soluciones propuestas.

Otra propuesta similar es realizada por Mahmoud et al. [165], que descompone la señal ECG en su transformada wavelet, elimina los coeficientes de baja frecuencia y reconstruye la señal ECG para su liberación. En el lado del proveedor, solo el personal autorizado con acceso a una clave secreta (derivada de la plantilla de transformada wavelet) puede reconstruir el ECG original a partir de la señal protegida liberada. Hasta qué punto estos datos liberados pueden salvaguardar la privacidad de los pacientes se evalúa a través de la diferencia cuadrática media porcentual (PRD), una medida de distorsión simple y ampliamente utilizada en aplicaciones de procesamiento de señales ECG [171] que cuantifica la diferencia entre el ECG original y su versión protegida.

Conversión Continua. Bennis et al. [23] propusieron un esquema simple de k-anonimidad para datos de ECG. En su primer paso, transforman la señal al dominio de la frecuencia. A continuación, eligen los k vecinos más cercanos de la señal y luego los agregan en una nueva señal antes de transformarla nuevamente al dominio del tiempo.

Piacentino et al. [221] utilizaron una GAN para generar datos de ECG sintéticos normalizando primero los datos y luego organizándolos en una matriz. Para la organización de los datos se realizan múltiples propuestas ordenando los valores de los datos por su tipo. No se realizó ninguna evaluación de la privacidad de los datos sintéticos. Jafarlou et al. [125] también proponen utilizar una GAN para generar muestras de datos de ECG anonimizadas. Su enfoque difiere del de Piacentino et al. en que utilizan la secuencia de ECG original como entrada para la GAN y utilizan la precisión de identificación como parte de la pérdida de entrenamiento para la GAN. Su evaluación muestra precisiones de identificación más bajas mientras que aún permite la detección de arritmias. Nolin-Lapalme et al. [203] también utilizan una GAN para la anonimización de ECG, pero apuntan a generar muestras de ECG neutrales en cuanto al sexo y utilizan la clasificación de sexo como parte de la pérdida de GAN.

Perturbación Aleatoria + Inyección de Ruido. Aunque el cifrado basado en la idea de CS puede lograr una noción computacional de secreto a través del paso de proyección aleatoria, se ha demostrado que esta técnica es vulnerable desde una perspectiva teórica de la información [237]. Para abordar este problema, Chou et al. [46] proponen utilizar el análisis de componentes principales y SVD en un esquema CS, donde los datos de ECG se cifran en el sensor portátil añadiendo ruido dependiente de la señal. Miden la privacidad como la información mutua entre la señal ECG original y su versión cifrada, y muestran que se puede lograr una alta precisión de clasificación mientras se proporciona privacidad más allá del secreto computacional.

Conversión Discreta + Inyección de Ruido. A diferencia de los trabajos examinados anteriormente, el objetivo de Zare-Mirakabad et al. [317] es publicar representaciones adecuadas de datos de ECG con ciertas garantías de privacidad. Para hacer esto, Zare-Mirakabad et al. proponen convertir series temporales de ECG en representaciones simbólicas a lo largo del tiempo. Utilizan la popular Aproximación Agregada Simbólica (SAX) para reemplazar valores numéricos continuos con cadenas de símbolos. Con esta nueva representación de símbolos, la técnica de anonimización propuesta primero construye un modelo de n-gramas a partir de la cadena de series temporales completa, y luego asegura que cada n-grama tenga una frecuencia mínima de aparición, similar al criterio de k-anonimidad. Para asegurar que esta versión de k-anonimidad se satisfaga sobre la cadena de símbolos, los autores contemplan añadir n-gramas falsos a la cadena original. Los resultados experimentales en el conjunto de datos Eamonn Discord muestran que (una medida de) la pérdida de información apenas se ve afectada para valores de k hasta 20.

Conversión Continua + Perturbación Aleatoria. Chen et al. [44] y el trabajo posterior de Wu et al. [294], abordan el problema de hacer revocables las plantillas biométricas basadas en ECG, exactamente como claves o contraseñas, una propiedad que consideran indispensable para que los ECG se utilicen en la práctica. Para permitir la revocabilidad de la plantilla, la práctica común es asociar distintas plantillas con la misma biometría perturbándolas de una manera diferente. Sin embargo, para proteger la privacidad del usuario, este proceso debe garantizar que la recuperación de la biometría original de su plantilla sea inviable o computacionalmente difícil.

Esencialmente, las plantillas cancelables se obtienen como proyecciones aleatorias de un bloque de datos de ECG de un usuario. Sin embargo, a diferencia de los enfoques comunes, Wu et al. no imponen restricciones a la matriz generadora. En consecuencia, la idea es que cada realización de esta matriz permite cancelar sus plantillas correspondientes. La reidentificación se lleva a cabo entonces con el algoritmo de clasificación de señales múltiples [26], reportando tasas de más del 95

Un enfoque distinto de Hong et al. [116], propone un sistema de identificación sin plantillas para prevenir cualquier problema de privacidad de plantillas comprometidas o robadas. El sistema convierte los datos de ECG en imágenes a través de varios métodos de correlaciones espaciales y temporales y utiliza técnicas de aprendizaje profundo para entrenar un clasificador. Los autores realizan experimentos en la base de datos Physikalisch-Technische Bundesanstalt e informan tasas de identificación de más del 90

Conversión Continua + Inyección de Ruido. Sufi et al. [268] proponen construir plantillas de las ondas P, QRS y T a través de correlaciones cruzadas de la señal ECG. Cada una de esas plantillas se ofusca luego de forma concatenada con ruido aditivo generado sintéticamente, de modo que la ofuscación de una onda sirve como entrada para ofuscar la siguiente onda. El resultado son formas ruidosas de las tres ondas y plantillas ruidosas de las mismas. Toda esta información constituye la clave disponible para el personal autorizado, que podrá reconstruir el ECG original a partir de la versión ruidosa (que es compartida o puesta a disposición pública por el propio paciente o usuario). El personal no autorizado, per contra, solo tendrá acceso a la señal ECG ruidosa, lo que, según los autores, puede prevenir la divulgación de identidad y atributos.

Huang et al. [120] proponen un sistema de autenticación que protege la privacidad de las plantillas de ECG en una base de datos con privacidad diferencial. Los autores asumen el entorno interactivo de esta noción de privacidad, donde un analista consulta la base de datos para obtener datos de ECG. Específicamente, se supone que el analista solicita los coeficientes de un polinomio de Legendre, que el sistema de anonimización utiliza para ajustar y comprimir la señal ECG. El ruido de Laplace se calibra a la sensibilidad de esos coeficientes y se añade a ellos, y la respuesta ruidosa se devuelve al analista. El parámetro ε de DP regula por lo tanto el compromiso entre la privacidad del usuario y la precisión de la autenticación, dependiendo este último aspecto de dos fuentes de error: la

aproximación del ajuste polinómico y el ruido inyectado. Los autores evalúan el sistema en las bases de datos MIT-BIH ECG y MIT-BIH Noise Strees, reportando una precisión de autenticación decente. Sin embargo, parecen malinterpretar cómo se calcula la sensibilidad de los coeficientes y, por lo tanto, sus resultados parecen haberse obtenido incorrectamente.

Saleheen et al. [248] investigan si se pueden extraer inferencias sensibles de segmentos de datos de series temporales por un adversario de red bayesiana dinámica. Se asume que el adversario estima una gama de estados de comportamiento sobre el usuario, incluyendo, por ejemplo, si está o no en una conversación, corriendo, fumando y estrés, en el momento en que se recopilan los datos. Cuando es probable que el adversario infiera aspectos sensibles de un usuario, los segmentos correspondientes de datos se sustituyen por datos no sensibles más plausibles. Para estimar la privacidad proporcionada por estas sustituciones de datos, los autores proponen una variación de la noción de privacidad diferencial que limita la información filtrada resultante de las sustituciones. En otras palabras, la métrica propuesta asegura que la información filtrada sobre una inferencia sensible de un segmento sustituido esté siempre limitada. La pérdida de utilidad se calcula, por otro lado, como la diferencia absoluta entre la probabilidad de inferencia sobre cada estado de comportamiento no sensible a partir de datos reales, y la misma probabilidad a partir de datos liberados. Aunque los resultados experimentales muestran valores relativamente pequeños de pérdida de utilidad para $\varepsilon \in [0.05, 0.65]$, la solución propuesta tiene dos limitaciones principales: primero, la protección se proporciona solo para adversarios de redes bayesianas dinámicas; y segundo, asume que todos los datos de series temporales están disponibles de antemano, lo que impide su aplicación en escenarios de tiempo real.

5.5.4 Evaluación. Las técnicas revisadas miden cómo se degrada la funcionalidad del servicio debido a la anonimización con métricas comunes de aprendizaje automático como precisión, recuperación y exactitud, y con menos frecuencia con las cantidades DTW y PRD, que evalúan la similitud entre las series temporales originales y protegidas. En cuanto a la privacidad, el nivel de protección se evalúa a través de una variedad de nociones y medidas, incluida la precisión de un ataque de inferencia de pertenencia, el parámetro ε de privacidad diferencial, la información mutua entre la señal ECG original y su versión cifrada, la probabilidad de inferencias correctas sobre atributos sensibles con y sin protección, y a través de una noción similar a la k-anonimidad. Un conjunto de datos común utilizado es la base de datos de arritmias del MIT-BIH [189], que contiene las muestras de ECG de 47 personas.

5.6 Actividad Cerebral

Las ondas cerebrales son patrones de impulsos eléctricos medibles emitidos como resultado de la interacción de miles de millones de neuronas dentro del cerebro humano. Desde que se registró el primer electroencefalograma humano en 1924 [100], tanto los dispositivos de hardware para medir la actividad cerebral como las técnicas de análisis para procesar estas señales han mejorado significativamente. Las tecnologías actuales para medir ondas cerebrales se pueden clasificar como métodos invasivos y no invasivos. Los métodos invasivos registran señales dentro de la corteza implantando directamente electrodos cerca de la superficie del cerebro [132]. Estos métodos son demasiado arriesgados para su uso en circunstancias no críticas y se utilizan únicamente en aplicaciones clínicas. En cambio, los métodos no invasivos se utilizan con mayor frecuencia y son aplicables a muchas áreas además del ámbito médico, como las interfaces controladas por el cerebro. La más portátil y comúnmente utilizada de estas técnicas es la electroencefalografía (EEG), que registra la actividad eléctrica a través de sensores colocados en la superficie del cuero cabelludo.

Una señal EEG es una combinación de diferentes ondas cerebrales que ocurren a diferentes frecuencias. Cada tipo de onda transporta diferentes tipos de información, que se pueden utilizar

para obtener conocimientos sobre el estado actual del cerebro [10]. Los investigadores han intentado identificar ciertos estados mentales asociados a cada onda cerebral.La Tabla 1 presenta un resumen de los tipos de ondas más importantes, sus frecuencias respectivas, su ubicación de origen en el cerebro y su estado mental asociado.

Las tecnologías de interfaz cerebro-computadora (BCI) funcionan principalmente en grabaciones continuas de datos EEG, es decir, datos de series temporales. Pero también hay muchas aplicaciones basadas en la extracción de variaciones cerebrales bloqueadas en el tiempo que aparecen en reacción a estímulos externos. Estas variaciones, llamadas potenciales relacionados con eventos (ERP), se utilizan ampliamente para detectar enfermedades neurológicas. En ambos casos, ya sea utilizando ERP o una serie EEG más larga, se calculan características para la aplicación impulsada por datos de ondas cerebrales construida sobre ella. Estas características pueden pertenecer al dominio del tiempo y/o frecuencia y a uno o múltiples canales. Ejemplos de características comúnmente utilizadas incluyen coeficientes autorregresivos, transformadas de Fourier y Wavelet.

Table 1. Descripción general de las ondas cerebrales EEG - basado en [10] y [2].

Tipo de onda	Frec. (Hz)	Ubicación de origen	Estado mental
Gamma γ	30-100	Corteza somatosensorial	Procesamiento activo de información, respuesta fuerte a estímulos visuales [2]
Beta β	13-30	Ambos hemisferios, lóbulo frontal	Mayor estado de alerta, pensamiento ansioso, atención focalizada
Alpha α	8-13	Regiones posteriores, ambos hemisferios; Ondas de gran amplitud	Reposo, ojos cerrados, sin atención [138]; Ritmo más dominante
Theta θ	4-8	Sin ubicación específica	Inactividad, soñar, imaginar, concentración tranquila, recuperación de memoria
Delta δ	0.5-4	Regiones frontales; Ondas de gran amplitud	Sueño profundo y sin sueños, inconsciencia

5.6.1 Utilidad. La utilidad que debe preservarse al procesar datos de ondas cerebrales depende en gran medida de la aplicación. Para aplicaciones clínicas, por ejemplo, la información bruta podría ser necesaria para un diagnóstico adecuado o una prótesis controlada por el cerebro segura. En estos casos, suelen existir regulaciones como la Regla de Privacidad de HIPAA [110] para proteger la información personal identificable. Al pasar a otros campos de aplicación menos regulados, la necesidad de datos EEG brutos completos no está necesariamente justificada. Las aplicaciones EEG más destacadas incluyen la autenticación de usuarios, la personalización de experiencias de juego y las interfaces controladas por el cerebro. En estos casos, la utilidad a preservar debe ser suficiente para proporcionar una aplicación útil, es decir, reconocer al usuario, y ofrecer opciones personalizadas e interfaces receptivas, todo con un error tolerable que no obstaculice la seguridad y usabilidad del servicio.

5.6.2 Espacio de Amenazas. La actividad cerebral es rica en información. Se puede utilizar para identificar de forma única a los individuos dadas sus características únicas y, de hecho, se han propuesto varios sistemas biométricos basados en ondas cerebrales [98]. Además, la adquisición de señales EEG plantea problemas de privacidad porque las ondas cerebrales se correlacionan, entre otros, con nuestros estados mentales, capacidades cognitivas y condiciones médicas [269]. Martinovic et al. [172] demostraron que al manipular las imágenes presentadas a los usuarios, sus

señales EEG podían revelar información privada, por ejemplo, tarjetas bancarias, números PIN, área de residencia o si el usuario conocía a una persona en particular.

5.6.3 Técnicas de Anonimización. Encontramos que un gran número de anonimizaciones se basan en métodos de aprendizaje automático para realizar la anonimización de los datos, con enfoques como redes generativas antagónicas (GAN) y esquemas de perturbación adversaria dominando el campo. Con la disponibilidad de conjuntos de datos EEG, la anonimización de datos de actividad cerebral está ganando algo de tracción.

Supresión. Matovu et al. [173] exploran cómo reducir la fuga de información privada de las plantillas de autenticación de usuarios EEG. Asumen un tipo de atacante interno, como un administrador de base de datos sin escrúpulos, que hace un mal uso de su privilegio para explotar maliciosamente las plantillas. El atacante quiere inferir, específicamente, si el usuario asociado con una plantilla es alcohólico. Su técnica de anonimización prevista tiene como objetivo ocultar la información sobre el alcoholismo mientras sigue proporcionando una buena precisión de autenticación. Es, por lo tanto, un mecanismo de protección de atributos. Conceptualmente, se basa en la hipótesis de que diferentes diseños de plantillas (características, canales, frecuencias) tendrán un impacto en la cantidad de información no de autenticación (emociones, condiciones de salud) que se puede inferir. Los autores demuestran esta hipótesis eligiendo dos plantillas diferentes y calculando la capacidad predictiva para autenticar a los usuarios y determinar su comportamiento de consumo de alcohol.

Conversión Continua. En la misma dirección de selección de características, Yao et al. [308] proponen el uso de redes generativas adversarias (GAN) [95] para filtrar información sensible de los datos EEG. Su objetivo es reducir la posibilidad de inferir alcoholismo mientras mantienen las grabaciones de actividad cerebral útiles para detectar tareas mentales, específicamente para predecir qué estímulo visual está mirando el usuario. El filtro propuesto basado en GAN implica redes neuronales profundas que realizan una transformación de dominio, es decir, traducir EEG de una distribución de dominio fuente X con características tanto deseadas como relacionadas con la privacidad a una distribución de dominio objetivo Y con características deseadas solamente. Sus resultados después de aplicar la técnica de filtrado muestran una reducción significativa en el porcentaje de secuencias EEG de usuarios alcohólicos que pueden clasificarse como tales (del 90,6

Pascual et al. [215] utilizan una GAN para generar datos EEG sintéticos para entrenar un sistema de monitoreo de epilepsia, ya que compartir grandes cantidades de EEG médicos es un problema de privacidad. Los autores se centran en señales EEG interictales (señales entre dos convulsiones) ya que son más fáciles de registrar que las convulsiones reales. Como generador se utiliza un autocodificador convolucional, pero en lugar de decodificar una interictal, el código latente se traduce en una muestra ictal. El discriminador compara entonces la ictal sintética con una real. Sus resultados muestran que los datos sintéticos alcanzan tasas de identificación cercanas al nivel de azar, incluso cuando solo hay dos pacientes en el conjunto de prueba. Sin embargo, esto es solo una seudonimización de los pacientes, ya que todos los valores ictales sintéticos generados para un paciente específico aún pueden vincularse entre sí.

Bethge et al. [25] propusieron codificadores de privacidad para eliminar la información sensible de cada uno de los flujos de datos de actividad cerebral antes de que se utilicen en una tarea de clasificación. Para cada conjunto de datos, se entrena una red neuronal convolucional como codificador utilizando la discrepancia media máxima (MMD) entre los diferentes conjuntos de datos codificados como función de pérdida. De esta manera, los codificadores deberían aprender una representación invariante del dominio de los datos. Prueban su enfoque en cuatro conjuntos de datos y encuentran que la clasificación de qué conjunto de datos originó una muestra cae del 99

Conversión Continua + Inyección de Ruido. Debie et al. [62] también utilizan una GAN para generar nuevos datos sintéticos a partir de los originales. Difieren de Yao et al. y Pascual et al. en que utilizan el descenso de gradiente estocástico diferencialmente privado en el discriminador de la red. Este método reduce la influencia de cada individuo en el cálculo de los gradientes. Evaluaron su GAN en el conjunto de datos Graz A con datos EEG de 9 sujetos. Sus resultados muestran que la utilidad de los datos sintéticos se conserva bien; sin embargo, no se realizó ninguna evaluación de privacidad adicional.

5.6.4 Evaluación. Los trabajos revisados, similares a las propuestas para anonimizar la marcha, evalúan la calidad de la protección contra inferencias comparando la precisión de la predicción para el atributo protegido antes y después de modificar los datos EEG. Las métricas utilizadas para este análisis son métricas típicas de aprendizaje automático, que incluyen precisión, tasas de falsos positivos y tasas de falsos negativos. De manera similar, la pérdida de utilidad se evalúa midiendo la reducción en la precisión de clasificación al usar los datos EEG originales y anonimizados.

Para sus evaluaciones, los trabajos utilizan una variedad de conjuntos de datos EEG diferentes. El conjunto de datos más grande es el corpus de datos EEG del Hospital Universitario de Temple [205] que contiene 579 sujetos, seguido por el conjunto de datos BCI2000 [250] con 106 sujetos. Específicamente registrado para autenticación fue el conjunto de datos de Arias et al. [15] que registró a 56 personas. Un conjunto de datos especial es el conjunto de datos médico SUNY con datos EEG de 25 sujetos alcohólicos y 25 sujetos de control mientras miraban estímulos visuales [133, 202]. Además, existen un par de conjuntos de datos más pequeños [113, 266, 291].

6 Discusión

Todos los rasgos biométricos de comportamiento revisados tienen en común que se capturan como una serie temporal que rastrea el cambio del rasgo a lo largo del tiempo. La mayoría de los rasgos, como la marcha, los movimientos de las manos, la voz y la mirada, son rasgos manifiestos que se pueden observar a distancia y no requieren la participación del sujeto. Estos rasgos a menudo se capturan como un subproducto de otras grabaciones, por ejemplo, grabaciones de video. Por otro lado, el EEG y el ECG son rasgos secretos que en su mayoría solo se pueden registrar conectando directamente sensores al sujeto para medirlos. Encontramos la mayor cantidad de métodos de anonimización para la voz y la menor cantidad para el EEG. Para los rasgos tacto, térmico y labio-facial no pudimos encontrar ningún mecanismo.

La **utilidad** de estos rasgos es muy diversa y es en su mayoría única para cada rasgo y la aplicación que lo utiliza. Varía desde utilidades como la naturalidad de un movimiento hasta la inteligibilidad de las proferencias.

Con respecto a su **espacio de amenazas**, los rasgos son similares entre sí, ya que debido a la omnipresencia de los dispositivos de captura digital se capturan más instancias de ellos. Los dispositivos vestibles (wearables) y móviles son de special interés ya que están conectados al sujeto y, por lo tanto, pueden permitir la captura continua de datos de comportamiento. Como ha demostrado nuestra revisión de la literatura, todos los rasgos se pueden utilizar tanto para la inferencia de identidad como de atributos, que luego se pueden utilizar indebidamente para una amplia variedad de amenazas a la privacidad, como la vigilancia, el robo de identidad o la inferencia de atributos privados. Los objetivos de privacidad, protección de la identidad y protección de atributos también son los mismos para todos los rasgos. Sin embargo, la voz tiene un objetivo de privacidad adicional en el que el contenido del discurso debe hacerse ininteligible.

Para las **técnicas** (ver Tabla 2 y Tabla 3) que revisamos, encontramos que la mayoría de ellas entran en la categoría de conversión continua, seguidas de eliminación de características e inyección de ruido. A continuación están la perturbación aleatoria y la conversión discreta, con la mayoría

Table 2. Una visión general de todos los métodos encontrados, clasificados por rasgo y método. Los artículos que proponen múltiples métodos pueden aparecer en varias filas. Los artículos que combinan varios métodos se marcan de la siguiente manera: * con inyección de ruido, † con perturbación aleatoria, ‡ con conversión discreta.

Rasgo / Method	Voz	Marcha	Mov. Mano	Mirada	Ritmo Cardíaco	Activ. Cerebral
Perturbación Aleatoria	[213] [192] [253]	[112]	[166] [96] [167] [286]	[55]	[46]*	
Inyección de Ruido	[270] [106] [102] [207] [283] [162] [103]	[275] [276] [174] [104] [182]	[187] [251]	[264] [155] [152] [57] [118] [293]		
Generalización		[197]	[167] [286]	[57][293]		
Supresión	[214] [212] [295] [320] [200] [49] [69] [199] [7]	[130] [89][104] [63][245]			[315] [316] [165]	[173] [308]
Conversión Discreta	[216] [228] [229] [27]		[247][150] [188][286] [84][193]		[317]*	
Conversión Continua	[128][224][261][131][3][233][17] [81][137][82][1][163][160] [262][99][11][312][231] [9][217][176][45][209][185][109] [304] [306][184][201][40][183] [314][161][305][186][185][218] [307][43][65][47][297][239][177] [91][232]†[256]†[252]*[39]†[142]* [143]*[235]*[234]* [262]*	[8] [124] [274] [101] [190] [195] [111]‡	[166] [170] [249] [296] [80]	[55] [85] [293] [56]	[23][221] [125] [203] [44]†[294]† [116]†[268]* [120]*[248]*	[215] [25] [180] [257][62]*

de los métodos de conversión discreta apuntando a la protección de plantillas. El coarsening (generalización) es la categoría con la menor cantidad de métodos. Observamos varias diferencias para las categorías de nuestra taxonomía; para los métodos de eliminación encontramos que la eliminación no es directamente reversible; sin embargo, debido a la alta redundancia en los datos biométricos de comportamiento, aún podría ser posible reconstruir los datos eliminados. Para los métodos de conversión, a menudo observamos que el espacio de parámetros para las anonimizaciones es a menudo bastante pequeño, lo que hace posible que un atacante pueda vincular datos en claro y anonimizados mediante fuerza bruta sobre los parámetros cuando se conoce la técnica de anonimización. En general, encontramos que la reversibilidad de las técnicas de conversión todavía tiene que evaluarse mejor. Para las técnicas de inyección de ruido encontramos que la fuerte dependencia tanto temporal como fisiológica es un problema ya que pueden usarse para filtrar el ruido.

Con respecto a las técnicas que proporcionan **privacidad diferencial**, hemos observado que ninguna de ellas puede utilizarse continuamente a lo largo del tiempo sin comprometer por completo la privacidad del usuario. La razón radica en que el presupuesto de privacidad es necesariamente finito, lo que significa, por la propiedad de composición secuencial de la privacidad diferencial [178],

Table 3. Visión general de los objetivos de privacidad que las diferentes técnicas intentan alcanzar.

Rasgo / Obj. Privacidad	Voz	Marcha	Mov. Mano	Mirada	Ritmo Cardíaco	Activ. Cerebral
Atributo	[192][102][162] [216][228][229] [27][233][82][11][39][47][109]	[112] [89] [104]	[166][96] [167][286] [247][188] [166]	[264] [33] [85]	[315][316] [165][44] [294][116] [268][120] [248]	[173] [308] [25] [62]
Identidad	[213][212][106][102][162][207] [283][103][214][295][320][200] [199][49][128][224][261][131] [3][233][17][81][176][231] [137][1][160][163][11][262] [9][312][217][99][142][143] [235][234][253][7][45][209] [185][109][304][306][184][201] [40][183][314][161][305][186] [185][218][307][43][65] [297][239][177][91][232][256] [252]	[174][275] [276][277] [130][89] [8][124] [274][111] [104][182] [197][63] [245][101] [190][195]	[187] [251][150] [84][193] [170][249] [296][80]	[55][264] [33][155] [57][118] [152][55] [85][293] [293] [293] [56]	[23][221] [46] [317] [125] [203]	[215] [62] [180] [257]

que se consumirá completamente en algún instante de tiempo. Sorprendentemente, esto parece estar en contradicción con el uso previsto de la mayoría de las aplicaciones donde se garantiza la privacidad diferencial, a saber, el monitoreo continuo en escenarios de atención médica, y los servicios de identificación y autenticación (que claramente no son servicios de un solo uso). A este respecto, el uso de nociones de privacidad relacionadas destinadas a observaciones continuas (por ejemplo, privacidad diferencial de eventos w [136]) puede ser útil. En general, se necesita más investigación sobre cómo aplicar eficazmente la privacidad diferencial a los datos de comportamiento.

Hicimos la observación de que la mayoría de los métodos no **manipulan el aspecto temporal** de sus datos. Excepciones notables son Hirose et al.[111] y Maiti et al.[167]. Dado que todos los rasgos resultan en datos de series temporales, manipular el orden temporal o las diferencias de tiempo entre eventos podría conducir a algunas técnicas generales de anonimización que funcionen para múltiples rasgos. Para la protección de atributos, encontramos que anonimizar atributos intrínsecos (por ejemplo, edad, sexo) es difícil ya que no está claro qué parte de los datos de comportamiento es relevante para estos atributos. Por lo tanto, encontramos que los enfoques de aprendizaje automático generativo son un enfoque prometedor para abordar este problema, ya que los modelos de aprendizaje automático pueden aprender las dependencias intrínsecas entre datos y atributos. Además, notamos una falta de incluso una comprensión básica de la **conciencia de privacidad de los usuarios** y las preocupaciones sobre la privacidad del comportamiento. Estas son necesarias para diseñar técnicas de protección que consideren las necesidades y requisitos del usuario.

Encontramos que la **metodología de evaluación** entre los rasgos y métodos es bastante similar. En general, se utiliza un sistema de inferencia/reconocimiento en los datos en claro y en los anonimizados y luego se informa la diferencia en precisión, a menudo sin reentrenar el sistema de inferencia en los datos anonimizados. Encontramos que esta metodología es demasiado simple ya que la suposición subyacente es que el atacante no es consciente de la anonimización. Una excepción notable son las técnicas de anonimización de voz más recientes, que ahora dependen principalmente

Table 4. Conjuntos de datos biométricos conductuales disponibles.

Nombre	Participantes	Publicado	Fuente	Rasgo
TIMIT	630	1993	[90]	Voz
Albayzin	164	1993	[191]	Voz
YOHO	137	1994	[37]	Voz
BioSecureID	400	2009	[83]	Voz
Billeb et al.	701	2014	[27]	Voz
Librispeech	1166	2015	[210]	Voz
RSR2015	300	2015	[149]	Voz
VCC 2016	10	2016	[278]	Voz
DAIC-WOZ	189	2016	[284]	Voz
VoxCeleb	1251	2018	[194]	Voz
CSTR VCTK Corpus	110	2019	[300]	Voz
AISHELL-3	218	2020	[309]	Voz
Kassel State of Fluency	37	2022	[20]	Voz
CASIA-B	124	2005	[323]	Marcha
BEHAVE	125	2010	[28]	Marcha
OU-ISIR	200	2012	[169]	Marcha
EPIC-Kitchens	32	2020	[52]	Marcha
IITMD-WFP	31	2021	[273]	Marcha
ETRI-activity 3D	100	2020	[126]	Movimiento
NTU60	40	2020	[156]	Movimiento
BOXRR-23	105852	2023	[196]	Movimiento
MCYT baseline corpus	330	2003	[208]	Mov. Mano
SVC2004	100	2004	[311]	Mov. Mano
GREYC	133	2009	[92]	Mov. Mano
MNIST	500	2012	[66]	Mov. Mano
Web-based keystroke	83	2012	[93]	Mov. Mano
SMILE	30	2018	[76]	Mov. Mano
ASLLRP	33	2022	[198]	Mov. Mano
DOVES	29	2009	[285]	Mirada
VR-Saliency	169	2018	[258]	Mirada
Gaze Prediction	43	2018	[298]	Mirada
Video viewing	50	2017	[158]	Mirada
MPIIDPEye	20	2019	[265]	Mirada
OpenEDS	157	2019	[87]	Mirada
EHTask	30	2022	[119]	Mirada
DGaze	22	2020	[71]	Mirada
GazeBaseVR	407	2023	[159]	Mirada
SUNY EEG database	50	1999	[202]	Activ. Cerebral
UCI EEG database	122	1999	[21]	Activ. Cerebral
BCI2000	106	2004	[250]	Activ. Cerebral
DEAP	32	2011	[141]	Activ. Cerebral
SEED	15	2015	[324]	Activ. Cerebral
DREAMER	23	2018	[134]	Activ. Cerebral
Temple University Hospital	579	2016	[205]	Activ. Cerebral
Arias et al.	56	2021	[15]	Activ. Cerebral
MIT-BIH ECG Arrhythmia	47	1979	[189]	Ritmo Cardíaco
Phys. Technische Bundesanstalt	290	1995	[32]	Ritmo Cardíaco

del marco de evaluación comparativa del Desafío VoicePrivacy para evaluar la privacidad y utilidad de sus técnicas. Esto demuestra que las iniciativas comunitarias pueden proporcionar una base común para la comparación y mejorar la metodología de evaluación general de un campo.

Solo un pequeño número de artículos comparan sus propios métodos con los de otros, y debido a las diferencias en los modelos de atacante y las fuentes de datos, son difíciles de comparar para los lectores. También encontramos que no hay muchos enfoques [236, 319] para formalizar la privacidad de los métodos de anonimización biométrica conductual, y la mayoría de las evaluaciones se basan en estimaciones empíricas de privacidad. Otro problema es que la metodología de evaluación está demasiado cerca de la metodología de evaluación del sistema de reconocimiento que busca inferir personas en un gran conjunto de datos con mala calidad de datos, mientras que un método de anonimización también debería funcionar en un tamaño de grupo pequeño con alta calidad de datos. Creemos que la falta de conjuntos de datos disponibles (ver Tabla 4) es uno de los principales problemas que frena a los rasgos biométricos de comportamiento menos investigados. Para un posible trabajo futuro, vemos la anonimización de los datos de mirada ocular y movimiento como áreas de investigación prometedoras, ya que quedan muchos desafíos, como lograr una buena utilidad y aplicabilidad en tiempo real. Al igual que el Desafío VoicePrivacy, la mayoría de los datos biométricos de comportamiento se beneficiarían de marcos de evaluación impulsados por la comunidad para aumentar la comparabilidad y el rigor de las evaluaciones de privacidad y utilidad. Un área donde se combinan muchos rasgos biométricos de comportamiento es la creación de gemelos digitales, donde es una pregunta abierta si anonimizar los rasgos de comportamiento independientemente unos de otros es suficiente para crear gemelos digitales respetuosos con la privacidad, por ejemplo, para la realidad mixta.

7 Conclusiones

Anonimizar los datos biométricos de comportamiento es una tarea importante para proteger la privacidad de las personas. En nuestra revisión de la literatura, encontramos muchos rasgos de comportamiento diferentes que deben tenerse en cuenta y desarrollamos una taxonomía para clasificar las técnicas de anonimización que se les pueden aplicar según el tipo de transformación de datos que realizan. Si bien la anonimización de voz ya es un campo de investigación establecido con muchos hallazgos, la mayoría de los rasgos biométricos de comportamiento han recibido poca atención. Su protección, por lo tanto, sigue siendo una pregunta de investigación abierta. Además, encontramos que la mayoría de las técnicas de anonimización solo se evalúan de forma rudimentaria asumiendo un atacante débil. Mejorar la metodología de evaluación es, por lo tanto, otra pregunta de investigación abierta. Por último, encontramos que el aspecto temporal de los datos fue mayormente descuidado: por un lado, solo existen pocos enfoques de anonimización para flujos de datos y, por otro, la mayoría de las técnicas de anonimización no perturban el aspecto temporal de sus datos.

Bibliografía

[1] Alberto Abad, Alfonso Ortega, António Teixeira, Carmen García Mateo, Carlos D. Martínez Hinarejos, Fernando Perdigão, Fernando Batista, and Nuno Mamede (Eds.). 2016. *Advances in Speech and Language Technologies for Iberian Languages*. Lecture Notes in Computer Science, Vol. 10077. Springer International Publishing. doi:10.1007/978-3-319-49169-1

[2] Mohammed Abo-Zahhad, Sabah Mohammed Ahmed, and Sherif Nagib Abbas. 2015. State-of-the-art methods and future perspectives for personal recognition based on electroencephalogram signals. *Biometrics* 4, 3 (Sept. 2015), 179–190. doi:10.1049/iet-bmt.2014.0040

[3] Mohamed Abou-Zleikha, Zheng-Hua Tan, Mads Graesboll Christensen, and Soren Holdt Jensen. 2015. A discriminative approach for speaker selection in speaker de-identification systems. In *European Signal Processing Conference*. IEEE, 2102–2106. doi:10.1109/eusipco.2015.7362755

[4] Richard A Abrams, David E Meyer, and Sylvan Kornblum. 1989. Speed and accuracy of saccadic eye movements: Characteristics of impulse variability in the oculomotor system. *J Exp Psychol Hum Percept Performf* 15, 3 (1989), 529. doi:10.1037/0096-1523.15.3.529

[5] Christopher Ackad, Andrew Clayphan, Roberto Martinez Maldonado, and Judy Kay. 2012. Seamless and continuous user identification for interactive tabletops using personal device handshaking and body tracking. In *Extended Abstracts on Human Factors in Computing Systems*. ACM, 1775–1780. doi:10.1145/2212776.2223708

[6] Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin, and Elissa M. Redmiles. 2018. Ethics Emerging: the Story of Privacy and Security Perceptions in Virtual Reality. In *Symposium on Usable Privacy and Security*. USENIX, Baltimore, MD, 427–442.

[7] Ayush Agarwal, Amitabh Swain, and S. R. Mahadeva Prasanna. 2022. Speaker Anonymization for Machines using Sinusoidal Model. In *2022 IEEE International Conference on Signal Processing and Communications (SPCOM)*. 1–5. doi:10.1109/SPCOM55316.2022.9840792

[8] Prachi Agrawal and P. J. Narayanan. 2011. Person De-Identification in Videos. *Trans. Circuits Syst. Video Technol.* 21, 3 (March 2011), 299–310. doi:10.1109/tcsvt.2011.2105551

[9] Hafiz Shehbaz Ali, Fakhar ul Hassan, Siddique Latif, Habib Ullah Manzoor, and Junaid Qadir. 2021. Privacy Enhanced Speech Emotion Communication using Deep Learning Aided Edge Computing. In *International Conference on Communications Workshops* (2021-06). IEEE, 1–5. doi:10.1109/ICCWorkshops50388.2021.9473669

[10] Abdulaziz Almehmadi and Khalil El-Khatib. 2013. The state of the art in electroencephalogram and access control. In *Conference on Communications and Information Technology (ICCIT)*. IEEE, Beirut, Lebanon, 49–54. doi:10.1109/iccitechnology.2013.6579521

[11] Ranya Aloufi, Hamed Haddadi, and David Boyle. 2020. Privacy-preserving Voice Analysis via Disentangled Representations. In *Conference on Cloud Computing Security Workshop* (2020-11-09). ACM, 1–14. doi:10.1145/3411495.3421355

[12] Arwa Alsultan and Kevin Warwick. 2013. Keystroke dynamics authentication: a survey of free-text methods. *International Journal of Computer Science Issues (IJCSI)* 10, 4 (2013), 1.

[13] Abdulaziz Alzubaidi and Jugal Kalita. 2016. Authentication of Smartphone Users Using Behavioral Biometrics. *Communications Surveys & Tutorials* 18, 3 (2016), 1998–2026. doi:10.1109/comst.2016.2537748

[14] Miguel E Andrés, Nicolás E Bordenabe, Konstantinos Chatzikokolakis, and Catuscia Palamidessi. 2013. Geo-indistinguishability: Differential privacy for location-based systems. In *ACM CCS*. 901–914.

[15] Patricia Arias-Cabarcos, Thilo Habrich, Karen Becker, Christian Becker, and Thorsten Strufe. 2021. Inexpensive brainwave authentication: new techniques and insights on user acceptance. In *30th USENIX Security Symposium (USENIX Security 21)*. 55–72.

[16] A.Terry Bahill, Michael R. Clark, and Lawrence Stark. 1975. The main sequence, a tool for studying human eye movements. *Math. Biosci.* 24, 3-4 (Jan. 1975), 191–204. doi:10.1016/0025-5564(75)90075-9

[17] Fahimeh Bahmaninezhad, Chunlei Zhang, and John Hansen. 2018. Convolutional Neural Network Based Speaker De-Identification. In *Speaker and Language Recognition Workshop*. ISCA, 255–260. doi:10.21437/odyssey.2018-36

[18] Dustin Bales, Pablo A. Tarazaga, Mary Kasarda, Dhruv Batra, A. G. Woolard, J. D. Poston, and V. V. N. S Malladi. 2016. Gender Classification of Walkers via Underfloor Accelerometer Measurements. *Internet of Things Journal* 3, 6 (Dec. 2016), 1259–1266. doi:10.1109/jiot.2016.2582723

[19] Salil Partha Banerjee and Damon Woodard. 2012. Biometric Authentication and Identification Using Keystroke Dynamics: A Survey. *Journal of Pattern Recognition Research* 7, 1 (2012), 116–139. doi:10.13176/11.427

[20] Sebastian Peter Bayerl, Alexander Wolff von Gudenberg, Florian Hönig, Elmar Noeth, and Korbinian Riedhammer. 2022. KSoF: The Kassel State of Fluency Dataset – A Therapy Centered Dataset of Stuttering. In *Proceedings of the Language Resources and Evaluation Conference*. European Language Resources Association, Marseille, France, 1780–1787.

[21] Henri Begleiter. 1999. EEG Database Data Set. https://archive.ics.uci.edu/ml/datasets/EEG+Database

[22] BehavioSec. [n. d.]. Continuous Authentication Through Behavioral Biometrics. Webpage. https://www.behaviosec.com Accessed: 17.05.2019.

[23] Zineb Bennis and Pierre-Antoine Gourraud. 2021. Application of a novel Anonymization Method for Electrocardiogram data. In *International Conference on Arab Women in Computing* (2021-08-25). ACM, 1–5. doi:10.1145/3485557.3485581

[24] Shlomo Berkovsky, Ronnie Taib, Irena Koprinska, Eileen Wang, Yucheng Zeng, Jingjie Li, and Sabina Kleitman. 2019. Detecting Personality Traits Using Eye-Tracking Data. In *Conference on Human Factors in Computing Systems CHI*. ACM, 1–12. doi:10.1145/3290605.3300451

[25] David Bethge, Philipp Hallgarten, Tobias Grosse-Puppendahl, Mohamed Kari, Ralf Mikut, Albrecht Schmidt, and Ozan Ozdenizci. 2022. Domain-Invariant Representation Learning from EEG with Private Encoders. In *International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (2022-05-23). IEEE, 1236–1240. doi:10.1109/ICASSP43922.2022.9747398

[26] G. Bienvenu and L. Kopp. 1980. Adaptivity to background noise spatial coherence for high resolution passive methods. In *ICASSP*, Vol. 5. 307–310. doi:10.1109/icassp.1980.1171029

[27] Stefan Billeb, Christian Rathgeb, Herbert Reininger, Klaus Kasper, and Christoph Busch. 2015. Biometric template protection for speaker recognition based on universal background models. *Biometrics* 4, 2 (June 2015), 116–126. doi:10.1049/iet-bmt.2014.0031

[28] Scott Blunsden and RB Fisher. 2010. The BEHAVE video dataset: ground truthed video for multi-person behavior classification. *Annals of the BMVA* 4, 1-12 (2010), 4.

[29] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2012. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes. In *Symposium on Security and Privacy*. IEEE, 553–567. doi:10.1109/sp.2012.44

[30] Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, and Frank Stajano. 2015. Passwords and the evolution of imperfect authentication. *Commun. ACM* 58, 7 (June 2015), 78–87. doi:10.1145/2699390

[31] Zillah Boraston and Sarah-Jayne Blakemore. 2007. The application of eye-tracking technology in the study of autism. *Physiol. J.* 581, 3 (June 2007), 893–898. doi:10.1113/jphysiol.2007.133587

[32] R Bousseljot, D Kreiseler, and A. Schnabel. 1995. Nutzung der EKG-Signaldatenbank CARDIODAT der PTB über das Internet. *Biomedizinische Technik* 40, 1 (1995).

[33] Efe Bozkir, Onur Günlü, Wolfgang Fuhl, Rafael F. Schaefer, and Enkelejda Kasneci. 2021. Differential privacy for eye tracking with temporal correlations. 16, 8 (2021), e0255979. doi:10.1371/journal.pone.0255979

[34] Attaullah Buriro, Zahid Akhtar, Bruno Crispo, and Filippo Del Frari. 2016. Age, Gender and Operating-Hand Estimation on Smart Mobile Devices. In *BIOSIG*. IEEE, 1–5. doi:10.1109/biosig.2016.7736910

[35] Tom Bäckström, Okko Räsänen, Abraham Zewoudie, and Pablo Pérez Zarazaga. [n. d.]. Introduction to Speech Processing. WebPage. https://wiki.aalto.fi/display/ITSP/ Accessed: 02.02.2021.

[36] W.M. Campbell, D.E Sturim, and D.A. Reynolds. 2006. Support vector machines using GMM supervectors for speaker verification. *IEEE Signal Process. Lett.* 13, 5 (May 2006), 308–311. doi:10.1109/lsp.2006.870086

[37] Campbell, Joseph and Higgins, Alan. 1994. YOHO Speaker Verification Corpus. *Linguistic Data Consortium* (Nov. 1994). doi:10.35111/3WC3-N668

[38] Emmanuel J. Candes, Justin Romberg, and Terence Tao. 2006. Robust uncertainty principles: exact signal reconstruction from highly incomplete frequency information. *Trans. Inf. Theory* 52, 2 (Feb. 2006), 489–509. doi:10.1109/tit.2005.862083

[39] Anne M. P. Canuto, Fernando Pintro, and Michael C. Fairhurst. 2014. An effective template protection method for face and voice cancellable identification. *International Journal of Hybrid Intelligent Systems* 11, 3 (2014), 157–166. doi:10.3233/HIS-140192

[40] Hyung-Pil Chang, In-Chul Yoo, Changhyeon Jeong, and Dongsuk Yook. 2022. Zero-Shot Unseen Speaker Anonymization via Voice Conversion. *IEEE Access* 10 (2022), 130190–130199. doi:10.1109/ACCESS.2022.3227963

[41] Jagmohan Chauhan, Yining Hu, Suranga Seneviratne, Archan Misra, Aruna Seneviratne, and Youngki Lee. 2017. BreathPrint: Breathing acoustics-based user authentication. In *Conference on Mobile Systems, Applications, and Services*. ACM, 278–291. doi:10.1145/3081333.3081355

[42] Jagmohan Chauhan, Suranga Seneviratne, Yining Hu, Archan Misra, Aruna Seneviratne, and Youngki Lee. 2018. Breathing-Based Authentication on Resource-Constrained IoT Devices using Recurrent Neural Networks. *Computer* 51, 5 (May 2018), 60–67. doi:10.1109/mc.2018.2381119

[43] Meng Chen, Li Lu, Junhao Wang, Jiadi Yu, Yingying Chen, Zhibo Wang, Zhongjie Ba, Feng Lin, and Kui Ren. 2023. VoiceCloak: Adversarial Example Enabled Voice De-Identification with Balanced Privacy and Utility. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 7, 2, Article 48 (June 2023), 21 pages. doi:10.1145/3596266

[44] Peng-Tzu Chen, Shun-Chi Wu, and Jui-Hsuan Hsieh. 2017. A cancelable biometric scheme based on multi-lead ECGs. In *Conference of Engineering in Medicine and Biology Society (EMBC)*. IEEE, 3497–3500. doi:10.1109/embc.2017.8037610

[45] Ming Cheng, Xingjian Diao, Shitong Cheng, and Wenjun Liu. 2024. Saic: Integration of speech anonymization and identity classification. In *AI for Health Equity and Fairness: Leveraging AI to Address Social Determinants of Health*. Springer, 295–306.

[46] Ching-Yao Chou, En-Jui Chang, Huai-Ting Li, and An-Yeu Wu. 2018. Low-Complexity Privacy-Preserving Compressive Analysis Using Subspace-Based Dictionary for ECG Telemonitoring System. *TBioCAS* 12, 4 (Aug. 2018), 801–811. doi:10.1109/tbcas.2018.2828031

[47] Oubaïda Chouchane, Michele Panariello, Chiara Galdi, Massimiliano Todisco, and Nicholas Evans. 2023. Fairness and Privacy in Voice Biometrics: A Study of Gender Influences Using wav2vec 2.0. In *2023 International Conference of the Biometrics Special Interest Group (BIOSIG)*. 1–7. doi:10.1109/BIOSIG58226.2023.10345975

[48] Valentina Ciriani, S De Capitani Di Vimercati, Sara Foresti, and Pierangela Samarati. 2008. k-anonymous data mining: A survey. *Privacy-Preserving Data Mining: Models and Algorithms* (2008), 105–136.

[49] Alice Cohen-Hadria, Mark Cartwright, Brian McFee, and Juan Pablo Bello. 2019. Voice Anonymization in Urban Sound Recordings. In *Workshop on Machine Learning for Signal Processing*. IEEE, 1–6. doi:10.1109/mlsp.2019.8918913

[50] Cristina Conati, Christina Merten, Saleema Amershi, and Kasia Muldner. 2007. Using eye-tracking data for high-level user modeling in adaptive interfaces. In *AAAI*. 1614–1617.

[51] Emiliano De Cristofaro. 2021. A Critical Overview of Privacy in Machine Learning. *IEEE Security & Privacy* 19, 4 (July 2021), 19–27. doi:10.1109/msec.2021.3076443

[52] Dima Damen, Hazel Doughty, Giovanni Maria Farinella, Sanja Fidler, Antonino Furnari, Evangelos Kazakos, Davide Moltisanti, Jonathan Munro, Toby Perrett, Will Price, and Michael Wray. 2020. The EPIC-KITCHENS Dataset: Collection, Challenges and Baselines. *IEEE TPAMI* (2020).

[53] Antitza Dantcheva, Petros Elia, and Arun Ross. 2016. What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. *IEEE TIFS* 11, 3 (March 2016), 441–467. doi:10.1109/tifs.2015.2480381

[54] Badhan Chandra Das, M. Hadi Amini, and Yanzhao Wu. 2025. Security and Privacy Challenges of Large Language Models: A Survey. *ACM Comput. Surv.* 57, 6, Article 152 (Feb. 2025), 39 pages. doi:10.1145/3712001

[55] Brendan David-John, Kevin Butler, and Eakta Jain. 2022. For Your Eyes Only: Privacy-preserving eye-tracking datasets. In *Symposium on Eye Tracking Research and Applications* (2022-06-08). ACM, 1–6. doi:10.1145/3517031.3529618

[56] Brendan David-John, Kevin Butler, and Eakta Jain. 2023. Privacy-preserving datasets of eye-tracking samples with applications in XR. *IEEE Transactions on Visualization and Computer Graphics* 29, 5 (2023), 2774–2784. doi:10.1109/TVCG.2023.3247048

[57] Brendan David-John, Diane Hosfelt, Kevin Butler, and Eakta Jain. 2021. A privacy-preserving approach to streaming eye-tracking data. 27, 5 (2021), 2555–2565. doi:10.1109/TVCG.2021.3067787

[58] Maria Cecilia Teixeira de Carvalho Bruno, Maria Aparecida Constantino Vilela, and Carlos Alberto B. Mendes de Oliveira. 2013. Study on dermatoses and their prevalence in groups of confirmed alcoholic individuals in comparison to a non-alcoholic group of individuals. *Anais Brasileiros de Dermatologia* 88, 3 (June 2013), 368–375. doi:10.1590/abd1806-4841.20131829

[59] Ana Lígia Silva de Lima, Luc J. W. Evers, Tim Hahn, Lauren Bataille, Jamie L. Hamilton, Max A. Little, Yasuyuki Okuma, Bastiaan R. Bloem, and Marjan J. Faber. 2017. Freezing of gait and fall detection in Parkinson’s disease using wearable sensors: a systematic review. *Journal of Neurology* 264, 8 (March 2017), 1642–1654. doi:10.1007/s00415-017-8424-0

[60] Wheidima Carneiro De Melo, Eric Granger, and Abdenour Hadid. 2019. Depression detection based on deep distribution learning. In *2019 IEEE international conference on image processing (ICIP)*. IEEE, 4544–4548.

[61] Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, and Vincent D. Blondel. 2013. Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports* 3, 1 (March 2013), 1376. doi:10.1038/srep01376

[62] Essam Debie, Nour Moustafa, and Monica T. Whitty. 2020. A Privacy-Preserving Generative Adversarial Network Method for Securing EEG Brain Signals. In *International Joint Conference on Neural Networks* (2020-07). IEEE, 1–8. doi:10.1109/IJCNN48605.2020.9206683

[63] Noëlie Debs, Théo Jourdan, Ali Moukadem, Antoine Boutet, and Carole Frindel. 2021. Motion sensor data anonymization by time-frequency filtering. In *2020 28th European Signal Processing Conference (EUSIPCO)*. 1707–1711. doi:10.23919/Eusipco47968.2020.9287683

[64] Najim Dehak, Patrick J Kenny, Réda Dehak, Pierre Dumouchel, and Pierre Ouellet. 2011. Front-End Factor Analysis for Speaker Verification. *Transactions on Audio, Speech, and Language Processing* 19, 4 (May 2011), 788–798. doi:10.1109/tasl.2010.2064307

[65] Jiangyi Deng, Fei Teng, Yanjiao Chen, Xiaofu Chen, Zhaohui Wang, and Wenyuan Xu. 2023. {V-Cloak}: Intelligibility-, Naturalness-& {Timbre-Preserving}{Real-Time} Voice Anonymization. In *32nd USENIX Security Symposium (USENIX Security 23)*. 5181–5198.

[66] Li Deng. 2012. The MNIST Database of Handwritten Digit Images for Machine Learning Research [Best of the Web]. *IEEE Signal Processing Magazine* 29, 6 (Nov. 2012), 141–142. doi:10.1109/msp.2012.2211477

[67] Joy Derwenskus, Janet C Rucker, Alessandro Serra, John S Stahl, Deborah L Downey, Nancy L Adams, and R John Leigh. 2005. Abnormal Eye Movements Predict Disability in MS: Two-Year Follow-Up. *Annals of the New York Academy of Sciences* 1039, 1 (April 2005), 521–523. doi:10.1196/annals.1325.058

[68] Clemens Deuser, Steffen Passmann, and Thorsten Strufe. 2020. Browsing Unicity: On the Limits of Anonymizing Web Tracking Data. In *Symposium on Security and Privacy*. IEEE, 279–292. doi:10.1109/sp40000.2020.00018

[69] Apiwat Ditthapron, Emmanuel O. Agu, and Adam C. Lammert. 2021. Privacy-Preserving Deep Speaker Separation for Smartphone-Based Passive Speech Assessment. 2 (2021), 304–313. doi:10.1109/OJEMB.2021.3063994

[70] Hamza Djelouat, Xiaojun Zhai, Mohamed Al Disi, Abbes Amira, and Faycal Bensaali. 2018. System-on-Chip Solution for Patients Biometric: A Compressive Sensing-Based Approach. *IEEE Sensors Journal* 18, 23 (Dec. 2018), 9629–9639. doi:10.1109/jsen.2018.2871411

[71] Isha Dua, Thrupthi Ann John, Riya Gupta, and CV Jawahar. 2020. DGAZE: Driver Gaze Mapping on Road. In *Conference on Intelligent Robots and Systems*.

[72] Andrew T. Duchowski. 2017. *Eye Tracking Methodology*. Springer International Publishing. doi:10.1007/978-3-319-57883-5

[73] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. 2017. Calibrating Noise to Sensitivity in Private Data Analysis. *Journal of Privacy and Confidentiality* 7, 3 (May 2017), 17–51. doi:10.29012/jpc.v7i3.405

[74] Cynthia Dwork and Aaron Roth. 2013. The Algorithmic Foundations of Differential Privacy. *Foundations and Trends® in Theoretical Computer Science* 9, 3-4 (2013), 211–407. doi:10.1561/0400000042

[75] Cynthia Dwork, Adam Smith, Thomas Steinke, and Jonathan Ullman. 2017. Exposed! A Survey of Attacks on Private Data. *Annual Review of Statistics and Its Application* 4, 1 (March 2017), 61–84. doi:10.1146/annurev-statistics-060116-054123

[76] Sarah Ebling, Necati Camgoz, Penny Braem, Katja Tissi, Sandra Sidler-Miserez, Stephanie Stoll, Simon Hadfield, Tobias Haug, Richard Bowden, Sandrine Tornay, Marzieh Razavi, and Mathew Magimai-Doss. 2018. SMILE Swiss German Sign Language Dataset. In *International Conference on Language Resources and Evaluation*.

[77] Khaled El Emam, Elizabeth Jonker, Luk Arbuckle, and Bradley Malin. 2011. A Systematic Review of Re-Identification Attacks on Health Data. *PLoS ONE* 6, 12 (Dec. 2011), e28071. doi:10.1371/journal.pone.0028071

[78] Fatih Ertam. 2019. An effective gender recognition approach using voice data via deeper LSTM networks. *Applied Acoustics* 156 (Dec. 2019), 351–358. doi:10.1016/j.apacoust.2019.07.033

[79] Ulrich Ettinger, Veena Kumari, Xavier A. Chitnis, Philip J. Corr, Trevor J. Crawford, Dominic G. Fannon, Séamus O'Ceallaigh, Alex L. Sumich, Victor C. Doku, and Tonmoy Sharma. 2004. Volumetric Neural Correlates of Antisaccade Eye Movements in First-Episode Psychosis. *American Journal of Psychiatry* 161, 10 (Oct. 2004), 1918–1921. doi:10.1176/ajp.161.10.1918

[80] Jiahao Fan and Xiaogang Hu. 2023. Privacy-Preserving Motor Intent Classification via Feature Disentanglement. In *2023 11th International IEEE/EMBS Conference on Neural Engineering (NER)*. 1–4. doi:10.1109/NER52421.2023.10123842

[81] Fuming Fang, Xin Wang, Junichi Yamagishi, Isao Echizen, Massimiliano Todisco, Nicholas Evans, and Jean-Francois Bonastre. 2019. Speaker Anonymization Using X-vector and Neural Waveform Models. In *Speech Synthesis Workshop*. doi:10.21437/ssw.2019-28

[82] Marcos Faundez-Zanuy, Enric Sesa-Nogueras, and Stefano Marinozzi. 2015. Speaker identification experiments under gender De-identification. In *Carnahan Conference on Security Technology*. IEEE, 1–6. doi:10.1109/ccst.2015.7389702

[83] J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano, G. Gonzalez de Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega, V. Cardeñoso-Payo, A. Viloria, C. E. Vivaracho, Q. I. Moro, J. J. Igarza, J. Sanchez, I. Hernaez, C. Orrite-Uruñuela, F. Martinez-Contreras, and J. J. Gracia-Roche. 2009. BiosecurID: a multimodal biometric database. *Pattern Analysis and Applications* 13, 2 (Feb. 2009), 235–246. doi:10.1007/s10044-009-0151-4

[84] Lucas Silva Figueiredo, Benjamin Livshits, David Molnar, and Margus Veanes. 2016. Prepose: Privacy, Security, and Reliability for Gesture-Based Programming. In *Symposium on Security and Privacy*. IEEE, 122–137. doi:10.1109/sp.2016.16

[85] Wolfgang Fuhl, Efe Bozkir, and Enkelejda Kasneci. 2021. Reinforcement learning for the privacy preservation and manipulation of eye tracking data. In *International Conference on Artificial Neural Networks*. Springer, 595–607.

[86] Bence Galai and Csaba Benedek. 2015. Feature selection for Lidar-based gait recognition. In *Workshop on Computational Intelligence for Multimedia Understanding*. IEEE, 1–5. doi:10.1109/iwcim.2015.7347076

[87] Stephan J. Garbin, Yiru Shen, Immo Schuetz, Robert Cavin, Gregory Hughes, and Sachin S. Talathi. 2019. *OpenEDS: Open Eye Dataset*. Technical Report 1905.03702. arXiv. doi:10.48550/ARXIV.1905.03702

[88] Ana García-Blanco, Ladislao Salmerón, Manuel Perea, and Lorenzo Livianos. 2014. Attentional biases toward emotional images in the different episodes of bipolar disorder: An eye-tracking study. *Psychiatry Research* 215, 3 (March 2014), 628–633. doi:10.1016/j.psychres.2013.12.039

[89] Giuseppe Garofalo, Tim Van hamme, Davy Preuveneers, and Wouter Joosen. 2020. A Siamese Adversarial Anonymizer for Data Minimization in Biometric Applications. In *European Symposium on Security and Privacy Workshops (EuroS&PW)* (2020-09). IEEE, 334–343. doi:10.1109/EuroSPW51379.2020.00052

[90] J. Garofolo, Lori Lamel, W. Fisher, Jonathan Fiscus, D. Pallett, N. Dahlgren, and V. Zue. 1992. TIMIT Acoustic-phonetic Continuous Speech Corpus. *Linguistic Data Consortium* (Nov. 1992).

[91] Ünal Ege Gaznepoglu and Nils Peters. 2023. Deep Learning-based F0 Synthesis for Speaker Anonymization. In *2023 31st European Signal Processing Conference (EUSIPCO)*. 291–295. doi:10.23919/EUSIPCO58844.2023.10290038

[92] Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. 2009. GREYC keystroke: A benchmark for keystroke dynamics biometric systems. In *Biometrics: Theory, Applications, and Systems*. IEEE, 1–6. doi:10.1109/btas.2009.5339051

[93] Romain Giot, Mohamad El-Abed, and Christophe Rosenberger. 2012. Web-Based Benchmark for Keystroke Dynamics Biometric Systems: A Statistical Analysis. In *Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 11–15. doi:10.1109/iih-msp.2012.10

[94] Abenezer Golda, Kidus Mekonen, Amit Pandey, Anushka Singh, Vikas Hassija, Vinay Chamola, and Biplab Sikdar. 2024. Privacy and Security Concerns in Generative AI: A Comprehensive Survey. *IEEE Access* 12 (2024), 48126–48144. doi:10.1109/ACCESS.2024.3381611

[95] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2020. Generative adversarial networks. *Commun. ACM* 63, 11 (Oct. 2020), 139–144. doi:10.1145/3422622

[96] Yuuki Goubaru, Yasushi Yamazaki, Takeru Miyazaki, and Tetsushi Ohki. 2014. A consideration on a common template-based biometric cryptosystem using on-line signatures. In *Global Conference on Consumer Electronics*. IEEE, 131–135. doi:10.1109/gcce.2014.7031229

[97] Erin Griffiths, Salah Assana, and Kamin Whitehouse. 2018. Privacy-preserving Image Processing with Binocular Thermal Cameras. *Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 4 (Jan. 2018), 1–25. doi:10.1145/3161198

[98] Qiong Gui, Maria V. Ruiz-Blondet, Sarah Laszlo, and Zhanpeng Jin. 2019. A Survey on Brain Biometrics. *Comput. Surveys* 51, 6 (Feb. 2019), 1–38. doi:10.1145/3230632

[99] Priyanka Gupta, Gauri P Prajapati, Shrishti Singh, Madhu R Kamble, and Hemant A Patil. 2020. Design of Voice Privacy System using Linear Prediction. (2020), 543–549.

[100] Lindsay F Haas. 2003. Hans Berger (1873-1941), Richard Caton (1842-1926), and electroencephalography. *J. Neurol. Neurosurg. Psychiatry* 74, 1 (Jan. 2003), 9–9. doi:10.1136/jnnp.74.1.9

[101] Agrya Halder, Pratik Chattopadhyay, and Sathish Kumar. 2023. Gait transformation network for gait de-identification with pose preservation. *Signal, Image and Video Processing* 17, 5 (2023), 1753–1761.

[102] Jihun Hamm. 2017. Enhancing utility and privacy with noisy minimax filters. In *ICASSP*. IEEE, 6389–6393. doi:10.1109/icassp.2017.7953386

[103] Yaowei Han, Sheng Li, Yang Cao, Qiang Ma, and Masatoshi Yoshikawa. 2020. Voice-Indistinguishability: Protecting Voiceprint In Privacy-Preserving Speech Data Release. In *Conference on Multimedia and Expo (ICME)* (2020-07). IEEE, 1–6. doi:10.1109/ICME46284.2020.9102875

[104] Simon Hanisch, Evelyn Muschter, Admantini Hatzipanayioti, Shu-Chen Li, and Thorsten Strufe. 2023. Understanding Person Identification Through Gait. *Proceedings on Privacy Enhancing Technologies* 1 (2023), 177–189.

[105] Katarzyna Harezlak and Pawel Kasprowski. 2018. Application of eye tracking in medicine: A survey, research issues and challenges. *Computerized Medical Imaging and Graphics* 65 (April 2018), 176–190. doi:10.1016/j.compmedimag.2017.04.006

[106] Kei Hashimoto, Junichi Yamagishi, and Isao Echizen. 2016. Privacy-preserving sound to degrade automatic speaker verification performance. In *International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 5500–5504. doi:10.1109/icassp.2016.7472729

[107] Jane Henriksen-Bulmer and Sheridan Jeary. 2016. Re-identification attacks—A systematic literature review. *International Journal of Information Management* 36, 6 (Dec. 2016), 1184–1192. doi:10.1016/j.ijinfomgt.2016.08.002

[108] Eckhard H Hess and James M Polt. 1960. Pupil Size as Related to Interest Value of Visual Stimuli. *Science* 132, 3423 (Aug. 1960), 349–350. doi:10.1126/science.132.3423.349

[109] Jan Hintz, Sebastian Bayerl, Yamini Sinha, Suhita Ghosh, Martha Schubert, Sebastian Stober, Korbinian Riedhammer, and Ingo Siegert. 2023. Anonymization of Stuttered Speech – Removing Speaker Information while Preserving the Utterance. In *3rd Symposium on Security and Privacy in Speech Communication*. 41–45. doi:10.21437/SPSC.2023-7

[110] HIPAA Compliance Assistance. 2003. Summary of the hipaa privacy rule. Office for Civil Rights. Publication of the US Dept. of Health and Human Services.

[111] Yuki Hirose, Kazuaki Nakamura, Naoko Nitta, and Noboru Babaguchi. 2019. Anonymization of Gait Silhouette Video by Perturbing Its Phase and Shape Components. In *Asia-Pacific Signal and Information Processing Association Annual Summit*. IEEE, 1679–1685. doi:10.1109/apsipaasc47483.2019.9023196

[112] Thang Hoang, Deokjai Choi, and Thuc Nguyen. 2015. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme. *International Journal of Information Security* 14, 6 (Jan. 2015), 549–560. doi:10.1007/s10207-015-0273-1

[113] Ulrich Hoffmann, Jean-Marc Vesin, Touradj Ebrahimi, and Karin Diserens. 2008. An efficient P300-based brain–computer interface for disabled subjects. *Journal of Neuroscience Methods* 167, 1 (2008), 115–125. doi:10.1016/j.jneumeth.2007.03.005 Brain-Computer Interfaces (BCIs).

[114] Giles Hogben. 2010. ENISA Briefing: Behavioural Biometrics. *Computational Intelligence* (2010).

[115] Philip S Holzman, Leonard R Proctor, and Dominic W Hughes. 1973. Eye-Tracking Patterns in Schizophrenia. *Science* 181, 4095 (July 1973), 179–181. doi:10.1126/science.181.4095.179

[116] Pei-Lun Hong, Jyun-Ya Hsiao, Chi-Hsun Chung, Yao-Min Feng, and Shun-Chi Wu. 2019. ECG Biometric Recognition: Template-Free Approaches Based on Deep Learning. In *Annual International Conference of Engineering in Medicine and Biology Society (EMBC)*. IEEE, 2633–2636. doi:10.1109/embc.2019.8856916

[117] Syed Monowar Hossain, Amin Ahsan Ali, Md. Mahbubur Rahman, Emre Ertine David Epstein, Ashley Kennedy, Kenzie Preston, Annie Umbricht, Yixin Chen, and Santosh Kumar. 2014. Identifying drug (cocaine) intake events from acute physiological response in the presence of free-living physical activity. In *International Symposium on Information Processing in Sensor Networks*. IEEE, 71–82. doi:10.1109/ipsn.2014.6846742

[118] Miao Hu, Zhenxiao Luo, Yipeng Zhou, Xuezheng Liu, and Di Wu. 2022. Otus: A Gaze Model-based Privacy Control Framework for Eye Tracking Applications. In *Conference on Computer Communications INFOCOM* (2022-05-02). IEEE, 560–569. doi:10.1109/INFOCOM48880.2022.9796665

[119] Zhiming Hu, Andreas Bulling, Sheng Li, and Guoping Wang. 2022. EHTask: Recognizing User Tasks from Eye and Head Movements in Immersive Virtual Reality. *Trans Vis Comput Graph* (2022).

[120] Pei Huang, Linke Guo, Ming Li, and Yuguang Fang. 2019. Practical Privacy-Preserving ECG-Based Authentication for IoT-Based Healthcare. *IEEE Internet of Things Journal* 6, 5 (Oct. 2019), 9200–9210. doi:10.1109/jiot.2019.2929087

[121] Anco Hundepool, Josep Domingo-Ferrer, Luisa Franconi, Sarah Giessing, Eric S. Nordholt, Keith Spicer, and Peter-Paul de Wolf. 2012. *Statistical Disclosure Control*. Wiley.

[122] J Thomas Hutton, JA Nagel, and Ruth B Loewenson. 1984. Eye tracking dysfunction in Alzheimer-type dementia. *Neurology* 34, 1 (Jan. 1984), 99–99. doi:10.1212/wnl.34.1.99

[123] Michiko Inoue, Masashi Nishiyama, and Yoshio Iwai. 2020. Gender Classification using the Gaze Distributions of Observers on Privacy-protected Training Images. In *International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications*. SCITEPRESS, 149–156. doi:10.5220/0008876101490156

[124] M. Ivasic-Kos, A. Iosifidis, A. Tefas, and I. Pitas. 2014. Person de-identification in activity videos. In *Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. IEEE, 1294–1299. doi:10.1109/mipro.2014.6859767

[125] Salar Jafarlou, Amir M. Rahmani, Nikil Dutt, and Sanaz Rahimi Mousavi. 2022. ECG Biosignal Deidentification Using Conditional Generative Adversarial Networks. In *2022 44th Annual International Conference of the IEEE Engineering in Medicine & Biology Society (EMBC)*. 1366–1370. doi:10.1109/EMBC48229.2022.9872015

[126] Jinhyeok Jang, Dohyung Kim, Cheonshu Park, Minsu Jang, Jaeyeon Lee, and Jaehong Kim. 2020. ETRI-Activity3D: A Large-Scale RGB-D Dataset for Robots to Recognize Daily Activities of the Elderly. In *2020 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)* (Las Vegas, NV, USA). IEEE Press, 10990–10997. doi:10.1109/IROS45743.2020.9341160

[127] J Jankovic. 2008. Parkinson's disease: clinical features and diagnosis. *J. neurol. neurosurg. psychiatry* 79, 4 (2008), 368–376. doi:10.1136/jnnp.2007.131045

[128] Qin Jin, Arthur R. Toth, Tanja Schultz, and Alan W. Black. 2009. Voice convergin: Speaker de-identification by voice transformation. In *ICASSP*. IEEE, 3909–3912. doi:10.1109/icassp.2009.4960482

[129] I. Joe Louis Paul, S. Sasirekha, S. Uma Maheswari, K. A. M. Ajith, S. M. Arjun, and S. Athesh Kumar. 2019. Eye gaze tracking-based adaptive e-learning for enhancing teaching and learning in virtual classrooms. In *Information and Communication Technology for Competitive Strategies*. Springer, 165–176.

[130] Théo Jourdan, Antoine Boutet, and Carole Frindel. 2018. Toward privacy in IoT mobile devices for activity recognition. In *International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*. ACM, 155–165. doi:10.1145/3286978.3287009

[131] Tadej Justin, Vitomir Struc, Simon Dobrisek, Bostjan Vesnicer, Ivo Ipsic, and France Mihelic. 2015. Speaker de-identification using diphone recognition and speech synthesis. In *Automatic Face and Gesture Recognition*. IEEE, 1–7. doi:10.1109/fg.2015.7285021

[132] E. Grace Mary Kanaga, R. Muthu Kumaran, M. Hema, R. Gowri Manohari, and Tina Anu Thomas. 2017. An experimental investigations on classifiers for Brain Computer Interface (BCI) based authentication. In *Conference on Trends in Electronics and Informatics (ICEI)*. IEEE, 1–6. doi:10.1109/icoei.2017.8300873

[133] Nader Karamzadeh, Yasaman Ardeshirpour, Matthew Kellman, Fatima Chowdhry, Afrouz Anderson, David Chorlian, Edward Wegman, and Amir Gandjbakhche. 2015. Relative brain signature: a population-based feature extraction procedure to identify functional biomarkers in the brain of alcoholics. *Brain and Behavior* 5, 7 (May 2015), e00335. doi:10.1002/brb3.335

[134] Stamos Katsigiannis and Naeem Ramzan. 2017. *DREAMER: A Database for Emotion Recognition through EEG and ECG Signals from Wireless Low-cost Off-the-Shelf Devices*. doi:10.1109/JBHI.2017.2688239

[135] Christina Katsini, Yasmeen Abdrabou, George E. Raptis, Mohamed Khamis, and Florian Alt. 2020. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In *Conference on Human Factors in Computing Systems CHI*. ACM, 1–21. doi:10.1145/3313831.3376840

[136] Georgios Kellaris, Stavros Papadopoulos, Xiaokui Xiao, and Dimitris Papadias. 2014. Differentially private event sequences over infinite streams. *Proceedings of the VLDB Endowment* 7, 12 (2014), 1155–1166.

[137] Gokce Keskin, Tyler Lee, Cory Stephenson, and Oguz H. Elibol. 2019. *Measuring the Effectiveness of Voice Conversion on Speaker Identification and Automatic Speech Recognition Systems*. Technical Report 1905.12531. arXiv.

[138] W Khalifa, A Salem, and M Roushdy. 2012. A Survey of EEG Based User Authentication Schemes. In *International Conference on INFOrmatics and Systems*. 55–60.

[139] Christopher Kirtley. 2006. *Clinical gait analysis: theory and practice*. Elsevier Health Sciences.

[140] Barbara Kitchenham. 2004. *Procedures for performing systematic reviews*. Technical Report TR/SE-0401. Keele University, Keele, UK.

[141] Sander Koelstra, Christian Muhl, Mohammad Soleymani, Jong-Seok Lee, Ashkan Yazdani, Touradj Ebrahimi, Thierry Pun, Anton Nijholt, and Ioannis Patras. 2012. DEAP: A Database for Emotion Analysis ;Using Physiological Signals.

Trans. Affect. Comput. 3, 1 (2012), 18–31. doi:10.1109/T-AFFC.2011.15

[142] Kazuhiro Kondo, Tomohiro Komiyama, and Shintaro Kashiwada. 2013. Towards Gender-Dependent Babble Maskers for Speech Privacy Protection. In *Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 275–278. doi:10.1109/iih-msp.2013.77

[143] Kazuhiro Kondo and Hiroki Sakurai. 2014. Gender-Dependent Babble Maskers Created from Multi-speaker Speech for Speech Privacy Protection. In *Conference on Intelligent Information Hiding and Multimedia Signal Processing*. IEEE, 251–254. doi:10.1109/iih-msp.2014.69

[144] M. Kosinski, D. Stillwell, and T. Graepel. 2013. Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences* 110, 15 (March 2013), 5802–5805. doi:10.1073/pnas.1218772110

[145] Krzysztof Krejtz, Andrew T. Duchowski, Anna Niedzielska, Cezary Biele, and Izabela Krejtz. 2018. Eye tracking cognitive load using pupil diameter and microsaccades with fixed gaze. *PLOS ONE* 13, 9 (Sept. 2018), e0203629. doi:10.1371/journal.pone.0203629

[146] Jacob Leon Kröger, Otto Hans-Martin Lutz, and Florian Müller. 2020. What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking. In *Privacy and Identity Management. Data for Better Living: AI and Privacy*. Springer International Publishing, 226–241. doi:10.1007/978-3-030-42504-3_15

[147] Craig A Kuechenmeister, Patrick H Linton, Thelma V Mueller, and Hilton B White. 1977. Eye Tracking in Relation to Age, Sex, and Illness. *Arch. Gen. Psychiatry* 34, 5 (May 1977), 578–579. doi:10.1001/archpsyc.1977.01770170088008

[148] Lamyanba Laishram, Muhammad Shaheryar, Jong Taek Lee, and Soon Ki Jung. 2025. Toward a Privacy-Preserving Face Recognition System: A Survey of Leakages and Solutions. *ACM Comput. Surv.* 57, 6, Article 147 (Feb. 2025), 38 pages. doi:10.1145/3673224

[149] Anthony Larcher, Kong Aik Lee, Bin Ma, and Haizhou Li. 2012. The RSR2015: Database for text-dependent speaker verification using multiple pass-phrases. *13th Annual Conference of the International Speech Communication Association 2012, INTERSPEECH 2012* 2 (Jan. 2012), 1578–1581.

[150] Juho Leinonen, Petri Ihantola, and Arto Hellas. 2017. Preventing Keystroke Based Identification in Open Data Sets. In *Conference on Learning @ Scale*. ACM, 101–109. doi:10.1145/3051457.3051458

[151] Deborah L. Levy, Anne B. Sereno, Diane C. Gooding, and Gilllian A. O'Driscoll. 2010. Eye Tracking Dysfunction in Schizophrenia: Characterization and Pathophysiology. In *Behavioral Neurobiology of Schizophrenia and Its Treatment*. Springer, 311–347. doi:10.1007/7854_2010_60

[152] Jingjie Li, Amrita Roy Chowdhury, Kassem Fawaz, and Younghyun Kim. 2021. Kaleido: Real-Time Privacy Control for Eye-Tracking Systems. In *USENIX Security*. 1793–1810. https://www.usenix.org/conference/usenixsecurity21/presentation/li-jingjie

[153] Yunji Liang, Sagar Samtani, Bin Guo, and Zhiwen Yu. 2020. Behavioral Biometrics for Continuous Authentication in the Internet-of-Things Era: An Artificial Intelligence Perspective. *Internet of Things Journal* 7, 9 (Sept. 2020), 9128–9143. doi:10.1109/jiot.2020.3004077

[154] Jae Lim and A. Oppenheim. 1978. All-pole modeling of degraded speech. *Transactions on Audio, Speech, and Language Processing* 26, 3 (June 1978), 197–210. doi:10.1109/tassp.1978.1163086

[155] Ao Liu, Lirong Xia, Andrew Duchowski, Reynold Bailey, Kenneth Holmqvist, and Eakta Jain. 2019. Differential privacy for eye-tracking data. In *Symposium on Eye Tracking Research & Applications*. ACM, 1–10. doi:10.1145/3314111.3319823

[156] Jun Liu, Amir Shahroudy, Mauricio Perez, Gang Wang, Ling-Yu Duan, and Alex C Kot. 2020. NTU RGB+D 120: A large-scale benchmark for 3D human activity understanding. *IEEE Transactions on Pattern Analysis and Machine Intelligence* 42, 10 (2020), 2684–2701.

[157] Xinwen Liu, Huan Wang, Zongjin Li, and Lang Qin. 2021. Deep learning in ECG diagnosis: A review. *Knowledge-Based Systems* 227 (2021), 107187. doi:10.1016/j.knosys.2021.107187

[158] Wen-Chih Lo, Ching-Ling Fan, Jean Lee, Chun-Ying Huang, Kuan-Ta Chen, and Cheng-Hsin Hsu. 2017. 360° Video Viewing Dataset in Head-Mounted Virtual Reality. In *Multimedia Systems Conference (MMSys)*. ACM, New York, NY, USA, 211–216. doi:10.1145/3083187.3083219

[159] Dillon Lohr, Samantha Aziz, Lee Friedman, and Oleg V Komogortsev. 2023. GazeBaseVR, a large-scale, longitudinal, binocular eye-tracking dataset collected in virtual reality. *Scientific Data* 10, 1 (2023), 177.

[160] Paula Lopez-Otero, Carmen Magariños, Laura Docio-Fernandez, Eduardo Rodriguez-Banga, Daniel Erro, and Carmen Garcia-Mateo. 2017. Influence of speaker de-identification in depression detection. *Signal Processing* 11, 9 (Dec. 2017), 1023–1030. doi:10.1049/iet-spr.2016.0731

[161] Yuanjun Lv, Jixun Yao, Peikun Chen, Hongbin Zhou, Heng Lu, and Lei Xie. 2023. Salt: Distinguishable Speaker Anonymization Through Latent Space Transformation. In *2023 IEEE Automatic Speech Recognition and Understanding Workshop (ASRU)*. IEEE, 1–8.

[162] Xiaosong Ma, Yubo Song, Zhongwei Wang, Shang Gao, Bin Xiao, and Aiqun Hu. 2021. You Can Hear But You Cannot Record: Privacy Protection by Jamming Audio Recording. In *International Conference on Communications* (2021-06).

IEEE, 1–6. doi:10.1109/ICC42927.2021.9500456

[163] Carmen Magariños, Paula Lopez-Otero, Laura Docio-Fernandez, Eduardo Rodriguez-Banga, Daniel Erro, and Carmen Garcia-Mateo. 2017. Reversible speaker de-identification using pre-trained transformation functions. *Computer Speech & Language* 46 (Nov. 2017), 36–52. doi:10.1016/j.csl.2017.05.001

[164] Ahmed Mahfouz, Tarek M. Mahmoud, and Ahmed Sharaf Eldin. 2017. A survey on behavioral biometric authentication on smartphones. *Journal of Information Security and Applications* 37 (Dec. 2017), 28–37. doi:10.1016/j.jisa.2017.10.002

[165] Seedahmed S. Mahmoud. 2016. A generalised wavelet packet-based anonymisation approach for ECG security application. *Security and Communication Networks* 9, 18 (Dec. 2016), 6137–6147. doi:10.1002/sec.1762

[166] Emanuele Maiorana, Patrizio Campisi, and Alessandro Neri. 2011. Bioconvolving: Cancelable templates for a multi-biometrics signature recognition system. In *International Systems Conference*. IEEE, 495–500. doi:10.1109/syscon.2011.5929064

[167] Anindya Maiti, Oscar Armbruster, Murtuza Jadliwala, and Jibo He. 2016. Smartwatch-Based Keystroke Inference Attacks and Context-Aware Protection Mechanisms. In *AsiaCCS*. ACM, 795–806. doi:10.1145/2897845.2897905

[168] Päivi Majaranta and Andreas Bulling. 2014. Eye Tracking and Eye-Based Human–Computer Interaction. In *Human–Computer Interaction*. Springer London, 39–65. doi:10.1007/978-1-4471-6392-3_3

[169] Yasushi Makihara, Hidetoshi Mannami, Akira Tsuji, Md. Altab Hossain, Kazushige Sugiura, Atsushi Mori, and Yasushi Yagi. 2012. The OU-ISIR Gait Database Comprising the Treadmill Dataset. *IPSJ Trans. Comput. Vis. Appl.* 4 (April 2012), 53–62. doi:10.2197/ipsjtcva.4.53

[170] Mohammad Malekzadeh, Richard G. Clegg, Andrea Cavallaro, and Hamed Haddadi. 2020. Privacy and utility preserving sensor-data transformations. 63 (2020), 101132. doi:10.1016/j.pmcj.2020.101132

[171] M. Sabarimalai Manikandan and S. Dandapat. 2008. ECG Distortion Measures and their Effectiveness. In *Emerging Trends in Engineering and Technology*. IEEE, 705–710. doi:10.1109/icetet.2008.248

[172] Ivan Martinovic, Doug Davies, Mario Frank, Daniele Perito, Tomas Ros, and Dawn Song. 2012. On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In *USENIX Security*. Bellevue, WA, 143–158.

[173] Richard Matovu and Abdul Serwadda. 2016. Your substance abuse disorder is an open secret! Gleaning sensitive personal information from templates in an EEG-based authentication system. In *International Conference on Biometrics Theory, Applications and Systems*. IEEE, 1–7. doi:10.1109/btas.2016.7791210

[174] Richard Matovu, Abdul Serwadda, David Irakiza, and Isaac Griswold-Steiner. 2018. Jekyll and Hyde: On The Double-Faced Nature of Smart-Phone Sensor Noise Injection. In *BIOSIG*. IEEE, 1–6. doi:10.23919/biosig.2018.8553043

[175] Gerald Matthews, W Middleton, Bernard Gilmartin, and Mark A Bullimore. 1991. Pupillary diameter and cognitive load. *J Psychophysiol* (1991).

[176] Candy Olivia Mawalim, Kasorn Galajit, Jessada Karnjana, Shunsuke Kidani, and Masashi Unoki. 2022. Speaker anonymization by modifying fundamental frequency and x-vector singular value. 73 (2022), 101326. doi:10.1016/j.csl.2021.101326

[177] Candy Olivia Mawalim, Shogo Okada, and Masashi Unoki. 2022. Speaker anonymization by pitch shifting based on time-scale modification. In *Proc. 2nd Symp. Secur. Privacy Speech Commun.* 35–42.

[178] Frank D. McSherry. 2009. Privacy Integrated Queries: An Extensible Platform for Privacy-preserving Data Analysis. In *SIGMOD*. ACM, 19–30. doi:10.1145/1559845.1559850

[179] Blaž Meden, Peter Rot, Philipp Terhörst, Naser Damer, Arjan Kuijper, Walter J. Scheirer, Arun Ross, Peter Peer, and Vitomir Štruc. 2021. Privacy–Enhancing Face Biometrics: A Comprehensive Survey. *IEEE TIFS* 16 (2021), 4147–4183. doi:10.1109/TIFS.2021.3096024

[180] Lubin Meng, Xue Jiang, Jian Huang, Wei Li, Hanbin Luo, and Dongrui Wu. 2023. User Identity Protection in EEG-Based Brain–Computer Interfaces. *IEEE Transactions on Neural Systems and Rehabilitation Engineering* 31 (2023), 3576–3586. doi:10.1109/TNSRE.2023.3310883

[181] Weizhi Meng, Duncan S. Wong, Steven Furnell, and Jianying Zhou. 2015. Surveying the Development of Biometric User Authentication on Mobile Phones. *IEEE Communications Surveys & Tutorials* 17, 3 (2015), 1268–1293. doi:10.1109/comst.2014.2386915

[182] Yan Meng, Yuxia Zhan, Jiachun Li, Suguo Du, Haojin Zhu, and Xuemin Shen. 2024. De-Anonymizing Avatars in Virtual Reality: Attacks and Countermeasures. *IEEE Transactions on Mobile Computing* 23, 12 (2024), 13342–13357. doi:10.1109/TMC.2024.3426046

[183] Sarina Meyer, Florian Lux, Pavel Denisov, Julia Koch, Pascal Tilli, and Ngoc Thang Vu. 2022. Speaker Anonymization with Phonetic Intermediate Representations. In *Interspeech 2022*. 4925–4929. doi:10.21437/Interspeech.2022-10703

[184] Sarina Meyer, Florian Lux, Julia Koch, Pavel Denisov, Pascal Tilli, and Ngoc Thang Vu. 2023. Prosody Is Not Identity: A Speaker Anonymization Approach Using Prosody Cloning. In *ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 1–5. doi:10.1109/ICASSP49357.2023.10096607

[185] Xiaoxiao Miao, Xin Wang, Erica Cooper, Junichi Yamagishi, and Natalia Tomashenko. 2022. Language-Independent Speaker Anonymization Approach Using Self-Supervised Pre-Trained Models. In *The Speaker and Language Recognition Workshop (Odyssey 2022)*. 279–286. doi:10.21437/Odyssey.2022-39

[186] Xiaoxiao Miao, Xin Wang, Erica Cooper, Junichi Yamagishi, and Natalia Tomashenko. 2023. Speaker Anonymization Using Orthogonal Householder Neural Network. *IEEE/ACM Trans. Audio, Speech and Lang. Proc.* 31 (Sept. 2023), 3681–3695. doi:10.1109/TASLP.2023.3313429

[187] Denis Migdal and Christophe Rosenberger. 2019. Keystroke Dynamics Anonymization System. In *International Joint Conference on e-Business and Telecommunications*. SCITEPRESS, 448–455. doi:10.5220/0007923804480455

[188] Denis Migdal and Christophe Rosenberger. 2019. My Behavior is my Privacy & Secure Password !. In *Conference on Cyberworlds*. IEEE, 299–307. doi:10.1109/cw.2019.00056

[189] G.B. Moody and R.G. Mark. 1990. The MIT-BIH Arrhythmia Database on CD-ROM and software for use with it. In *Proceedings Computers in Cardiology*. IEEE, 185–188. doi:10.1109/cic.1990.144205

[190] Saemi Moon, Myeonghyeon Kim, Zhenyue Qin, Yang Liu, and Dongwoo Kim. 2023. Anonymization for skeleton action recognition. In *Proceedings of the Thirty-Seventh AAAI Conference on Artificial Intelligence and Thirty-Fifth Conference on Innovative Applications of Artificial Intelligence and Thirteenth Symposium on Educational Advances in Artificial Intelligence (AAAI'23/IAAI'23/EAAI'23)*. AAAI Press, Article 1685, 9 pages. doi:10.1609/aaai.v37i12.26754

[191] Asunción Moreno, Dolors Poch, Antonio Bonafonte, Eduardo Lleida, Joaquim Llisterri, José Mariño, and Climent Nadeu. 1993. Albayzin speech database: Design of the phonetic corpus. In *Eurospeech*, Vol. 1.

[192] Aymen Mtibaa, Dijana Petrovska-Delacretaz, and Ahmed Ben Hamida. 2018. Cancelable speaker verification system based on binary Gaussian mixtures. In *Advanced Technologies for Signal and Image Processing*. IEEE, 1–6. doi:10.1109/atsip.2018.8364513

[193] Naoya Mukojima, Masaki Yasugi, Yasuhiro Mizutani, Takeshi Yasui, and Hirotsugu Yamamoto. 2022. Deep-Learning-Assisted Single-Pixel Imaging for Gesture Recognition in Consideration of Privacy. E105.C, 2 (2022), 79–85. doi:10.1587/transele.2021DII0002

[194] Arsha Nagrani, Joon Son Chung, and Andrew Zisserman. 2017. VoxCeleb: A Large-Scale Speaker Identification Dataset, In Interspeech 2017. *CoRR* abs/1706.08612. doi:10.21437/interspeech.2017-950

[195] Vivek Nair, Wenbo Guo, James F. O'Brien, Louis Rosenberg, and Dawn Song. 2024. Deep Motion Masking for Secure, Usable, and Scalable Real-Time Anonymization of Ecological Virtual Reality Motion Data. In *2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW)*. 493–500. doi:10.1109/VRW62533.2024.00096

[196] Vivek Nair, Wenbo Guo, Rui Wang, James F O'Brien, Louis Rosenberg, and Dawn Song. 2024. Berkeley Open Extended Reality Recordings 2023 (BOXRR-23): 4.7 Million Motion Capture Recordings from 105,000 XR Users. *IEEE Transactions on Visualization and Computer Graphics* (2024).

[197] Vivek Nair, Mark Roman Miller, Rui Wang, Brandon Huang, Christian Rack, Marc Erich Latoschik, and James F. O'Brien. 2024. Effect of Data Degradation on Motion Re-Identification. In *2024 IEEE 25th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. 85–90. doi:10.1109/WoWMoM60985.2024.00026

[198] Carol Neidle, Augustine Opoku, and Dimitris Metaxas. 2022. ASL Video Corpora and Sign Bank: Resources Available through the American Sign Language Linguistic Research Project (ASLLRP). doi:10.48550/ARXIV.2201.07899

[199] Alexandru Nelus and Rainer Martin. 2021. Privacy-Preserving Audio Classification Using Variational Information Feature Extraction. 29 (2021), 2864–2877. doi:10.1109/TASLP.2021.3108063

[200] Alexandru Nelus and Rainer Martin. 2018. Gender Discrimination Versus Speaker Identification Through Privacy-Aware Adversarial Feature Extraction. In *Speech Communication*.

[201] Francesco Nespoli, Daniel Barreda, Jöerg Bitzer, and Patrick A. Naylor. 2023. Two-Stage Voice Anonymization for Enhanced Privacy. In *INTERSPEECH 2023*. 3854–3858. doi:10.21437/Interspeech.2023-1341

[202] SUNY Downstate Medical Center Neurodynamics Laboratory. 1999. EEG Database. http://kdd.ics.uci.edu/databases/eeg/eeg.data.html

[203] Alexis Nolin-Lapalme, Robert Avram, and Hussin Julie. 2023. PrivECG: generating private ECG for end-to-end anonymization. In *Machine Learning for Healthcare Conference*. PMLR, 509–528.

[204] Nymi. [n. d.]. Always On Authantication. Webpage. https://nymi.com/ Accessed: 01.06.2019.

[205] Iyad Obeid and Joseph Picone. 2016. The temple university hospital EEG data corpus. *Frontiers in neuroscience* 10 (2016), 196.

[206] Ikenna Odinaka, Po-Hsiang Lai, Alan D. Kaplan, Joseph A. O'Sullivan, Erik J. Sirevaag, and John W. Rohrbaugh. 2012. ECG Biometric Recognition: A Comparative Analysis. *IEEE TIFS* 7, 6 (Dec. 2012), 1812–1824. doi:10.1109/tifs.2012.2215324

[207] Yoshitaka Ohshio, Haruka Adachi, Kenta Iwai, Takanobu Nishiura, and Yoichi Yamashita. 2018. Active Speech Obscuration with Speaker-dependent Human Speech-like Noise for Speech Privacy. In *Asia-Pacific Signal and Information Processing Association Annual Summit*. IEEE, 1252–1255. doi:10.23919/apsipa.2018.8659754

[208] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro. 2003. MCYT baseline corpus: a bimodal biometric database. *Vision, Image, and Signal Processing* 150, 6 (2003), 395. doi:10.1049/ip-vis:20031078

[209] Michele Panariello, Francesco Nespoli, Massimiliano Todisco, and Nicholas Evans. 2024. Speaker anonymization using neural audio codec language models. In *ICASSP 2024-2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 4725–4729.

[210] Vassil Panayotov, Guoguo Chen, Daniel Povey, and Sanjeev Khudanpur. 2015. Librispeech: An ASR corpus based on public domain audio books. In *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 5206–5210. doi:10.1109/icassp.2015.7178964

[211] Julien Pansiot, Danail Stoyanov, Douglas McIlwraith, Benny P.L. Lo, and G. Z. Yang. 2007. Ambient and Wearable Sensor Fusion for Activity Recognition in Healthcare Monitoring Systems. In *Workshop on Wearable and Implantable Body Sensor Networks*. Springer, 208–212. doi:10.1007/978-3-540-70994-7_36

[212] Sree Hari Krishnan Parthasarathi, Herve Bourlard, and Daniel Gatica-Perez. 2011. LP Residual Features for Robust, Privacy-Sensitive Speaker Diarization. In *Interspeech*.

[213] Sree Hari Krishnan Parthasarathi, H. Bourlard, and D. Gatica-Perez. 2013. Wordless Sounds: Robust Speaker Diarization Using Privacy-Preserving Audio Representations. *Transactions on Audio, Speech, and Language Processing* 21, 1 (Jan. 2013), 85–98. doi:10.1109/tasl.2012.2215588

[214] Sree Hari Krishnan Parthasarathi, Mathew Magimai.-Doss, Daniel Gatica-Perez, and Hervé Bourlard. 2009. Speaker change detection with privacy-preserving audio cues. In *International conference on Multimodal interfaces*. ACM Press, 343. doi:10.1145/1647314.1647385

[215] Damian Pascual, Alireza Amirshahi, Amir Aminifar, David Atienza, Philippe Ryvlin, and Roger Wattenhofer. 2021. EpilepsyGAN: Synthetic Epileptic Brain Activities With Privacy Preservation. 68, 8 (2021), 2435–2446. doi:10.1109/TBME.2020.3042574

[216] Manas A. Pathak and Bhiksha Raj. 2012. Privacy-preserving speaker verification as password matching. In *ICASSP*. IEEE, 1849–1852. doi:10.1109/icassp.2012.6288262

[217] Jose Patino, Natalia Tomashenko, Massimiliano Todisco, Andreas Nautsch, and Nicholas Evans. 2021. Speaker Anonymisation Using the McAdams Coefficient. In *Interspeech* (2021-08-30). ISCA, 1099–1103. doi:10.21437/Interspeech.2021-1070

[218] Juan M. Perero-Codosero, Fernando M. Espinoza-Cuadros, and Luis A. Hernández-Gómez. 2022. X-vector anonymization using autoencoders and adversarial training for preserving speech privacy. *Comput. Speech Lang.* 74, C (July 2022), 13 pages. doi:10.1016/j.csl.2022.101351

[219] David I. Perrett, Sean N. Talamas, Patrick Cairns, and Audrey J. Henderson. 2020. Skin Color Cues to Human Health: Carotenoids, Aerobic Fitness, and Body Fat. *Frontiers in Psychology* 11 (March 2020). doi:10.3389/fpsyg.2020.00392

[220] Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek, and Florian Alt. 2019. Behavioural Biometrics in VR. In *CHI Conference on Human Factors in Computing Systems*. ACM, 1–12. doi:10.1145/3290605.3300340

[221] Esteban Piacentino and Cecilio Angulo. 2020. Generating fake data using GANs for anonymizing healthcare data. In *International Work-Conference on Bioinformatics and Biomedical Engineering*. Springer, 406–417.

[222] R. Plamondon and S.N. Srihari. 2000. Online and off-line handwriting recognition: a comprehensive survey. *IEEE TPAMI* 22, 1 (2000), 63–84. doi:10.1109/34.824821

[223] Kurt Plarre, Andrew Raij, Syed Monowar Hossain, Amin Ahsan Ali, Motohiro Nakajima, Mustafa Al'absi, Emre Ertin, Thomas Kamarck, Santosh Kumar, Marcia Scott, Daniel Siewiorek, Asim Smailagic, and Lorentz E. Wittmers. 2011. Continuous inference of psychological stress from sensory measurements collected in the natural environment. In *International Conference on Information Processing in Sensor Networks*. IEEE,ACM, 97–108.

[224] M. Pobar and I. Ipsic. 2014. Online speaker de-identification using voice transformation. In *Convention on Information and Communication Technology, Electronics and Microelectronics*. IEEE, 1264–1267. doi:10.1109/mipro.2014.6859761

[225] Bogdan Pogorelc, Zoran Bosnić, and Matjaž Gams. 2011. Automatic recognition of gait-related health problems in the elderly using machine learning. *Multimedia Tools and Applications* 58, 2 (Nov. 2011), 333–354. doi:10.1007/s11042-011-0786-1

[226] Frank E. Pollick, Jim W. Kay, Katrin Heim, and Rebecca Stringer. 2005. Gender recognition from point-light walkers. *J Exp Psychol Hum Percept Perform* 31, 6 (Dec. 2005), 1247–1265. doi:10.1037/0096-1523.31.6.1247

[227] Alex Poole and Linden J. Ball. 2006. Eye Tracking in HCI and Usability Research. In *Encyclopedia of Human Computer Interaction*. IGI Global, 211–219. doi:10.4018/978-1-59140-562-7.ch034

[228] Jose Portelo, Alberto Abad, Bhiksha Raj, and Isabel Trancoso. 2013. Secure Binary Embeddings of Front-End Factor Analysis for Privacy Preserving Speaker Verification. In *INTERSPEECH*. 2494–2498.

[229] Jose Portelo, Bhiksha Raj, Alberto Abad, and Isabel Trancoso. 2014. Privacy-preserving speaker verification using secure binary embeddings. In *Convention on Information and Communication Technology, Electronics and Microelectronics*. IEEE, 1268–1272. doi:10.1109/mipro.2014.6859762

[230] Daniel Povey, Arnab Ghoshal, Gilles Boulianne, Lukas Burget, Ondrej Glembek, Nagendra Goel, Mirko Hannemann, Petr Motlicek, Yanmin Qian, Petr Schwarz, et al. 2011. The Kaldi speech recognition toolkit. In *Workshop on automatic speech recognition and understanding*. IEEE Signal Processing Society.

[231] Gauri P. Prajapati, Dipesh K. Singh, Preet P. Amin, and Hemant A. Patil. 2021. Voice Privacy Through x-Vector and CycleGAN-Based Anonymization. In *Interspeech* (2021-08-30). ISCA, 1684–1688. doi:10.21437/Interspeech.2021-1573

[232] Gauri P. Prajapati, Dipesh K. Singh, Preet P. Amin, and Hemant A. Patil. 2022. Voice privacy using CycleGAN and time-scale modification. *Comput. Speech Lang.* 74, C (July 2022), 30 pages. doi:10.1016/j.csl.2022.101353

[233] Jiří Přibil, Anna Přibilová, and Jindřich Matoušek. 2018. Evaluation of speaker de-identification based on voice gender and age conversion. *Journal of Electrical Engineering* 69, 2 (March 2018), 138–147. doi:10.2478/jee-2018-0017

[234] Jianwei Qian, Haohua Du, Jiahui Hou, Linlin Chen, Taeho Jung, and Xiangyang Li. 2021. Speech Sanitizer: Speech Content Desensitization and Voice Anonymization. *TDSC* (2021). doi:10.1109/tdsc.2019.2960239

[235] Jianwei Qian, Haohua Du, Jiahui Hou, Linlin Chen, Taeho Jung, and Xiang-Yang Li. 2018. Hidebehind: Enjoy Voice Input with Voiceprint Unclonability and Anonymity. In *Conference on Embedded Networked Sensor Systems*. ACM, 82–94. doi:10.1145/3274783.3274855

[236] Jianwei Qian, Feng Han, Jiahui Hou, Chunhong Zhang, Yu Wang, and Xiang-Yang Li. 2018. Towards Privacy-Preserving Speech Data Publishing. In *INFOCOM*. IEEE, 1079–1087. doi:10.1109/infocom.2018.8486250

[237] Yaron Rachlin and Dror Baron. 2008. The secrecy of compressed sensing measurements. In *Allerton Conference*. IEEE, 813–817. doi:10.1109/allerton.2008.4797641

[238] Vibhor Rastogi and Suman Nath. 2010. Differentially private aggregation of distributed time-series with transformation and encryption. In *SIGMOD*. ACM, 735–746. doi:10.1145/1807167.1807247

[239] Vijay Ravi, Jinhan Wang, Jonathan Flint, and Abeer Alwan. 2024. Enhancing accuracy and privacy in speech-based depression detection through speaker disentanglement. *Comput. Speech Lang.* 86, C (June 2024), 24 pages. doi:10.1016/j.csl.2023.101605

[240] SRS Reddy, Sravani Nalluri, Subramanyam Kunisetti, S Ashok, and B Venkatesh. 2019. Content-based movie recommendation system using genre correlation. In *Smart Intelligent Computing and Applications*. Springer, 391–397.

[241] Kenneth Revett, Hamid Jahankhani, Sérgio Tenreiro de Magalhães, and Henrique Santos. 2008. A survey of user authentication based on mouse dynamics. In *International Conference on Global e-Security*. Springer, 210–219.

[242] Douglas A. Reynolds. 1995. Speaker identification and verification using Gaussian mixture speaker models. *Speech Communication* 17, 1 (Aug. 1995), 91–108. doi:10.1016/0167-6393(95)00009-d

[243] Douglas A. Reynolds, Thomas F. Quatieri, and Robert B. Dunn. 2000. Speaker Verification Using Adapted Gaussian Mixture Models. *Digital Signal Processing* 10, 1 (Jan. 2000), 19–41. doi:10.1006/dspr.1999.0361

[244] Slobodan Ribaric, Aladdin Ariyaeeinia, and Nikola Pavesic. 2016. De-identification for privacy protection in multimedia content: A survey. *Signal Processing: Image Communication* 47 (Sept. 2016), 131–151. doi:10.1016/j.image.2016.05.020

[245] Pierre Rougé, Ali Moukadem, Alain Dieterlen, Antoine Boutet, and Carole Frindel. 2022. Generalizable Features for Anonymizing Motion Signals Based on the Zeros of the Short-Time Fourier Transform. *J. Signal Process. Syst.* 95, 1 (July 2022), 89–99. doi:10.1007/s11265-022-01798-9

[246] Zhang Rui and Zheng Yan. 2018. A survey on biometric authentication: Toward secure and privacy-preserving identification. *IEEE access* 7 (2018), 5994–6009.

[247] Napa Sae-Bae and Nasir Memon. 2013. A Simple and Effective Method for Online Signature Verification. *Lecture Notes in Informatics (LNI)*, 1–12.

[248] Nazir Saleheen, Supriyo Chakraborty, Nasir Ali, Md Mahbubur Rahman, Syed Monowar Hossain, Rummana Bari, Eugene Buder, Mani Srivastava, and Santosh Kumar. 2016. MSieve: Differential Behavioral Privacy in Time of Mobile Sensor Data. In *International Joint Conference on Pervasive and Ubiquitous Computing (UbiComp)*. ACM, New York, NY, USA, 706–717. doi:10.1145/2971648.2971753

[249] Ben Saunders, Necati Cihan Camgoz, and Richard Bowden. 2021. Anonysign: Novel Human Appearance Synthesis for Sign Language Video Anonymisation. In *Automatic Face and Gesture Recognition* (2021-12-15). IEEE, 1–8. doi:10.1109/FG52635.2021.9666984

[250] G. Schalk, D.J. McFarland, T. Hinterberger, N. Birbaumer, and J.R. Wolpaw. 2004. BCI2000: a general-purpose brain-computer interface (BCI) system. *IEEE Transactions on Biomedical Engineering* 51, 6 (2004), 1034–1043. doi:10.1109/TBME.2004.827072

[251] Abdur R. Shahid and Sajedul Talukder. 2021. Evaluating Machine Learning Models for Handwriting Recognition-based Systems under Local Differential Privacy. In *Innovations in Intelligent Systems and Applications Conference* (2021-10-06). IEEE, 1–6. doi:10.1109/ASYU52992.2021.9598983

[252] Ali Shahin Shamsabadi, Brij Mohan Lal Srivastava, Aurélien Bellet, Nathalie Vauquier, Emmanuel Vincent, Mohamed Maouche, Marc Tommasi, and Nicolas Papernot. 2023. Differentially Private Speaker Anonymization. *Proceedings on Privacy Enhancing Technologies* 1 (2023), 98–114.

[253] Dushyant Sharma, Francesco Nespoli, Rong Gong, and Patrick A. Naylor. 2023. Canonical Voice Conversion and Dual-Channel Processing for Improved Voice Privacy of Speech Recognition Data. In *2023 31st European Signal Processing Conference (EUSIPCO)*. 66–70. doi:10.23919/EUSIPCO58844.2023.10289777

[254] Michael Sherman, Gradeigh Clark, Yulong Yang, Shridatt Sugrim, Arttu Modig, Janne Lindqvist, Antti Oulasvirta, and Teemu Roos. 2014. User-generated free-form gestures for authentication. In *MobiSys*. ACM, New York, NY, USA, 176–189. doi:10.1145/2594368.2594375

[255] Md Shopon, Sanjida Nasreen Tumpa, Yajurv Bhatia, K. N. Pavan Kumar, and Marina L. Gavrilova. 2021. Biometric Systems De-Identification: Current Advancements and Future Directions. *Journal of Cybersecurity and Privacy* 1, 3 (2021), 470–495. doi:10.3390/jcp1030024

[256] Dipesh K. Singh, Gauri P. Prajapati, and Hemant A. Patil. 2024. Voice Privacy Using Time-Scale and Pitch Modification. *SN Comput. Sci.* 5, 2 (Jan. 2024), 19 pages. doi:10.1007/s42979-023-02549-8

[257] Girijesh Singh, Palak Patel, Muhammad Asaduzzaman, and Garima Bajwa. 2023. Selective EEG Signal Anonymization using Multi-Objective Autoencoders. In *2023 20th Annual International Conference on Privacy, Security and Trust (PST)*. 1–7. doi:10.1109/PST58708.2023.10320167

[258] Vincent Sitzmann, Ana Serrano, Amy Pavel, Maneesh Agrawala, Diego Gutierrez, Belen Masia, and Gordon Wetzstein. 2018. Saliency in VR: How Do People Explore Virtual Environments? *IEEE Trans Vis Comput Graph* 24, 4 (2018), 1633–1642. doi:10.1109/TVCG.2018.2793599

[259] David Snyder, Daniel Garcia-Romero, Gregory Sell, Daniel Povey, and Sanjeev Khudanpur. 2018. X-Vectors: Robust DNN Embeddings for Speaker Recognition. In *Conference on Acoustics, Speech and Signal Processing (ICASSP)*. IEEE, 5329–5333. doi:10.1109/icassp.2018.8461375

[260] Cristina Soaz and Klaus Diepold. 2016. Step Detection and Parameterization for Gait Assessment Using a Single Waist-Worn Accelerometer. *TBME* 63, 5 (2016), 933–942. doi:10.1109/TBME.2015.2480296

[261] Petr Sojka, Aleš Horák, Ivan Kopeček, and Karel Pala (Eds.). 2014. *Text, Speech and Dialogue*. Lecture Notes in Computer Science, Vol. 8655. Springer International Publishing. doi:10.1007/978-3-319-10816-2

[262] Brij Mohan Lal Srivastava, Nathalie Vauquier, Md Sahidullah, Aurelien Bellet, Marc Tommasi, and Emmanuel Vincent. 2020. Evaluating Voice Conversion-based Privacy Protection against Informed Attackers. (5 2020). doi:10.1109/icassp40776.2020.9053868

[263] Ioanna-Ourania Stathopoulou and George A Tsihrintzis. 2011. Emotion recognition from body movements and gestures. In *Intelligent interactive multimedia systems and services*. Springer, 295–303.

[264] Julian Steil, Inken Hagestedt, Michael Xuelin Huang, and Andreas Bulling. 2019. Privacy-Aware Eye Tracking Using Differential Privacy. In *Symposium on Eye Tracking Research & Applications (ETRA)*. ACM, New York, NY, USA. doi:10.1145/3314111.3319915

[265] Julian Steil, Inken Hagestedt, Michael Xuelin Huang, and Andreas Bulling. 2019. Privacy-Aware Eye Tracking Using Differential Privacy. In *Inter. Symp. on Eye Tracking Research and Applications (ETRA)*. ACM, 1–9. doi:10.1145/3314111.3319915

[266] Nathan J Stevenson, Karoliina Tapani, Leena Lauronen, and Sampsa Vanhatalo. 2019. A dataset of neonatal EEG recordings with seizure annotations. *Scientific data* 6, 1 (2019), 1–8.

[267] Tino Stöckel, Robert Jacksteit, Martin Behrens, Ralf Skripitz, Rainer Bader, and Anett Mau-Moeller. 2015. The mental representation of the human gait in young and older adults. *Frontiers in Psychology* 6 (2015), 943. doi:10.3389/fpsyg.2015.00943

[268] Fahim Sufi, Seedahmed Mahmoud, and Ibrahim Khalil. 2008. A new ECG obfuscation method: A joint feature extraction & corruption approach. In *Conference on Information Technology and Applications in Biomedicine*. IEEE, 334–337. doi:10.1109/itab.2008.4570644

[269] Shravani Sur and VK Sinha. 2009. Event-related potential: An overview. *Industrial Psychiatry Journal* 18, 1 (2009), 70. doi:10.4103/0972-6748.57865

[270] Takahiro Tamesue and Tetsuro Saeki. 2014. Sound masking for achieving speech privacy with parametric acoustic array speaker. In *Soft Computing and Intelligent Systems and Advanced Intelligent Systems*. IEEE, 1134–1137. doi:10.1109/scis-isis.2014.7044805

[271] Pin Shen Teh, Andrew Beng Jin Teoh, and Shigang Yue. 2013. A Survey of Keystroke Dynamics Biometrics. *The Scientific World Journal* 2013 (2013), 1–24. doi:10.1155/2013/408280

[272] Pin Shen Teh, Ning Zhang, Andrew Beng Jin Teoh, and Ke Chen. 2016. A survey on touch dynamics authentication in mobile devices. *Computers & Security* 59 (June 2016), 210–235. doi:10.1016/j.cose.2016.03.003

[273] Daksh Thapar, Chetan Arora, and Aditya Nigam. 2020. Is Sharing of Egocentric Video Giving Away Your Biometric Signature?. In *Computer Vision – ECCV 2020*, Andrea Vedaldi, Horst Bischof, Thomas Brox, and Jan-Michael Frahm (Eds.). Springer International Publishing, Cham, 399–416.

[274] Daksh Thapar, Aditya Nigam, and Chetan Arora. 2021. Anonymizing Egocentric Videos. In *International Conference on Computer Vision (ICCV)* (2021-10). IEEE, 2300–2309. doi:10.1109/ICCV48922.2021.00232

[275] Ngoc-Dung T. Tieu, Huy H. Nguyen, Hoang-Quoc Nguyen-Son, Junichi Yamagishi, and Isao Echizen. 2017. An approach for gait anonymization using deep learning. In *Workshop on Information Forensics and Security*. IEEE, 1–6. doi:10.1109/wifs.2017.8267657

[276] Ngoc-Dung T. Tieu, Huy H. Nguyen, Hoang-Quoc Nguyen-Son, Junichi Yamagishi, and Isao Echizen. 2019. Spatio-temporal generative adversarial network for gait anonymization. *Journal of Information Security and Applications* 46 (June 2019), 307–319. doi:10.1016/j.jisa.2019.03.002

[277] Ngoc-Dung T. Tieu, Junichi Yamagishi, and Isao Echizen. 2020. Color Transfer to Anonymized Gait Images While Maintaining Anonymization. In *Asia-Pacific Signal and Information Processing Association Annual Symposium*. 1406–1413.

[278] Toda Tomoki, Ling-Hui Chen, Daisuke Saito, Fernando Villavicencio, Mirjam Wester, Zhizheng Wu, and Junichi Yamagishi. 2016. The Voice Conversion Challenge 2016 dataset. University of Edinburgh. School of Informatics. Centre for Speech Technology Research. doi:10.7488/ds/1575

[279] Quang Nhat Tran, Benjamin P. Turnbull, and Jiankun Hu. 2021. Biometrics and Privacy-Preservation: How Do They Evolve? *Open Journal of the Computer Society* 2 (2021), 179–191. doi:10.1109/ojcs.2021.3068385

[280] Nikolaus F. Troje. 2002. Decomposing biological motion: A framework for analysis and synthesis of human gait patterns. *Journal of Vision* 2, 5 (Sept. 2002), 2. doi:10.1167/2.5.2

[281] TypingDNA. [n. d.]. Webpage. https://www.typingdna.com Accessed: 01.06.2019.

[282] Anthony Ngozichukwuka Uwaechia and Dzati Athiar Ramli. 2021. A Comprehensive Survey on ECG Signals as New Biometric Modality for Human Authentication: Recent Advances and Future Challenges. *IEEE Access* 9 (2021), 97760–97802. doi:10.1109/ACCESS.2021.3095248

[283] Tavish Vaidya and Micah Sherr. 2019. You Talk Too Much: Limiting Privacy Exposure Via Voice Input. In *Security and Privacy Workshops (SPW)*. IEEE, 84–91. doi:10.1109/spw.2019.00026

[284] Michel Valstar, Jonathan Gratch, Björn Schuller, Fabien Ringeval, Denis Lalanne, Mercedes Torres Torres, Stefan Scherer, Giota Stratou, Roddy Cowie, and Maja Pantic. 2016. AVEC 2016: Depression, Mood, and Emotion Recognition Workshop and Challenge. In *Proceedings of the 6th International Workshop on Audio/Visual Emotion Challenge* (Amsterdam, The Netherlands) *(AVEC '16)*. Association for Computing Machinery, New York, NY, USA, 3–10. doi:10.1145/2988257.2988258

[285] I. van der Linde, U. Rajashekar, A.C. Bovik, and L.K. Cormack. 2009. DOVES: A database of visual eye movements. Spatial Vision. 161-177 pages. http://live.ece.utexas.edu/research/doves

[286] Gabriele Vassallo, Tim Van hamme, Davy Preuveneers, and Wouter Joosen. 2017. Privacy-Preserving Behavioral Authentication on Smartphones. In *International Workshop on Human-centered Sensing, Networking, and Systems*. ACM, 1–6. doi:10.1145/3144730.3144731

[287] Voice Vault. [n. d.]. VoiceVault Voice Biometric Authentication. Webpage. https://voicevault.com/ Accessed: 01.06.2019.

[288] Changsheng Wan, Li Wang, and Vir V. Phoha. 2019. A Survey on Gait Recognition. *Comput. Surveys* 51, 5 (Jan. 2019), 1–35. doi:10.1145/3230633

[289] Shuo Wang, Ming Jiang, Xavier Morin Duchesne, Elizabeth A. Laugeson, Daniel P. Kennedy, Ralph Adolphs, and Qi Zhao. 2015. Atypical Visual Saliency in Autism Spectrum Disorder Quantified through Model-Based Eye Tracking. *Neuron* 88, 3 (Nov. 2015), 604–616. doi:10.1016/j.neuron.2015.09.042

[290] Tao Wang, Yushu Zhang, Shuren Qi, Ruoyu Zhao, Zhihua Xia, and Jian Weng. 2024. Security and Privacy on Generative Data in AIGC: A Survey. *ACM Comput. Surv.* 57, 4, Article 82 (Dec. 2024), 34 pages. doi:10.1145/3703626

[291] Yijun Wang, Xiaogang Chen, Xiaorong Gao, and Shangkai Gao. 2017. A Benchmark Dataset for SSVEP-Based Brain–Computer Interfaces. *IEEE Transactions on Neural Systems and Rehabilitation Engineering* 25, 10 (2017), 1746–1752. doi:10.1109/TNSRE.2016.2627556

[292] Leon Willenborg and Ton de Waal. 2001. *Elements of Statistical Disclosure Control*. Springer New York, New York. doi:10.1007/978-1-4613-0121-9

[293] Ethan Wilson, Azim Ibragimov, Michael J. Proulx, Sai Deep Tetali, Kevin Butler, and Eakta Jain. 2024. Privacy-Preserving Gaze Data Streaming in Immersive Interactive Virtual Reality: Robustness and User Experience. *IEEE Transactions on Visualization and Computer Graphics* 30, 5 (2024), 2257–2268. doi:10.1109/TVCG.2024.3372032

[294] Shun-Chi Wu, Peng-Tzu Chen, A. Lee Swindlehurst, and Pei-Lun Hung. 2019. Cancelable Biometric Recognition With ECGs: Subspace-Based Approaches. *IEEE TIFS* 14, 5 (May 2019), 1323–1336. doi:10.1109/tifs.2018.2876838

[295] Danny Wyatt, Tanzeem Choudhury, and Jeff Bilmes. 2007. Conversation Detection and Speaker Segmentation in Privacy-Sensitive Situated Speech Data. In *INTERSPEECH*.

[296] Zhaoyang Xia, Yuxiao Chen, Qilong Zhangli, Matt Huenerfauth, Carol Neidle, and Dimitris Metaxas. 2022. Sign Language Video Anonymization. In *Workshop on the Representation and Processing of Sign Languages*.

[297] Shilin Xiao, Xiaoyu Ji, Chen Yan, Zhicong Zheng, and Wenyuan Xu. 2023. MicPro: Microphone-based Voice Privacy Protection. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security* (Copenhagen,

Denmark) *(CCS '23)*. Association for Computing Machinery, New York, NY, USA, 1302–1316. doi:10.1145/3576915.3616616

[298] Yanyu Xu, Yanbing Dong, Junru Wu, Zhengzhong Sun, Zhiru Shi, Jingyi Yu, and Shenghua Gao. 2018. Gaze Prediction in Dynamic 360° Immersive Videos. In *CVPR*. 5333–5342. doi:10.1109/CVPR.2018.00559

[299] Sherif Yacoub, Steve Simske, Xiaofan Lin, and John Burns. 2003. Recognition of emotions in interactive voice response systems. In *EUROSPEECH*.

[300] Junichi Yamagishi, Christophe Veaux, and Kirsten MacDonald. 2019. CSTR VCTK Corpus: English Multi-speaker Corpus for CSTR Voice Cloning Toolkit (version 0.92). University of Edinburgh. The Centre for Speech Technology Research (CSTR). doi:10.7488/ds/2645

[301] Roman V. Yampolskiy and Venu Govindaraju. 2010. Taxonomy of Behavioural Biometrics. In *Behavioral Biometrics for Human Identification*. IGI Global, 1–43. doi:10.4018/978-1-60566-725-6.ch001

[302] Qing Yang, Tao Wang, Ning Su, Shifu Xiao, and Zoi Kapoula. 2012. Specific saccade deficits in patients with Alzheimer's disease at mild to moderate stage and in patients with amnestic mild cognitive impairment. *AGE* 35, 4 (May 2012), 1287–1298. doi:10.1007/s11357-012-9420-z

[303] Yulong Yang, Gradeigh D Clark, Janne Lindqvist, and Antti Oulasvirta. 2016. Free-form gesture authentication in the wild. In *Conference on Human Factors in Computing Systems*. ACM, 3722–3735.

[304] Yang Yang, Yury Kartynnik, Yunpeng Li, Jiuqiang Tang, Xing Li, George Sung, and Matthias Grundmann. 2024. STREAMVC: Real-Time Low-Latency Voice Conversion. In *ICASSP 2024 - 2024 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 11016–11020. doi:10.1109/ICASSP48485.2024.10446863

[305] Jixun Yao, Qing Wang, Pengcheng Guo, Ziqian Ning, and Lei Xie. 2024. Distinctive and Natural Speaker Anonymization via Singular Value Transformation-Assisted Matrix. *IEEE/ACM Transactions on Audio, Speech, and Language Processing* 32 (2024), 2944–2956. doi:10.1109/TASLP.2024.3407600

[306] Jixun Yao, Qing Wang, Yi Lei, Pengcheng Guo, Lei Xie, Namin Wang, and Jie Liu. 2023. Distinguishable Speaker Anonymization Based on Formant and Fundamental Frequency Scaling. In *ICASSP 2023 - 2023 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*. 1–5. doi:10.1109/ICASSP49357.2023.10095120

[307] Xin Yao and Senquan An. 2023. DP-VoicePub: Differential Privacy-based Voice Publication. In *2023 IEEE International Symposium on Circuits and Systems (ISCAS)*. 1–5. doi:10.1109/ISCAS46773.2023.10182113

[308] Yue Yao, Josephine Plested, Tom Gedeon, Yuchi Liu, and Zhengjie Wang. 2019. Improved Techniques for Building EEG Feature Filters. In *International Joint Conference on Neural Networks (IJCNN)*. IEEE, 1–6. doi:10.1109/ijcnn.2019.8852302

[309] Xin Xu Shaoji Zhang Ming Li Yao Shi, Hui Bu. 2015. AISHELL-3: A Multi-speaker Mandarin TTS Corpus and the Baselines. https://arxiv.org/abs/2010.11567

[310] Mang Ye, Jianbing Shen, Gaojie Lin, Tao Xiang, Ling Shao, and Steven C.H. Hoi. 2021. Deep Learning for Person Re-identification: A Survey and Outlook. *IEEE TPAMI* (2021), 1–1. doi:10.1109/tpami.2021.3054775

[311] Dit-Yan Yeung, Hong Chang, Yimin Xiong, Susan George, Ramanujan Kashi, Takashi Matsumoto, and Gerhard Rigoll. 2004. SVC2004: First International Signature Verification Competition. In *Biometric Authentication*, David Zhang and Anil K. Jain (Eds.). Vol. 3072. Springer Berlin Heidelberg, 16–22. doi:10.1007/978-3-540-25948-0_3 Title: Lecture Notes in Computer Science.

[312] In-Chul Yoo, Keonnyeong Lee, Seonggyun Leem, Hyunwoo Oh, Bonggu Ko, and Dongsuk Yook. 2020. Speaker Anonymization for Personal Information Protection Using Voice Conversion Techniques. 8 (2020), 198637–198645. doi:10.1109/ACCESS.2020.3035416

[313] Galit Yovel and Alice J. O'Toole. 2016. Recognizing People in Motion. *Trends in Cognitive Sciences* 20, 5 (May 2016), 383–395. doi:10.1016/j.tics.2016.02.005

[314] Ruibin Yuan, Yuxuan Wu, Jacob Li, and Jaxter Kim. 2022. DeID-VC: Speaker De-identification via Zero-shot Pseudo Voice Conversion. In *Interspeech 2022*. 2593–2597. doi:10.21437/Interspeech.2022-11036

[315] Emna Kalai Zaghouani, Adel Benzina, and Rabah Attia. 2017. ECG based authentication for e-healthcare systems: Towards a secured ECG features transmission. In *Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, 1777–1783. doi:10.1109/iwcmc.2017.7986553

[316] Emna Kalai Zaghouani, Adel Benzina, and Rabah Attia. 2017. ECG biometrie template protection based on secure sketch scheme. In *Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 1–5. doi:10.23919/softcom.2017.8115526

[317] Mohammad-Reza Zare-Mirakabad, Fatemeh Kaveh-Yazdy, and Mohammad Tahmasebi. 2013. Privacy preservation by k-anonymizing Ngrams of time. In *ISC Conference on Information Security and Cryptology*. 1–6. doi:10.1109/ISCISC.2013.6767335

[318] Gao Zhang, Zhiwei Guan, Guozhong Dai, and Xiangshi Ren. 1998. A comparison of four interaction modes for CAD systems. In *APCHI*. 82–87. doi:10.1109/APCHI.1998.704160

[319] Guanglin Zhang, Sifan Ni, and Ping Zhao. 2020. Enhancing Privacy Preservation in Speech Data Publishing. *Internet of Things Journal* 7, 8 (Aug. 2020), 7357–7367. doi:10.1109/jiot.2020.2983228

[320] Ni Zhang and Yoshinori Yaginuma. 2012. A privacy-preserving and language-independent speaking detecting and speaker diarization approach for spontaneous conversation using microphones. In *International Conference on Signal Processing*. IEEE, 499–502. doi:10.1109/icosp.2012.6491534

[321] Jianwei Zheng, Jianming Zhang, Sidy Danioko, Hai Yao, Hangyuan Guo, and Cyril Rakovski. 2020. A 12-lead electrocardiogram database for arrhythmia research covering more than 10,000 patients. *Scientific Data* 7, 1 (Feb. 2020). doi:10.1038/s41597-020-0386-x

[322] Nan Zheng, Aaron Paloski, and Haining Wang. 2016. An Efficient User Verification System Using Angle-Based Mouse Movement Biometrics. *IEEE TIFS* 18, 3 (April 2016), 1–27. doi:10.1145/2893185

[323] Shuai Zheng, Junge Zhang, Kaiqi Huang, Ran He, and Tieniu Tan. 2011. Robust view transformation model for gait recognition. In *International Conference on Image Processing*. IEEE, 2073–2076. doi:10.1109/icip.2011.6115889

[324] Wei-Long Zheng and Bao-Liang Lu. 2015. Investigating Critical Frequency Bands and Channels for EEG-based Emotion Recognition with Deep Neural Networks. *Trans Auton Ment Dev* 7, 3 (2015), 162–175. doi:10.1109/TAMD.2015.2431497

[325] Yu Zhong and Yunbin Deng. 2015. A Survey on Keystroke Dynamics Biometrics: Approaches, Advances, and Evaluations. In *Gate to Computer Science and Research*. Number 1. Science Gate Publishing P.C., 1–22. doi:10.15579/gcsr.vol2.ch1

[326] Mohammad Zohaib. 2018. Dynamic Difficulty Adjustment (DDA) in Computer Games: A Review. *Advances in Human-Computer Interaction* 2018 (Nov. 2018), 1–12. doi:10.1155/2018/5681652