Technische Hochschule Brandenburg

IT Sicherheit
Informatik und Medien
Biometrie – Dr. Tobias Scheidat

Teamaufgabe: Offline Handschrift

Wintersemester 2024
Abgabetermin 15. Januar 2025

Tobias Ende – Matr-Nr. 939628
Timo Schwabe – Matr-Nr. 20229002
Conrad Ferneding – Matr-Nr. 20226863
Mara Schulke – Matr-Nr. 20215853

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einleitung

Die Verwendung von biometrischen Verfahren ist nicht neu und findet in vielen Bereichen bereits Anwendung. Die Handschrift-Biometrie ist im Rahmen einer solchen Arbeit leicht und ohne technische Hilfsmittel realisierbar. Daher eignet sie sich gut für eine Analyse. Da die Analyse wie beispielsweise die Berechnung der Equal Error Rate (EER) bei jedem biometrischen Verfahren gleich ist, lässt sich so übertragbares Wissen aufbauen.

In dieser Arbeit soll die Handschrift-Biometrie näher betrachtet werden. Die Probanden sollen die Verifikations- und Enrollmentdaten für zwei Semantiken erstellen und erfassen. Aus den Daten ergibt sich für jeden Probanden eine Streumatrix.

Das Kernziel der Arbeit ist es, die erfassten Daten zu analysieren. Es werden wichtige Kennwerte wie die EER ermittelt. Anschließend sollen diese Zahlen interpretiert und diskutiert werden. Durch die Betrachtung von verschiedenen Fälschungen soll eine Aussage über die Sicherheit des Systems getroffen werden. Abschließend sollen Voraussetzungen definiert werden, wie ein System, dass Handschrift-Biometrie verwendet, gestaltet werden soll.

Zuerst werden im Kapitel Grundlagen die wichtigsten Begriffe, die in dieser Arbeit verwendet werden, erläutert. Anschließend wird das verwendete System zur Erfassung der Offline-Handschrift beschrieben. In der Analyse werden die verschiedenen Kennwerte der Semantiken berechnet und interpretiert. In der anschließenden Diskussion wird auf die Verwendbarkeit des Systems eingegangen. Im Kapitel der “Evaluation durch gezielte Angriffe” werden verschiedene Angriffe durch Fälschungen beschrieben und in den Kontext der Handschrift-Biometrie gesetzt. Die letzten beiden Kapitel befassen sich mit der Beschreibung des Systems aus technischer Sicht und verschiedenen Voraussetzungen, die für eine Handschrift-Biometrie zu treffen sind.

2 Grundlagen

Um ein biometrisches System aufzustellen und anschließend bewerten zu können, sollen in diesem Kapitel grundlegende Begriffe der Biometrie geklärt werden. Außerdem werden das biometrische System und die Modalität vorgestellt, die von diesem verwendet werden.

2.1 Definitionen

- Die False Rejection Rate (FRR) beschreibt die Anzahl der Versuche, bei denen ein Benutzer von einem Authentifizierungssystem fälschlicherweise abgelehnt wurde.
- Die Intra-Klassen-Varianz beschreibt die Variabilität der Merkmale für dieselbe Person. Ein biometrisches System strebt eine geringe Intra-Klassen-Varianz an, da dies den Wiedererkennungswert einer Person erhöht. Eine geringe Intra-Klassen-Varianz führt zu einer niedrigen FRR.
- Die False Acceptance Rate (FAR) ist der Gegensatz der FRR und beschreibt die Anzahl der Versuche, bei denen ein Nutzer fälschlicherweise angenommen wurde.
- Die Inter-Klassen Varianz beschreibt die Variabilität der Merkmale zwischen verschiedenen Nutzern. Eine hohe Inter-Klassen-Varianz bedeutet eine hohe Unterscheidbarkeit zwischen verschiedenen Personen. Eine hohe Inter-Klassen-Varianz führt zu einer geringen FAR.
- Die Equal Error Rate (EER) beschreibt die Leistung eines biometrischen Systems und ist der Punkt, an dem die FRR und FAR gleich sind. Die EER ist ein Schwellenwert für die Differenzen der Enrolment- gegen Verifikationswerte. Ein niedrigerer Schwellenwert würde

eine höhere FRR bedeuten, weil legitime Benutzer häufiger abgelehnt werden. Ein höherer Schwellenwert würde eine höhere FAR bedeuten, weil unberechtigte Benutzer häufiger fälschlicherweise akzeptiert werden. Ein "gutes" biometrisches System versucht daher, die ERR an einen Punkt zu setzen, an dem sowohl FRR als auch FAR möglichst gering sind.

2.2 Das biometrische System dieser Arbeit

Das biometrische System, das in dieser Arbeit betrachtet werden soll, nutzt die Modalität der Offline-Handschrift. Bei dieser Modalität werden biometrische Merkmale aus Schriftsätzen extrahiert, ohne die aktiven Merkmale zu betrachten, die beim Schreiben entstehen.

Die Phase der Datenerhebung umfasst für diese Arbeit vier Probanden, welche jeweils Enrolment- und Verifikationsdaten für zwei Semantiken ablegen. Für die erste Semantik (Semantik A) schreibt jeder Proband fünf Mal "78402" und liest die entstandenen biometrischen Merkmale ab, um sich für das System zu registrieren. Anschließend wird dieselbe Zahlenfolge weitere fünf Mal aufgeschrieben, um die Verifikation des Systems zu testen. Die Differenz der Enrolment- und Verifikationsdaten wird durch den euklidischen Abstand mit 7-Dimensionen berechnet. Letztlich wird dasselbe Vorgehen für eine weitere Semantik (Semantik B) wiederholt, bei der der Schriftzug der Probanden, dessen Geburtsort ist. Da die erste Semantik einen Schriftzug aus Zahlen beschreibt, welcher für alle Probanden gleich ist, und die zweite Semantik einen individuellen Schriftzug, werden sich die Ergebnisse gut in der Interpretation analysieren lassen.

Bei den sieben erwähnten Merkmalen handelt es sich um die folgende Liste:

- Breiten- und Höhenverhältnis
- Anzahl der kontinuierlich verbundenen Linienabschnitte (Segmentzahl)
- Grundlinien-Winkel
- Schleifenanzahl
- Gesamtzahl der lokalen X-Werte
- Gesamtzahl der lokalen Y-Werte
- Anzahl der Kreuzungspunkte

Für jeden Probanden entstehen durch dieses System (5x7)-Enrolment-Matrizen. Im Vergleich mit je vier (7x5)-Verifikations-Matrizen wird dadurch eine (20x20) Streumatrix entstehen. Die folgende Tabelle wird diese Streumatrix skizzieren. Die blau markierten Bereiche stellen die Intra-Klassen-Distanzwerte dar, während die roten Bereiche die Inter-Klassen-Distanzwerte darstellen.

	Proband 1 Ver.	Proband 2 Ver.	Proband 3 Ver.	Proband 4 Ver.
Proband 1 Enr.	Intra P1	Inter P2xP1	Inter P3xP1	Inter P4xP1
Proband 2 Enr.	Inter P1xP2	Intra P2	Inter P3xP2	Inter P4xP2
Proband 3 Enr.	Inter P1xP3	Inter P2xP3	Intra P3	Inter P4xP3
Proband 4 Enr.	Inter P1xP4	Inter P2xP4	Inter P3xP4	Intra P4

3 Auswertung des biometrischen Systems Offline-Handschrift

Dieses Kapitel wird sich mit der Interpretation des beschriebenen biometrischen Systems beschäftigen. Um das System zu bewerten, wird die resultierende EER diskutiert werden.

Wie zuvor beschrieben hängt die Leistung eines biometrischen Systems von der EER ab. Eine niedrige EER deutet auf ein genaues biometrisches System, da hier die Anzahl der Fehler - sowohl für legitime, als auch unberechtigte Nutzer - niedriger ist.

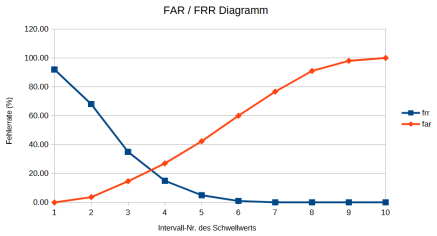

Abbildung 1: Semantik A - FAR/FRR

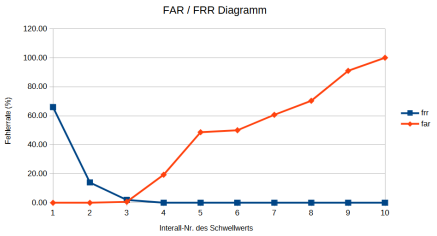

Abbildung 2: Semantik B - FAR/FRR

Die EER der ersten Semantik beträgt $\approx 22\%$, und ist in Abbildung 1 zu sehen. Die EER aus der zweiten Semantik $\approx 2\%$ beträgt und ist in Abbildung 2 zu sehen. Dass die EER der ersten Semantik höher als die der zweiten Semantik ist, war zu erwarten. Bei der ersten Semantik wurden dieselben Schriftzüge geschrieben und bei der zweiten Semantik unterschiedliche. Die Merkmalsextraktion bei gleichen Texten lassen weniger Unterschiede zu. Da es sich zudem um Zahlen handelte, bei denen z.B. Segmentierung und Schleifen nur begrenzt individualisierbar sind, fallen die FAR und die FRR insgesamt höher aus. Wie bereits aus der Beschreibung der Semantiken deutlich wird, handelt es sich bei diesen Diagrammen um einen "Zero-Effort" Fälschungs-Test. (Die Frage, ob diese Semantik bereits als blinde Fälschung betrachtet werden kann, wird in späteren Kapiteln diskutiert.)

Generell gibt es keinen Standard, welcher die Sicherheit eines biometrischen Systems anhand dessen EER-Wertes bewerten kann. Im Zuge dieser Betrachtung wird eine EER von $x < 1\%$ als sicher angesehen, während eine EER von $1\% <= x <= 5\%$ als ausreichend betrachtet werden kann. Eine EER von 5% wäre somit ausreichend sicher, sollte allerdings nicht in sicherheitskritischen Anwendungen genutzt werden. Solche Systeme würden den Komfort des Nutzers über die Sicherheit seiner Daten stellen, da weniger fehlerhafte Ablehnungen auftreten bzw. mehr fehlerhafte Anmeldungen zugelassen werden. In einem solchen System würden zwei von 100 Versuchen für einen ratenden Angreifer statistischen Erfolg versprechen (FAR). Bei Semantik A melden sich alle Nutzer mit demselben Schriftzug an (Enrollment) und erzielen eine 10-Mal höhere EER von 22%.

Diese ist größer als die bereits hohe EER von 2% und dadurch ebenfalls für ein sicherheitskritisches System ungenügend. Dadurch, dass bei Semantik A jede Person denselben Schriftzug verwendet, kann die resultierende EER als die Genauigkeit der genutzten Merkmale (bei Zahlen) betrachtet werden. Es ist anzunehmen, dass ein Schriftzug aus Buchstaben die EER für Semantik A senken würde. Zusätzlich muss an dieser Stelle angemerkt werden, dass lediglich vier Probanden für die Datenerhebung genutzt wurden, wodurch die Wirksamkeit dieses biometrischen Systems nicht final widerlegt werden kann.

Der Wertebereich der Differenzen der Verifikationen zu den Referenzen ist bei Semantik A kleiner als bei der Semantik B. Bei Semantik A liegen alle Distanzen im folgenden Bereich:

$$1,00 <= x <= 10,96$$

Für die Semantik B liegen alle Distanzen im folgenden Bereich:

$$0,31 <= x <= 22.09$$

Die Distanzen des Wertebereichs der Semantik A fallen kleiner aus, wodurch unterschiedliche Personen eine größere Wahrscheinlichkeit haben, in einen ähnlichen Wertebereich zu fallen. Ähnlichkeiten der Wertebereiche individueller Personen führen zu einer geringeren euklidischen Distanz. Dieser Zusammenhang führt bei Semantik 1 zu einer erhöhten EER. Es ist anzunehmen, dass ein Test mit mehr als vier Probanden den finalen Wertebereich vergrößern würde, da extremere Relationen zwischen biometrischen Merkmalen auftreten könnten. Ein solcher Test könnte wegen des beschriebenen Zusammenhangs die EER senken.

Bei der Betrachtung der Distanzwerte der FRR- (Intra-Klassen-) Matrizen wird klar, dass nicht alle euklidischen Distanzen auf ähnlichem Level gering sind. Es gibt einzelne Ausnahmen, wie z.B. einen Intra-Klassen-Wert von $6,95$ in der Semantik A, welcher die höchste Distanz zum Enrolment aufweist. Ein solch hoher Wert wird auch mit höheren Schwellwerten noch abgewiesen. Neben einzelnen Ausnahmen lassen sich durch die FRR-Tabelle auch Personen nachweisen, die einen inkonsistenten Schreibstil haben. So hat Proband 1 überwiegend Distanzen im Bereich von $3,29 <= x <= 4,39$, während Proband 4 ausschließlich Werte unter $3,29$ aufweist. Proband 1 hat einen ungleichmäßigeren Schreibstil als Proband 4, was zu einer höheren Rate an fehlerhaften Ablehnungen führt. Diese Inkonsequenz im Schreibstil führt dazu, dass die FRR-Kurve der ersten Semantik nicht typisch logarithmisch geformt ist, sondern zusätzlich einen Wendepunkt hat

Die Inkonsequenz im Schreibstil lässt sich auch in der zweiten Semantik finden. Allerdings hat diese keine Auswirkungen auf diese (wie zuvor festgestellt bessere) Semantik, da der Wertebereich größer ist. Durch diese Reichweite fallen die unterschiedlichen Werte in denselben Intervall, wodurch der Unterschied im Diagramm nicht sichtbar wird.

Bei der Betrachtung der FAR- (Inter-Klassen-) Matrizen zeigt sich, dass die festgestellten inkonsistenten Schreibstile, scheinbar keine/wenig Auswirkung auf die FAR-Werte haben. Denn obwohl Person 1 in beiden Semantiken eine höhere Anzahl an fehlerhaften Ablehnungen aufweist als Person 4, hat Person 4 eine höhere Anzahl an fehlerhaften Anmeldungen. Werte im höheren Bereich bei der FRR, schließen somit nicht auf mehr fehlerhafte Anmeldungen / ein leichteres Ziel für einen Angriff.

Zusätzlich wird klar, dass sich einige Personen biometrisch ähnlicher sind als andere. So hat Person 2 in Semantik B mit keiner anderen Person eine Distanz, die kleiner als $13,67$ ist. Im Gegensatz dazu hat Person 1 zu Person 3 und 4 nie eine Distanz, welche größer als 10,28 ist. Dadurch ergeben sich für Person 1 (im Vergleich zu Person 3 und 4) ausschließlich fehlerhafte Anmeldungen in einem Bereich / mit einem Schwellwert, der für Person 2 keinen einzigen ergibt. Das Schriftbild von Person 2 ist somit unähnlich dem, von allen anderen. Im Gegensatz dazu sind sich die Merkmale der Personen 1, 3 und 4 ähnlicher. Bei Semantik A und B ergibt sich durch die biometrische Unähnlichkeit des Schriftbildes von Person 2 zu allen anderen für die FAR ebenfalls keine logarithmische, sondern ebenfalls eine Kurve mit Wendepunkt. Die Distanzen liegen vermehrt in höheren Intervallen, wodurch die Kurve für die restlichen Werte abflacht.

4 Evaluation durch gezielte Fälschungen

4.1 Entwicklung der Testprotokolle

Die Entwicklung eines Testprotokolls für Fälschungsszenarien sollte derart gestaltet werden, dass alle relevanten Szenarien systematisch abgedeckt werden. Zunächst sollten Intra-Klassen Tests durchgeführt werden. Diese Tests prüfen, wie gut das biometrische System in der Lage ist, authentische Proben einer Person korrekt zu erkennen. Dabei werden Verifikationsproben mit den Enrolment-Daten derselben Person abgeglichen. Das Ziel dieser Tests ist die Bestimmung der False-Non-Match-Rate (FNMR), welche die Häufigkeit beschreibt, mit der authentische Proben fälschlicherweise abgelehnt werden.

Zusätzlich sollten Inter-Klassen Tests mit verschiedenen Angriffsstärken berücksichtigt werden, um die Robustheit des Systems gegen Fälschungsversuche zu evaluieren. Diese Tests umfassen:

- Blind-Force Angriffe: Bei dieser Angriffsstärke versucht der Angreifer, eine biometrische Probe zu fälschen, ohne Kenntnisse über das Schriftbild oder den Prozess, der zur Erstellung der authentischen Probe geführt hat.
- Low-Force Angriffe: Hier hat der Angreifer Zugang zu einem sichtbaren Ergebnis, wie beispielsweise einer Unterschrift, und versucht, dieses nachzuahmen. Es besteht jedoch kein Wissen über den dahinterliegenden Erstellungsprozess, wie etwa Geschwindigkeit, Druck oder Reihenfolge der Bewegungen.

4.2 Erstellung gezielter Fälschungsdaten

Zur Erstellung gezielter Fälschungsdaten müssen spezifische Angriffstypen berücksichtigt werden, um die Robustheit des biometrischen Systems unter realistischen Bedingungen zu bewerten. Bei den Blind-Force Daten handelt es sich um Proben, die ohne jegliche Kenntnis des Originals erstellt werden. Der Angreifer versucht, das System zu täuschen, ohne eine Vorlage oder Informationen über das authentische Schriftbild oder den Schreibprozess zu haben. Bei Low-Force Daten werden auf Grundlage eines sichtbaren Endergebnisses, wie beispielsweise einer Unterschrift, erstellt. Dabei hat der Angreifer keine Kenntnis über den eigentlichen Schreibprozess, wie etwa Bewegungsdynamiken, Geschwindigkeit oder Druck.

4.3 Implementierung und Durchführung

Zur Implementierung und Durchführung von Tests sollten mehrere Szenarien berücksichtigt werden, um die Leistungsfähigkeit und Sicherheit des biometrischen Systems zu bewerten. Für den Verifikationstest (Intra-Klassen-Test) werden authentische Proben mit den Enrolment-Daten der gleichen Person abgeglichen. Ziel dieses Tests ist die Messung der False-Non-Match-Rate (FNMR) oder False-Rejection-Rate (FRR), die die intraindividuelle Fehlklassifikation darstellt. Die zuvor erstellten Fälschungsproben werden gegen die Enrolment-Daten der angegriffenen Personen geprüft. Ziel dieser Tests ist die Messung der False-Match-Rate (FMR) oder False-Acceptance-Rate (FAR) für die jeweiligen Angriffsszenarien (FMRBlind, FMRLow-Force).

4.4 Analyse der Ergebnisse

Zur Bewertung der Testergebnisse werden folgende Punkte analysiert. Der Punkt, an dem die False-Match-Rate (FMR) und die False-Non-Match-Rate (FNMR) gleich sind ist die Equal-Error-Rate (EER). Für die Angriffsszenarien Blind und Low-Force wird jeweils eine separate EER berechnet, um die Robustheit des Systems gegenüber unterschiedlichen Angriffsstärken zu bewerten. Durch den Vergleich der Fehlerraten wird dann analysiert, wie sich die Falscherkennungsraten zwischen Blind- und Low-Force-Angriffen verändern. Ein Anstieg der FMR von Blind- zu Low-Force-Angriffen kann auf Schwachstellen im System hinweisen.

4.5 Bewertung und Optimierung des Systems

Auf Grundlage der Testergebnisse können gezielte Maßnahmen zur Verbesserung des biometrischen Systems ergriffen werden. Zum einen kann eine Verbesserung der Algorithmen vorgenommen werden. Es sollten spezifische Fälschungserkennungsmethoden entwickelt werden, die gezielt

auf die Schwachstellen des Systems bei Blind- und Low-Force-Angriffen eingehen. Außerdem kann die Systemschwelle erhöht werden. Die Anpassung der Entscheidungsschwellen kann dazu beitragen, die Falscherkennungsrate bei Angriffen zu verringern, ohne die Benutzerfreundlichkeit zu beeinträchtigen. Zuletzt können mehrere Merkmale kombiniert werden. Die Integration zusätzlicher biometrischer Eigenschaften wie Schreibdruck oder Schreibgeschwindigkeit kann die Sicherheit des Systems erhöhen und es widerstandsfähiger gegen gezielte Fälschungen machen.

4.6 Iterative Tests und Validierung

Nach der Optimierung des biometrischen Systems sollten erneut Tests durchgeführt werden, um die Wirksamkeit der vorgenommenen Anpassungen zu validieren.

- Langzeitbeobachtungen: Es ist wichtig zu überprüfen, ob die Verbesserungen des Systems über einen längeren Zeitraum hinweg stabil und nachhaltig bleiben. Dies hilft, potenzielle Schwächen oder Verschlechterungen in der Leistung frühzeitig zu erkennen.
- Cross-Validation: Die Ergebnisse sollten auf unterschiedliche Benutzergruppen und Nutzungsszenarien übertragen werden, um sicherzustellen, dass die Verbesserungen universell anwendbar sind und nicht nur unter spezifischen Bedingungen funktionieren.

Ausschluss von Zero-Effort

Ein erwähnenswerter Angriff, der aber nicht gezielt für dieses Szenario relevant ist, ist der Zero- Effort/Random-Angriff. Das ist ein Angriff, dessen Ziel es ist, ohne gezielte Fälschungen, also zufälligen Versuchen, das System zu täuschen. Ein Zero-Effort Fälschungstest ist also ein Test, bei dem zufällige Proben gegen die Enrolment-Daten anderer Personen geprüft werden. Das Ziel dieses Tests ist die Bestimmung der False-Match-Rate (FMR) oder False-Acceptance-Rate (FAR) für zufällige Übereinstimmungen.

5 Rahmenvorgaben der Datenerfassung

Insbesondere die technische Infrastruktur und die Umgebung der Erfassung der Daten müssen für alle Probanden gleich sein, um vergleichbare Resultate zu erzielen.

5.1 Umgebung

Die Schriftproben sollten so erhoben werden, dass kein anderer Proband die Erfassung beobachten kann, zum Beispiel durch einen Sichtschutz. So können Brute-Force Angriffe früh unterbunden werden.

5.2 Erfassung

Offline Handschriften können über verschiedene technische Verfahren erhoben werden. Im Folgenden werden zwei Beispiele

5.2.1 Scanner

Eine Möglichkeit bieten handelsübliche Dokumentenscanner. Sie beleuchten die Schriftprobe und erfassen das reflektierte Licht der Schrift. Wichtig hierbei ist eine hohe Auflösung des Geräts, damit das Schriftbild detailliert erfasst werden kann und auch feine Striche, kleine Punkte oder Lücken in der Schrift erkannt werden können.

Scanner haben den Vorteil, dass sie unter immer gleichen Bedingungen arbeiten. Die Beleuchtung und Auflösung ändern sich nicht. Dafür sind sie aber nicht mobil und brauchen Platz. Sie werden ungenau, wenn die Schriftproben beschädigt oder geknittert sind.

5.2.2 Digitalkameras

Alternativ können Digitalkameras zur Erfassung von Schriftproben verwendet werden. Hierbei spielt die Auflösung ebenfalls eine Rolle. Eine bessere Auflösung bietet mehr Details. Des Weiteren spielt das verwendete Objektiv eine große Rolle, um Verzerrungen zu verhindern. Der Vorteil von Digitalkameras ist, dass sie in vielen verschiedenen Größen existieren. Sie sind mobil und nicht stationär. Ein Nachteil ist, dass es schwer ist, identische Voraussetzung für die Erfassung zu gewährleisten, da Licht, Winkel und Abstand zur Schriftprobe leicht verändert werden können.

Jeder Sensor muss entsprechend kalibriert und gewartet werden, damit identische Bedingungen bei der Erfassung herrschen.

5.3 Speicherung

Eine sichere und effiziente Speicherung spielt eine tragende Rolle. Damit später eine präzise Analyse der erfassten Daten möglich ist, müssen die Rohdaten in einem verlustfreien Format gespeichert werden. Relevante Metadaten, wie Informationen zum Sensor und den Probanden sind ebenfalls zu erheben, damit bei Fehlern ein entsprechendes Troubleshooting erfolgen kann.

Da es sich um biometrische, und damit besonders schützenswerte Daten handelt, ist ein Zugriffs- und Berechtigungssystem nötig. Dadurch kann der Zugriff auf die Daten sowohl eingeschränkt, als auch nachvollzogen werden. Außerdem müssen biometrische Daten immer ausreichend verschlüsselt gespeichert und übertragen werden.

6 Protokoll für die Datenerhebung gezielter Fälschungen

6.1 Vorbereitung der Datenerhebung

6.1.1 Definition der Zielsetzung

Das Ziel dieser Datenerhebung ist die Evaluierung der Fälschungssicherheit unseres biometrischen Systems im Hinblick auf die, handschriftliche erfassten, Semantiken:

- **Semantik A**: Numerische, 5-stellige PIN (78402)
- **Semantik B**: Der Geburtsort jedes Probanden

Es wird ein besonderer Fokus auf zwei gezielte Angriffe gelegt: Blind-Force: Angriffe basierend auf visuellen Vorlagen. Low-Force: Angriffe mit Zugriff auf eine authentische Verifikationsprobe

6.1.2 Auswahl der Probanden

Idealerweise 50–100 Probanden (angenommen es handelt sich um ein echtes biometrisches System) bzw. 2-4 (in dem Rahmen dieses Moduls)

Probanden sollten ein unterschiedliches Alter, Geschlecht und einen unterschiedlichen Schreibstil haben, um eine ausreichende Intra-Class-Variabilität zu gewährleisten.

Eine schriftliche Einwilligung gemäß Datenschutzrichtlinien (z. B. DSGVO) ist einzuholen.

6.1.3 Technische Infrastruktur

Es müssen abhängig von der Probanden-Anzahl mehrere Schreibtabletts oder Touchscreens zur Datenerfassung bereitgestellt werden. Speicherung der Proben als Bild- oder Vektordaten. Umgebung: Einheitliche Bedingungen (z. B. Beleuchtung, Schreibfläche).

6.2 Durchführung der Datenerhebung

Da diese Datenerhebung ausschließlich auf gezielte Angriffe bezogen ist, werden Enrolment- und Verifikationsproben nicht erneut erhoben. Eine Variante (falls mehr authentische Probanden gefordert sind) könnte sein, diese ebenfalls zu erheben, da der logistische Aufwand fast identisch ist.

6.2.1 Erhebung der Fälschungsproben

Blind-Force-Angriffe

Semantik A: Angreifer erhalten die Pin und erfassen 5 Fälschungsproben für diese
Semantik B: Angreifer erstellen für jeden authentischen Nutzer 5 Fälschungsproben

Low-Force-Angriffe

Semantik A und B: Angreifer erhalten für jeden Nutzer (4 in unserem Fall) Zugriff auf Bilder der authentischen Proben und erfassen jeweils 5 Fälschungsproben!

6.3 Verarbeitung der Daten

6.3.1 Qualitätssicherung

Semantik A: Prüfung auf numerische Vollständigkeit und Klarheit
Semantik B: Prüfung auf Lesbarkeit und Textvollständigkeit, sowie Übereinstimmung des Geburtsortes mit dem authentischen.

6.3.2 Anonymisierung

Um eine DSGVO-konforme Verarbeitung von Probandendaten zu gewährleisten, werden alle Referenzen zu personenbezogenen Daten durch pseudonymisierte IDs ersetzt. Somit lassen sich Angreifer unterscheiden, es gibt allerdings keine Möglichkeit, einen Rückschluss auf den tatsächlichen Probanden zu ziehen.

6.3.3 Datenaufteilung

Die erhobenen Daten werden in zwei Gruppen unterteilt (angenommen es handelt sich um eine große Anzahl an Probanden):

1. Trainingsdaten, die für eine weitere Systemoptimierung verwendet werden können
2. Testdaten, die für eine Evaluation des biometrischen Systems genutzt werden können

6.4 Evaluierung der Angrifftests

Um die Evaluierung des Systems gegen die zwei Arten von Angriffen durchzuführen werden sogenannte Angrifftests durchgeführt:

6.4.1 Blind-Force-Angrifftests

In den Blind-Force-Angrifftests werden:

1. In Semantik A, pro Angreifer 5 Verifikationsversuche unternommen und die FAR berechnet
2. In Semantik B, pro Nutzer 5 Verifikationsversuche unternommen und die FAR berechnet

Die unterschiedliche Natur der beiden Semantiken führt bei Blind-Force-Angriffen dazu, dass es unterschiedlich viele Angriffe für Semantik A & B gibt.

6.4.2 Low-Force-Angrifftests

In den Low-Force-Angrifftests werden:

1. In Semantik A, pro Angreifer und Proband Verifikationsversuche unternommen und die FAR berechnet
2. In Semantik B, pro Angreifer und Proband, Verifikationsversuche unternommen und die FAR berechnet

6.5 Dokumentation und Auswertung

6.5.1 Fehleranalyse

In die bestehenden Diagramme aus Aufgabe 1) für FAR/FRR können nun, für jede Semantik, zwei weitere Graphen eingezeichnet werden:

1. Blind-Force-FAR – Die Acceptance-Rate von Angreifern, die Zugriff auf das geheime Wissen (bspw. Pin/Ort respektive) hatten, aber kein Beispiel für die Handschrift hatten.
2. Low-Force-FAR – Die Acceptance-Rate von Angreifern, die Zugriff auf authentische offline Verifikationsdaten von authentischen Probanden hatten.

Des Weiteren könnte eine Fehleranalyse dieser Charakteristiken erfolgen:

1. Schriftproben haben (bspw. wie schneiden Schreibschrift vs. Druckschrift ab?)
2. Inhalte haben (bspw. wie schneiden kurze Städtenamen vs. lange ab?)

um Rückschlüsse auf das Verhalten der Merkmalsextraktion zu erhalten.

6.5.2 Berichterstellung

Wie oben bereits beschrieben, müssen Semantik A und B separat ausgewertet werden. Die eingezeichnete FAR der verschiedenen Angriffe in den Diagrammen kann daraufhin genutzt werden, um einen verbesserten Schwellwert oder Änderungen am biometrischen System vorzuschlagen.

6.5.3 Optimierung

Letztlich sollten Anpassungen des Systems vorgenommen werden, um die Robustheit gegen gezielte Fälschungen zu erhöhen. Nach erfolgten Anpassungen kann das System mit den hier erstellten Angrifftests erneut getestet und ausgewertet werden, um eine Verbesserung bzw. Verschlechterung festzustellen.