Ann-Kathrin Freiberg

Lebenderkennung – Schutz für die biometrische Identität

Lebenderkennung erkennt die Lebendigkeit einer Person – oder? Nicht ganz. Der auch als Presentation Attack Detection (PAD) bezeichnete Mechanismus schützt biometrische Systeme vor Betrug. Nicht die Lebendigkeit wird also geprüft, sondern die Echtheit von biometrischen Merkmalen, wie einem Gesicht.

1 Präsentationsangriffe in der Gesichtserkennung

Aufgrund der Allgegenwärtigkeit von Kameras, der Intuitivität des Fotografierens und aus hygienischen Gründen ist die Gesichtserkennung heute ein weit verbreiteter biometrischer Ansatz. Mittels Gesichtserkennung kann zudem eine effektive digitale Ausweisbesitzprüfung stattfinden. Gesichtserkennungssysteme sind jedoch auch anfällig für Angriffe durch unechte oder manipulierte Gesichter. Im Gegensatz zu Handvenenabdrücken oder Tastendruckverhalten sind Gesichtsbilder von Personen online verfügbar. Videos in guter Qualität können leicht unwissentlich erhalten werden. Mit etwas Aufwand und Können kann sogar ein 3D-Druck erstellt werden, um die Gesichtszüge einer Person vorzutäuschen.

Eine der Herausforderungen für biometrische Erkennungssysteme ist also immer noch die betrügerische Identität durch nachgeahmte körperliche Merkmale. Dies wird als Präsentations- oder Spoofing-Angriff bezeichnet. Dabei präsentiert jemand beispielsweise beim Login mit Gesichtserkennung statt des eigenen Gesichtes ein Video auf seinem Handy und versucht so, sich Zugang zu einem fremden Konto zu verschaffen.

Präsentationsangriffe können mit verschiedenen Materialien durchgeführt werden, in 2D und 3D, statisch oder bewegt bzw. animiert.

Einige Beispiele finden sich im Folgenden:

- 2D-Fotos mit hochauflösenden Gesichtsbildern auf Flachpapier.
- Bildaustausch mit mehreren 2D-Fotos in Folge.
- 2D-Ausschnitte und Papiermasken, z. B. mit Löchern.
- 3D-Papiermasken.
- Videos auf verschiedenen Displays.
- Projektionen auf verschiedene Materialien.
- 3D-Drucke, Wachsköpfe oder Skulpturen.
- 3D-Masken aus Harz, Latex oder Silikon mit Löchern für Augen, Mund oder andere Bereiche.
- Deepfakes, digitale Doubles oder Avatare.

Abbildung 1 | Beispiele von Präsentationsangriffen in der Gesichtserkennung

PAD bzw. Lebenderkennung ist ein Mechanismus, der verhindert, dass die aufgezeigten künstlichen Artefakte biometrische Erkennungssysteme täuschen. So vielfältig die Angriffsszenarien sind, so umfassend muss auch die Lebenderkennung gestaltet werden. Erst wenn verschiedenste Sicherheitsmerkmale geprüft wurden, kann ein PAD-Mechanismus entscheiden, ob die eingegangenen biometrischen Merkmale von einer echten Person vor der Kamera stammen.

Ann-Kathrin Freiberg

Manager Business Development und Marketing, BioID GmbH, Nürnberg

E-Mail: A.Freiberg@bioid.com

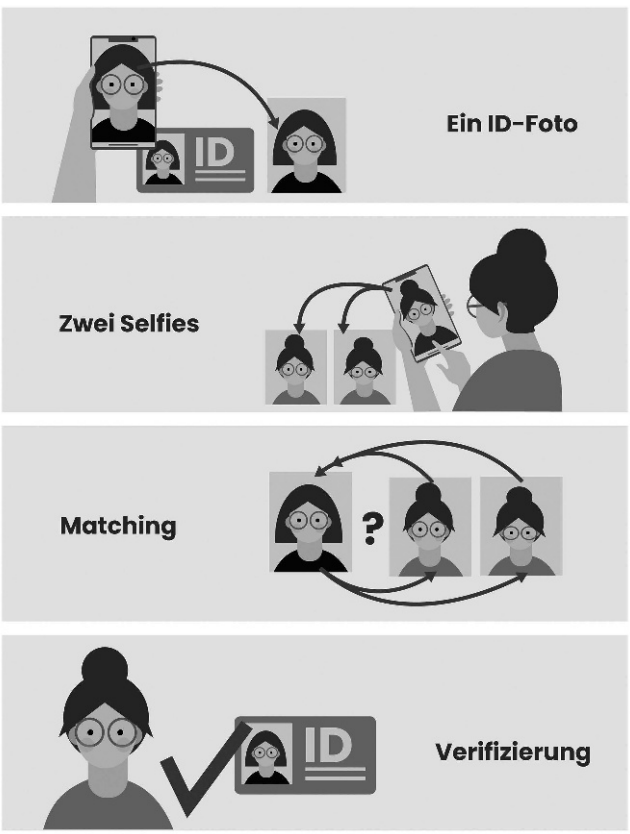
Neben dem vorangegangenen Überblick von Präsentationsangriffen in der Gesichtserkennung wird im Folgenden die Notwendigkeit von Lebenderkennungstechnologien in der Praxis aufgezeigt. Anschließend erläutert dieser Artikel, welche Techniken für PAD zum Einsatz kommen. Auch relevante Standards wie ISO 30107 werden erwähnt. Schließlich folgt ein Einblick in die Zukunft des längst nicht abgeschlossenen Forschungsfeldes der Lebenderkennung.

2 PAD in der Praxis

Nicht zuletzt durch COVID-19 sind digitale Angebote von Regierungen und Unternehmen heute weit verbreitet. Bankkonten können vollständig digital eröffnet werden, wobei Bankmitarbeiter an diesem Prozess kaum noch oder gar nicht beteiligt sind. Um in diesem Kontext die Identität einer Person festzustellen, wird häufig Biometrie verwendet. So ist der Gang zur Bank- oder Postfiliale Geschichte, bei dem man seinen Ausweis vorzeigen und anschließend auf die tatsächliche Eröffnung des Bankkontos warten musste.

Stattdessen bieten eine Vielzahl von Identitätsprovidern inzwischen entsprechende online Anwendungen oder Apps. Diese benötigen zur geldwäschegesetzkonformen Identitätsprüfung lediglich ein Foto der Person sowie ihres Ausweises. Die Fotos werden mit biometrischen Verfahren vollautomatisch auf ihre Echtheit und Übereinstimmung überprüft[1].

Abbildung 2 | Funktionsweise von BioID PhotoVerify zur automatischen Ausweisbesitzprüfung mit Lebenderkennung



Diese kritischen Prozesse unterliegen höchsten Sicherheitsstandards. Doch der Erfindergeist von Kriminellen kennt keine Grenzen: Angefangen bei Fotos eines Familienmitglieds oder einem aus Social Media gestohlenen Video über aufwändige 3D Papiermasken bis hin zu professionell gefertigten Silikonmasken, alles wird getestet.

Gegen Betrüger wird deshalb eine spezielle Technologie eingesetzt: PAD verhindert im Rahmen der vollautomatischen Authentifizierung Identitätsdiebstahl, Geldwäsche, Datenmissbrauch und unzulässigen Zugriff auf Konten oder Informationen. Auch zur Unterstützung der Entscheidungsfindung von menschlichen Prüfern wird Lebenderkennung herangezogen. Denn viele Manipulationen, beispielsweise Deepfakes, sind mit dem bloßen Auge nicht zu erkennen.

Weitere Einsatzgebiete von Lebenderkennung[2]:

- Digitale Identitätsprüfung zur Nutzung von Regierungsdiensten
- Authentifizierung von Mitarbeitern im Home Office
- Physischer Zugang zu Gebäuden mittels Gesichtserkennung
- Sicherung des Logins zu Mitgliederbereichen oder Konten
- Prüfung von Foto- und Videomaterial zur Gerichtsverwertbarkeit

3 Exkurs: Deepfakes

Deepfakes sind durch KI manipuliertes Foto- oder Videomaterial[3]. So werden einem Worte in den Mund gelegt oder man wird bei Aktionen gezeigt, die man nie getätigt hat. Potenziell kann jeder, der entsprechendes Trainingsmaterial besitzt, solche Manipulationen in mehr oder weniger guter Qualität erstellen. Hierfür gibt es beispielsweise Apps wie Avatarify oder MyHeritage.

Obwohl sie als weiterer Ansatz für den Diebstahl digitaler Identitäten eingestuft werden können, sind sie als Präsentationsangriff einem normalen Video gleichzustellen. Schließlich müssen auch sie auf einem Display präsentiert werden. Unabhängig von der Qualität der Deepfakes werden sie folglich als Fälschung erkannt, wenn sie einem biometrischen Sensor wie einer Kamera vorgehalten werden.

4 Wie Lebenderkennung funktioniert

Ohne PAD/Lebenderkennung ist es einem Gesichtserkennungssystem unmöglich, selbst die einfachsten Spoofing-Angriffe abzuwehren, die ein Mensch leicht erkennen würde. Denn die Aufgabe der Gesichtserkennung ist der reine Abgleich von Merkmalen hinsichtlich ihrer Übereinstimmung. Wird also ein Foto der Person genutzt, dem ein Bankkonto gehört, muss nicht die Gesichtserkennung diesen Betrugsversuch ablehnen, sondern die Lebenderkennung.

Nicht nur die Dreidimensionalität der eingehenden biometrischen Merkmale wird dabei geprüft. Auch die Abwesenheit verräterischer Artefakte wie dem Moiré-Effekt ist entscheidend. Diese entstehen unter anderem, wenn ein Display abgefilmt wird.

1 URL: https://www.bioid.com/identity-proofing-photoverify

2 URL: https://www.bioid.com/liveness-detection

3 URL: https://www.bioid.com/blog/2022/03/deepfakes-in-biometrics

Lebenderkennung basiert heute zum Großteil auf Künstlicher Intelligenz. Dennoch können auch klassische Methoden eingesetzt werden, um die Sicherheit zusätzlich zu erhöhen.

Folgende Techniken werden in verschiedenen Abwandlungen und Kombinationen zur Erkennung von Fälschungen genutzt[4,5]:

- Künstliche Intelligenz (KI): DCNNs (Deep Convolutional Neural Networks) klassifizieren Fotos hinsichtlich der Echtheit ihrer Quelle. DCNNs werden mit großen Mengen dedizierter Daten trainiert, um Präsentationsangriffe wie 3D-Papier- und Silikonmasken, Videos auf Displays, Videoprojektionen auf verschiedene Materialien usw. zu erkennen. Diese Methode ist abhängig von der Qualität und Vielfältigkeit des Trainingsmaterials, bringt jedoch die vielversprechendsten Ergebnisse für PAD.
- Bewegungsbasierte Analyse: z. B. Verwendung der Optischen-Fluss-Analyse (engl. optical flow) zur Berechnung der 3D-Bewegung aus zwei aufeinanderfolgenden 2D-Bildern. Augenzwinkern oder Lächeln sind weitere Beispiele der bewegungsbasierten Lebenderkennung. Diese Analyse verhindert 2D-Spoofing-Angriffe wie gedruckte Fotos, zweidimensionale Masken mit Ausschnitten, usw.
- Bildforensik: Klassische Methoden der Bildforensik können verwendet werden, um über die Quelle der biometrischen Merkmale zu entscheiden. Eine kopierte oder manipulierte Version eines Gesichts unterscheidet sich in bestimmten Eigenschaften von einem echten Gesicht. Dieser Unterschied kann ausgenutzt werden, um echte biometrische Merkmale zu erkennen.
- Challenge-Response[6]: Der Benutzer kann beispielsweise angeleitet werden, seinen Kopf auf eine bestimmte, zufällige Weise zu drehen. Die Richtungsanalyse und die Interaktion mit dem Benutzer verhindern, dass vorab aufgezeichnete Videos, 3D-Avatare oder Deepfakes die Lebenderkennung passieren. Je nach benötigtem Sicherheitsniveau kann die Anzahl der „Challenges“ erhöht werden.

Es sei erwähnt, dass die oben genannten Techniken sogenannte Software-basierte Lösungen darstellen. Im Gegensatz dazu nutzen z. B. iPhones mit Gesichtserkennung spezielle 3D Kameras zur Lebenderkennung. Diese Hardware-basierte Methode ist ebenfalls effektiv, um Präsentationsangriffe abzuwehren. Jedoch ist eine solche 3D Kamera kostspielig und nicht in jedem Endgerät verfügbar.

Bei der digitalen Identitätsprüfung, einer der größten Anwendungsbereiche der Gesichts- und Lebenderkennung, nutzen die Anwender ihre eigenen Endgeräte, deren Art, Alter und Ausstattung sich stark unterscheiden. Somit muss für die Anwendung auf Software-basierte Lösungen zurückgegriffen werden. Da die Nutzer zudem ohne weitere Anleitung fähig sein müssen, die Lebenderkennung durchzuführen, ist es wichtig, dass diese möglichst einfach und schnell funktioniert.

Für die Lebenderkennung der BioID GmbH[7], einem Nürnberger Hersteller von Gesichtserkennung, wird der Nutzer beispielsweise lediglich gebeten, leicht zu nicken. Dabei werden zwei Fotos mit leicht veränderter Position des Gesichtes aufgenommen und hinsichtlich Dreidimensionalität und Echtheit geprüft. BioID kombiniert dabei klassische Optischer-Fluss-Analysen mit modernster KI-Technologie und bestimmt in Echtzeit, ob ein biometrisches Merkmal vertrauenswürdig ist[8].

Abbildung 3 | Funktionsweise der BioID Lebenderkennung

Als Branchenpionier begann die BioID die Entwicklung der Gesichtslebenderkennung bereits im Jahr 2000. Das erste entsprechende Patent wurde 2004 eingereicht. Heute wird die deutsche Software international genutzt, um digitale Identitätsprüfung und biometrische Authentifizierung abzusichern.

Für Interessierte gibt es auf dem BioID Playground[9] die Möglichkeit, die Lebenderkennung kostenfrei zu testen.

5 ISO-Standard

Der internationale PAD-Standard ISO/IEC 30107[10] definiert die Kriterien für die Konformität eines Lebenderkennungssystems. Für eine objektive Bewertung der Lebenderkennung werden biometrische Prüflabore wie die TÜV Informationstechnik GmbH[11] herangezogen. Auch FIDO-Zertifizierungen für biometrische Komponenten testen PAD im Rahmen der Prüfung von

4 Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., & Busch, C. (Eds.). (2022). Handbook Of Digital Face Manipulation And Detection: From DeepFakes to Morphing Attacks. Cham, Switzerland: Springer.

5 Marcel, S., Nixon, M. S., Fierrez, J., & Evans, N. (Eds.). (2019). Handbook of biometric anti-spoofing: Presentation attack detection (Vol. 2). Cham, Switzerland: Springer.

6 Frischholz, R., & Werner, A. (2003). Avoiding replay-attacks in a face recognition system using head-pose estimation. 2003 IEEE International SOI Conference. Proceedings (Cat. No.03CH37443), 234-235.

7 URL: https://www.bioid.com

8 URL: https://www.bioid.com/liveness-detection

9 URL: https://playground.bioid.com

10 URL: https://www.iso.org/standard/67381.html

11 URL: https://www.tuvit.de/de/ueber-uns/referenzen

Springer

Highlight

T. Hess
Digitale Transformation strategisch steuern
Vom Zufallstreffer zum systematischen Vorgehen
2019, XII, 216 S. 37 Abb., 1 Abb. in Farbe. Book + eBook. Geb.
€ (D) 24,99 | € (A) 25,58 | *sFr 27,00
ISBN 978-3-658-24474-3
€ 19,99 | *sFr 21,50
ISBN 978-3-658-24475-0 (eBook)

- Ein Leitfaden für Unternehmen zum richtigen Umgang mit der digitalen Transformation
- Enger Bezug zu neusten wissenschaftlichen Erkenntnissen

Ihre Vorteile in unserem Online Shop:
Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar | Kostenloser Versand für Printbücher weltweit

€ (D) sind gebundene Ladenpreise in Deutschland und enthalten 7 % für Printprodukte bzw. 19 % MwSt. für elektronische Produkte. € (A) sind gebundene Ladenpreise in Österreich und enthalten 10 % für Printprodukte bzw. 20% MwSt. für elektronische Produkte. Die mit * gekennzeichneten Preise sind unverbindliche Preis-empfehlungen und enthalten die landesübliche MwSt. Preisänderungen und Irrtümer vorbehalten.

Part of SPRINGER NATURE

springer.com/dts

A70439

Gesichtserkennungssystemen gemäß den Standards ISO 19795 und ISO/IEC 30107.

Reine Zertifizierungen für Lebenderkennung gibt es derweil nicht. Unternehmen können stattdessen ihre Konformität mit dem ISO-Standard für PAD prüfen lassen[12].

6 Ausblick: Das Wettrüsten

Die Herausforderung bei der Entwicklung von Lebenderkennung ist, dass die Technologie höchst zuverlässig und dabei so bequem wie möglich nutzbar sein muss. Zudem eröffnet der technische Fortschritt nicht nur jenen, die Spoofing Angriffe aufspüren, neue Möglichkeiten. Beispielsweise brauchte man neben Fachkenntnis noch vor wenigen Jahren auch Hochleistungscomputer, um einen realistischen Deepfake zu erstellen. Heute geht das in wenigen Sekunden mit einer kostenfreien App auf einem handelsüblichen Smartphone.

Das Wettrüsten gewinnt folglich an Tempo: Während Betrüger ständig neue Spoofing-Methoden entwickeln, wirken Biometrie-Anbieter wie BioID sowie internationale Forschung dem entgegen. Hierfür ist eine enge Verzahnung zwischen Wissenschaft und Praxis wichtig: Dafür sorgen beispielsweise Forschungsprojekte wie FAKE-ID, einem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Konsortium zur Erkennung von manipuliertem Bildmaterial[13].

Während Biometrie effiziente Prozesse im Rahmen der digitalen Identitätsprüfung ermöglicht, hat die Sicherheit von (digitalen) Identitäten oberste Priorität. Lebenderkennung ist und bleibt dementsprechend ein spannendes Feld, dessen Weiterentwicklung Grundlage dafür ist, dass wir auch zukünftig vor Identitätsdiebstahl und -betrug geschützt sind.

Literatur

[1] URL: https://www.bioid.com/identity-proofing-photoverify
[2] URL: https://www.bioid.com/liveness-detection
[3] URL: https://www.bioid.com/blog/2022/03/deepfakes-in-biometrics
[4] Rathgeb, C., Tolosana, R., Vera-Rodriguez, R., & Busch, C. (Eds.). (2022). Handbook Of Digital Face Manipulation And Detection: From DeepFakes to Morphing Attacks. Cham, Switzerland: Springer.
[5] Marcel, S., Nixon, M. S., Fierrez, J., & Evans, N. (Eds.). (2019). Handbook of biometric anti-spoofing: Presentation attack detection (Vol. 2). Cham, Switzerland: Springer.
[6] Frischholz, R., & Werner, A. (2003). Avoiding replay-attacks in a face recognition system using head-pose estimation. 2003 IEEE International SOI Conference. Proceedings (Cat. No.03CH37443), 234-235.
[7] URL: https://www.bioid.com
[8] URL: https://www.bioid.com/liveness-detection
[9] URL: https://playground.bioid.com
[10] URL: https://www.iso.org/standard/67381.html
[11] URL: https://www.tuvit.de/de/ueber-uns/referenzen
[12] URL: https://www.bioid.com/blog/2020/06/liveness-detection-certification
[13] URL: https://www.sifo.de/sifo/shareddocs/Downloads/files/projektumriss_fake_id

12 URL: https://www.bioid.com/blog/2020/06/liveness-detection-certification
13 URL: https://www.sifo.de/sifo/shareddocs/Downloads/files/projektumriss_fake_id