Institut für Visualisierung und Interaktive Systeme
Universität Stuttgart
Universitätsstraße 38
D–70569 Stuttgart

Studienarbeit Nr. 2393

Blickbasierte Authentifizierung – Langzeitstudie über die Erinnerungsfähigkeit an graphische Passwörter mit und ohne Saliency Mask

Mateusz Mikusz

Studiengang:	Informatik
Prüfer:	Prof. Dr. Albrecht Schmidt
Betreuer:	Dipl.-Medieninf. Florian Alt M. Sc. Stefan Schneegaß
begonnen am:	1. Juni 2012
beendet am:	1. Dezember 2012
CR-Klassifikation:	H.5.2, K.6.5

Kurzfassung

Vorgegebene graphische Passwörter, die in Form von mehreren Passwortpunkten auf einem Bild definiert wurden, haben großes Potenzial für ein sicheres und benutzbares Authentifizierungssystem. Insbesondere, wenn die graphischen Passwörter auf Bildern mit Saliency Mask definiert wurden, die dazu dienen, dass Passwortpunkte nicht in einfach hervorsagbare bzw. in oft genutzte Bereiche gesetzt werden können, steigt die Sicherheit solcher graphischen Passwörter. Im Rahmen dieser Studienarbeit wurde in einer mehrwöchigen Studie untersucht, welchen Einfluss die Saliency Maks auf die Erinnerungsfähigkeit auf die jeweils darauf definierten graphischen Passwörter hat. Hierfür wurde ein spezielles Webinterface entwickelt, das die Definition und Eingabe solcher graphischen Passwörter durch simples Klicken auf das Bild ermöglicht und gleichzeitig auch die Korrektheit der Eingabe überprüft. Zunächst wurde in zwei Vorstudien jeweils eine Auswahl der Bilder getroffen, die später für die Passwortdefinition genutzt werden sollten. Durch die Teilnehmer der ersten Studie wurde die Komplexität dieser Bilder bewertet – basierend darauf konnte jeweils ein Bild mit geringer, mittlerer und hoher Komplexität ausgewählt werden. Anschließend wurden im Rahmen der zweiten Vorstudie durch andere Teilnehmer verschiedene graphische Passwörter definiert, auf jeweils einem Bild mit und ohne Saliency Mask aus den drei Komplexitätsklassen. Diese definierten Passwörter wurden für die Hauptstudie genutzt, in der schließlich die Erinnerungsfähigkeit in Hinblick auf die drei verschiedenen Komplexitätsklassen sowie die Saliency Maks untersucht wurde. Teilnehmer mussten sich über einen Zeitraum von vier Wochen mit den zu Beginn der Studie vergebenen Passwörtern insgesamt vier Mal einloggen: Direkt nach der Passwortvergabe sowie nach einer, zwei und vier Wochen. Die Ergebnisse der Hauptstudie bestätigten, dass graphische Passwörter, die auf Grundlage von Bildern mit Saliency Mask definiert wurden, über einen langen Zeitraum von mehreren Wochen gleich gut in Erinnerung behalten werden können, wie ohne. Demnach bewirkt die Saliency Mask eine deutliche Verbesserung in Hinblick auf die Sicherheit, während sie keinen Einfluss auf die Erinnerungsfähigkeit hat. Vorgegebene graphische Passwörter auf Grundlage von Bildern mit Saliency Mask sind demnach sowohl benutzbar, als auch sicher.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1. Einleitung

Authentifizierungssysteme dienen grundsätzlich einem Zweck: Ein System vor dem Zugriff fremder bzw. unautorisierter Personen zu schützen und somit zu gewährleisten, dass nur solche Personen Zugriff auf ein System bekommen, die dafür autorisiert sind. Es existieren derzeit viele verschiedene Authentifizierungssysteme, wie die bei Bankautomaten übliche PIN-Eingabe, die Passwortauthentifizierung oder biometrische Systeme. Insbesondere bei PINs und Passwörtern besteht die Problematik der vermeidlich schlechten Erinnerungsfähigkeit. Für den Menschen ist es schwer, sich an ein abstraktes Passwort, das aus einer Anordnung von Zahlen, Buchstaben und Sonderzeichen besteht, zu erinnern – insbesondere, wenn viele verschiedene solcher Passwörter im Alltag genutzt werden. Können die PINs und Passwörter von den Benutzern selbst definiert werden, so zeigen regelmäßige Studien und Veröffentlichungen genutzter Passwörter, dass von den Benutzern immer sehr einfache Buchstabenkombinationen gewählt werden, die oft auch aus dem Wörterbuch stammen[1]. Eine weitere Problematik, insbesondere bei frei wählbaren Passwörtern, ist, dass die Gefahr besteht, Wörter aus dem Wörterbuch zu benutzen. Diese können durch einen Angreifer leicht erraten werden. Entweder, weil dieser die Vorlieben der angegriffenen Person kennt oder, weil als Grundlage für eine Brute-Force-Attacke ein Wörterbuch genutzt wird. Dieses Wissen über die angegriffene Person erspart einem Angreifer viel Zeit da nicht mehr die Notwendigkeit besteht, alle Buchstabenkombinationen ausprobieren zu müssen sondern stattdessen auf ein Wörterbuch zurückgegriffen werden kann.

Um die Möglichkeit Passwörter aufzuschreiben einzugrenzen sowie die Verwendung von aus Wörterbüchern stammenden Passwörtern direkt durch das Design des Authentifizierungssystems zu unterbinden, wurden alternative Systeme entwickelt. Eine dieser Systeme stellt die bildbasierte Authentifizierung dar. Es existieren hiervon nach [SZO05, BCVO12] im Wesentlichen zwei Arten von bildbasierten Systemen. Eine davon beschränkt sich auf die Wiedererkennung, wie beispielsweise Déjà Vu [DP00]. Es müssen hierbei aus vielen Bildern, die mit einem Algorithmus zufällig generiert werden, eine bestimmte Anzahl zuvor ausgewählten Bildern wiedererkannt und ausgewählt werden, um die Authentifizierung erfolgreich zu durchlaufen. Die zweite Art beschreibt solche Systeme, die es für die Authentifizierung erforderlich machen, ein zuvor eingeprägtes Muster wiederzugeben. Diese zwei Arten stellen somit völlig verschiedene Anforderungen an einen Benutzer: „Wiedererkennung“ und „Wiedergabe“.

Die in dieser Studienarbeit untersuchten graphischen Passwörter fallen in die Kategorie „Wiedergabe“. Auf einem beliebigen Bild – in diesem Fall üblicherweise auf einer Fotografie

[1] Siehe Heise-Meldung: http://www.heise.de/security/meldung/Gawker-Einbruch-Beliebtestes-Passwort-ist-123456-1153267.html

Abbildung 1.1.: Ein Beispiel eines graphischen Passworts, das durch die grünen Passwortpunkte visualisiert wird. Zum Login müssen diese Passwortpunkte in gleicher Reihenfolge und an gleicher Stelle im Bild eingegeben werden.

– werden die graphischen Passwörter zuerst durch das Setzen von Passwortpunkten auf diesem Bild definiert, wie in Abb. 1.1 durch grüne Punkte und Linien visualisiert wird. Zur Authentifizierung an einem solchen System muss ein Benutzer diese definierten Punkte in der gleichen Reihenfolge und an der in etwa gleichen Position eingeben. Die Eingabe muss in einem gewissen Toleranzbereich liegen, innerhalb dem die Eingaben noch akzeptiert werden. Es existieren verschiedene Möglichkeiten und Ansätze, wie solch eine Eingabe graphischer Passwortpunkte vorgenommen werden kann. Denkbar ist die Gestik des Auges mit Hardware zur Blickerfassung aufzunehmen und auf das Bild zu übertragen. Doch auch eine Eingabe mit klassischen Eingabegeräten ist problemlos möglich. Mit einer Computermaus können beispielsweise durch das Klicken auf bestimmte Positionen auf einem Bild Passwortpunkte gesetzt und anschließend durch das System mit den definierten Punkten verglichen werden.

1.1. Motivation

Graphische Passwörter haben in der Praxis große Vorteile gegenüber bestimmten Arten von Angriffen, wie bereits in [BCVO12] ausführlich beschrieben wurde. Bei der Eingabe durch Blickerfassung kann die Augengestik nicht so einfach abgefangen bzw. abgefilmt werden, wie bei durch eine Tastatur vorgenommenen Eingaben, beispielsweise PIN-Eingaben an Bankautomaten. Auch bei einer Eingabe graphischer Passwörter mit klassischen Eingabegeräten, wie einer Computermaus, mit der die Passwortpunkte durch Klicken mit einer Maustaste an die entsprechende Position gesetzt werden, kann das Abfilmen effektiver verhindert werden. Wird auf die Visualisierung der gesetzten Passwortpunkte verzichtet, so stellt auch hier das Abfilmen oder „über die Schulter schauen“ eine deutlich größere Herausforderung dar, als bei der Eingabe einer PIN oder eines Passworts.

Eine weitere Möglichkeit, Angriffe auf ein solches Authentifizierungssystem zu führen, ist ein wissensbasierter Angriff. Erlangt der Angreifer das entsprechende Wissen über Vorlieben des Benutzers, so könnte dies dafür genutzt werden zu erraten, an welcher Position der Benutzer Punkte auf einem Bild für die Definition des graphischen Passworts gesetzt hat. Doch auch ohne solch ein Wissen sind Angriffe möglich: Sind auf einem Bild nur wenige einprägsame Punkte oder Bereiche vorhanden, so wäre es denkbar, dass eher in diesen Bereichen ein Passwortpunkt gesetzt wurde, da diese einfacher wiedergefunden werden können. Auf Grundlage dieser Annahmen wurde die Sicherheit der hier verwendeten bildbasierten bzw. graphischen Passwörter bereits in [BAS12] ausführlich untersucht. Um solche Attacken zu unterbinden, wurden in der Studie Bilder mit so genannten Saliency Masks (in Kapitel 2.2 ausführlich beschrieben) auf ihre verbesserte Sicherheit untersucht. Die Saliency Mask visualisiert die Stellen eines Bildes, die solche einprägsamen, eindeutigen Punkte darstellen und vermeidlich oft für die Definition eines graphischen Passworts genutzt werden. Diese Bereiche wurden durch die Saliency Mask für die Definition der Passwortpunkte gesperrt – das Setzen solcher Punkte war in diesen Bereichen nicht mehr möglich. Die Ergebnisse der Studie zeigten, dass es einen großen Einfluss auf die Sicherheit hatte: Graphische Passwörter auf Grundlage von Bildern mit Saliency Masks waren signifikant sicherer als solche Passwörter auf Bildern ohne Saliency Mask sowie auch signifikant Sicherer als eine vierstellige PIN.

Grundsätzlich gibt es, wie in [DLDH09] beschrieben, drei Anforderungen, die ein Authentifizierungssystem erfüllen muss. Neben der *Sicherheit* von solchen Authentifizierungssystemen spielt allerdings auch die *Einfachheit* und *Benutzbarkeit* eine große Rolle, da sie einen wesentlichen Einfluss auf die spätere Akzeptanz bei Benutzern hat. Zur Benutzbarkeit gehört hinzu, wie gut oder schlecht sich Benutzer an ein solches graphisches Passwort erinnern können und ob dies schwieriger ist, als bei bereits akzeptierten und weit verbreiteten Authentifizierungssystemen. Dass die Erinnerungsfähigkeit an graphische Authentifizierungssysteme im Vergleich zu den üblichen Systemen besser ist, wurde bereits in [ML07] gezeigt. Das Potenzial bei graphischen Passwörtern an der Erinnerungsfähigkeit zudem deutlich größer: Durch bestimmte Eselsbrücken und Mnemotechniken kann die Erinnerungsfähigkeit nochmals deutlich gesteigert werden. Daher stellt sich in dieser Studie als Anknüpfung zu [BAS12] im wesentlichen die Frage, ob die Saliency Mask einen negativen Einfluss auf die

Erinnerungsfähigkeit der darauf definierten graphischen Passwörter hat als bei einem Bild ohne Saliency Mask. Genau diese Frage soll im Rahmen dieser Studienarbeit untersucht werden: Wie gut können sich Teilnehmer an graphische Passwörter, die auf Grundlage von Bildern mit Saliency Masks definiert wurden, im Vergleich zu solchen ohne Saliency Mask sowie, als Messbasis, im Vergleich zu einer vierstelligen PIN erinnern. Ein weiteren Einfluss auf die Erinnerungsfähigkeit könnte, unabhängig von der Saliency Mask, auch das Bild selbst spielen. Aus diesem Grund sollen im Rahmen dieser Studienarbeit zusätzlich auch mögliche Einflüsse untersucht werden, die durch Bilder verschiedener Komplexitätsklassen entstehen können. Für die Beantwortung dieser Fragen wird eine vierwöchige Langzeitstudie durchgeführt, an der über ein eigens dafür entwickeltes Webinterface Benutzer teilnehmen können.

Die Ziele dieser Studienarbeit sind demnach die Folgenden:

1. Evaluierung der Erinnerungsfähigkeit an graphische Passwörter, die auf Grundlage von Bildern mit und ohne Saliency Mask erstellt wurden, sowie an vierstellige PINs.
2. Vergleich der Erinnerungsfähigkeit an graphische Passwörter auf Grundlage von Bildern verschiedener Komplexitätsstufen, jeweils mit und ohne Saliency Mask, im Vergleich zur PIN.

Zudem sollen die in Kapitel 1.2 aufgestellten Hypothesen bestätigt bzw. widerlegt werden.

1.2. Hypothesen

Die im Rahmen dieser Studienarbeit durchgeführte Studie dient dazu herauszufinden, wie sich die Erinnerungsfähigkeit eines graphischen Passworts mit und ohne Saliency Mask in den drei Komplexitätsklassen im Vergleich zu einer vierstelligen PIN, wie sie bei Bankautomaten üblich ist, über einen längeren Zeitraum von vier Wochen verhält. Dazu wurden zwei Hypothesen aufgestellt:

1. Vorgegebene graphische Passwörter, die auf einem Bild mit Saliency Mask definiert wurden, sind nicht schwerer zu merken als auf dem gleichen Bild ohne Saliency Mask.
2. Die Bildkomplexität hat keinen Einfluss auf die Erinnerungsfähigkeit an vorgegebene graphische Passwörter.

Die Hypothesen werden mit der Hauptstudie (Kapitel 4) untersucht und in den Ergebnissen (Kapitel 5) ausgewertet.

1.3. Aufbau dieser Ausarbeitung

Die Arbeit ist in folgender Weise gegliedert:

Kapitel 1 – Einleitung: In diesem Kapitel werden die Notwendigkeit und Motivation für diese Studie erläutert.

Kapitel 2 – Hintergrund und verwandte Arbeiten: Hintergründe sowie verwandte Studien und Ausarbeitungen zum Thema der graphischen Passwörter sowie der auf Grundlage dieser Studienarbeit erarbeitete Artikel werden in diesem Kapitel vorgestellt.

Kapitel 3 – Vorstudien beschreibt die im Rahmen dieser Studienarbeit durchgeführten Vorstudien sowie deren Notwendigkeit und die daraus resultierenden Erkenntnisse und Ergebnisse.

Kapitel 4 – Hauptstudie: Hier wird schließlich die Vorbereitung, Implementierung und Durchführung der Hauptstudie zur Erinnerungsfähigkeit an bildbasierte Passwörter im Vergleich zur PIN beschrieben.

Kapitel 5 – Ergebnisse: Dieses Kapitel dient der Vorstellung und Analyse der Ergebnisse aus der Hauptstudie.

Kapitel 6 – Zusammenfassung und Ausblick fasst die Ergebnisse dieser Studienarbeit zusammen und stellt Anknüpfungspunkte vor.

2. Hintergrund und verwandte Arbeiten

Graphische und bildbasierte Authentifizierungssysteme wurden bereits in vielen verschiedenen Studien in Hinblick auf ihre Sicherheit, Benutzbarkeit oder die Erinnerungsfähigkeit genauer untersucht und dabei mit konventionellen Authentifizierungssystemen verglichen. In diesem Kapitel gibt es einen Überblick aller verwandter und bereits veröffentlichter Arbeiten und der dort jeweils erlangten Ergebnisse und Erkenntnisse. Zudem gibt es eine Einführung in die Saliency Mask, die im Rahmen anderer Studien und Arbeiten entwickelt wurde und in dieser Studienarbeit eines der Testobjekte darstellt.

2.1. Verwandte Studien

Es wurden bereits eine Vielzahl von Studien über die Messung der Erinnerungsfähigkeit bildbasierter Passwörter sowie über Techniken zur Verbesserung der Erinnerungsfähigkeit sowohl an graphische als auch alphanumerische Passwörter durchgeführt.

2.1.1. Studien zur Erinnerungsfähigkeit an graphische Passwörter

Die Erinnerungsfähigkeit an ein Passwort bzw. an mehrere Passwörter stellt das wesentliche Problem dieses Authentifizierungssystems dar. Brown et al. zeigten in [BBZD04], dass eben diese Erinnerungsfähigkeit daran das Hauptproblem eines Systems darstellt. Ein gravierendes, in den vorherigen Abschnitten bereits angesprochenes Problem wurde hier bestätigt: Mehr als Zweidrittel der genutzten Passwörter konnten auf das persönliche Umfeld oder Vorlieben zurückgeführt werden, wie beispielsweise der Namen von Verwandten oder Geburtsdaten. Zudem stellte sich auch die Erinnerungsfähigkeit als Problematisch dar. Eindrittel der dortigen Teilnehmer vergaßen das Passwort, mehr als die Hälfte der befragten Personen nutzte sogar die Möglichkeit, ein solches Passwort aufgeschrieben auf einem Blatt Papier o.ä. aufzubewahren. Ferner stellte sich in [AS99] heraus, dass vier bis fünf durch Benutzer regelmäßig genutzte Passwörter das Maximum der Erinnerungsfähigkeit darstellen. Grundsätzlich führen demnach mehrere Passwörter, an die sich ein Benutzer erinnern muss, zu einer Verringerung der Erinnerungsfähigkeit. Dagegen zeigten gleich mehrere Studien [DACJR05, EBFK09], dass die Erinnerungsfähigkeit an graphische und bildbasierte Passwörter im Vergleich zu konventionellen alphanumerischen Passwörtern und PINs besser sind.

Es existiert bereits eine kommerzielle Lösung eines Authentifizierungssystemen, das auf das Wiedererkennungsprinzip graphischer Passwörter setzt. Bei dem als PassShape bezeichneten

System muss ein Benutzer zunächst vier Gesichtsaufnahmen bzw. Portraits definieren. Um sich gegenüber einem System zu authentifizieren, müssen genau diese vier zuvor definierten Portraits innerhalb vieler anderer Portraits wiedererkannt werden. Dieses Authentifizierungssystem wurde von Brostoff und Sasse auf die Erinnerungsfähigkeit im Vergleich zu konventionellen Passwörtern untersucht [BS00]. Das Ergebnis dieser Studie fällt zugunsten von PassShapes: Benutzer machten bei der Authentifizierung durch PassShape deutlich weniger Fehler im Gegensatz zu normalen Passwörtern, obwohl die Studie so gestaltet war, dass die Anzahl der Authentifizierungen mit PassShape geringer war, als mit normalen Passwörtern, sodass dadurch der Lerneffekt deutlich geringer war. Davis et al. führten eine Untersuchung der Erinnerungsfähigkeit zwischen PassShapes und graphischen Passwörtern, die aus einer Sequenz von Bildern bestanden (zur Authentifizierung an solch einem System muss eine Sequenz von mehreren Bildern in entsprechender Reihenfolge wiedererkannt werden), durch [DMR04]. Auch die Ergebnisse dieser Studie bescheinigten der Wiedererkennbarkeit von Bildern – hier im Speziellen von Portraits – eine deutlich bessere Erinnerungsfähigkeit.

Zu einem damit im Einklang stehenden Ergebnis kommen auch Dhamija und Perrig [DP00]. Das Anwendungsszenario in dieser Studie stellte ebenfalls die Wiedererkennung zuvor gesehener Bilder innerhalb von vielen angezeigten Bildern dar. Hier wurde ein Vergleich zwischen den graphischen Passwörtern, konventionellen Passwörtern (bestehend aus Buchstaben) und vierstelligen PINs durchgeführt. Das Ergebnis dieser Studie ist auch in diesem Fall eindeutig zugunsten der graphischen Passwörter. Die Teilnehmer der Studie mussten sich nach einer Woche mit den zuvor definierten Passwörtern an dem System einloggen. Es konnten sich 35% der Teilnehmer nicht mehr an die PIN und 30% nicht mehr an das konventionelle Passwort erinnern, während die Fehlerquote bei der Wiedererkennung der zuvor definierten Bilder bei lediglich 5% lag.

Mit PassPoints haben Widenbeck et al. erstmals ein Authentifizierungssystem entwickelt, für das ein Benutzer zunächst ein graphisches Passwort durch die Auswahl von Bereichen bzw. das Setzen von Passwortpunkten auf einem Bild definieren musste. Für den Authentifizierungsvorgang gegenüber solch einem System muss der Benutzer diese Bereiche in der gleichen Reihenfolge wiedererkennen und in das System eingeben [WWB+05b]. Verglichen wurden die PassPoints ebenfalls mit konventionellen, aus Buchstabenkombinationen bestehenden Passwörter in einer Langzeitstudie über mehrere Wochen. Die Studie ergab, dass die Erinnerungsfähigkeit zwischen beiden Passworttypen in etwa gleich ist, allerdings die Eingabe graphischer Passwörter mehr Zeit in Anspruch nimmt. In einer weiterführenden Studie haben sie zudem den Einfluss verschiedener Bildarten sowie des Toleranzbereichs, innerhalb dessen Eingaben noch akzeptiert werden, untersucht [WWB+05a]. Verschiedene Bildarten haben demnach keinen oder nur marginalen Einfluss auf die Erinnerungsfähigkeit an graphische Passwörter. Dagegen spielt die Wahl der Größe des Toleranzbereichs eine große Rolle und hat auch einen starken Einfluss auf die Quote erfolgreicher Login-Versuche der Teilnehmer. Bei einem sehr kleinen Toleranzbereich leidet die Erinnerungsfähigkeit massiv. Für einen Benutzer ist es sehr schwierig, den zuvor definierten Punkt exakt oder nahezu exakt zu treffen. Zum einen liegt dies an den verfügbaren Anzeige- und Eingabemethoden – ein Pixel eines Bildes hat, je nach auf welchem Bildschirm dieses Bild angezeigt wird, weniger als einen Millimeter Durchmesser. Zum anderen jedoch liegt das an der

fehlenden Wiedererkennbarkeit einzelner Pixel, da Passwortpunkte oft auf einen Bereich (z.B. menschlichen Kopf) gesetzt werden, die mehr als nur einen Pixel einnehmen und daher nicht exakt wiedergegeben werden können.

In einer weiteren Studie untersuchten Chiasson et al. die Benutzbarkeit und Sicherheit der PassPoints im Vergleich zu einem leicht abgewandeltem System [COB07]. Die Benutzer mussten statt auf einem Bild mehrere Passwortpunkte zu definieren und dieser später wiederzugeben, für eine Sequenz von Bildern jeweils nur ein Passwortpunkt definieren. Die Verfasser der Studie sind zum Ergebnis gekommen, dass es für Benutzer einfacher ist, sich auf mehreren Bildern an jeweils nur einen Punkt zu erinnern, statt an mehrere Punkte auf einem Bild. Ferner wurde für dieses Verfahren eine schnellere Eingabezeit und geringere Fehlerquote gemessen als bei den ebenfalls getesteten PassPoints. Chiasson et al. konnten in einer zweiten Studie ihre zuvor erlangten Ergebnisse validieren [CBO07]. Diesmal war die Teilnehmerzahl mit mehreren hundert Studenten zudem sehr hoch. Die Ergebnisse bestätigten das vorher getroffene Fazit in Hinblick auf die Erinnerungsfähigkeit sowie Benutzbarkeit dieser Art von graphischen Passwörtern. Zudem wurde festgestellt, dass die Wahl der Bilder einen signifikanten Einfluss auf die Erinnerungsfähigkeit an die darauf definierten graphischen Passwörter hat.

2.1.2. Techniken zur Verbesserung der Erinnerungsfähigkeit an Passwörter

In der Vergangenheit gab es diverse Untersuchungen zu Entwicklungen von Techniken zur Verbesserung der Erinnerungsfähigkeit an multiple graphische sowie konventionelle Passwörter. Nach Zhang et al. ist die Erinnerung an mehrere verschiedene Passwörter die größte Herausforderung für einen Menschen [ZLAZ09] – demnach verschlechtert sich die Erinnerungsfähigkeit mit der Anzahl der zu erinnernden Passwörter. Für die von Zhang et al. Studie wurden zwei verschiedene Techniken, die dem Gedächtnis als Hilfestellung dienen sollen, evaluiert. Teilnehmer sollten für mehrere verschiedene Anwendungszwecke (Einkaufen, Finanzen, Reise u.ä.) verschiedene alphanumerische Passwörter definieren, die bestimmten Passwortregeln entsprechen müssen, und diese zu einem späteren Zeitpunkt wiedergeben. Eine der Techniken liefert einem Benutzer als Hilfestellung den ersten Buchstaben des gewählten Passworts, während die andere Technik die Passwortregel, nach der das entsprechende Passwort definiert werden musste, anzeigte. Die Untersuchungen zeigten, dass die Erinnerungsfähigkeit an alphanumerische Passwörter signifikant besser ist, wenn der Anfangsbuchstabe des Passworts angezeigt wird.

Vu et al. haben in einer ähnlichen Studie eine weitere alternative Technik entwickelt, die Passwörter aus Anfangsbuchstaben von Wörtern aus einem Satz generiert [ZLAZ09]. Mit der durchgeführten Studie sollte die Exaktheit der Wiedergabe der neu entwickelten Technik im Vergleich zu zufällig generierten Passwörtern evaluiert werden. Die Analyse ergab, dass die aus Anfangsbuchstaben bestehenden Passwörter von Menschen besser im Gedächtnis behalten werden können als die zufällig generierten Passwörter. In einer großflächigen von Yan et al. durchgeführten Studie wurde ebenfalls die Erinnerungsfähigkeit an Passwörter bestehend aus Anfangsbuchstaben von Wörtern, die aus unüblichen oder persönlichen Sätzen stammen („Mein Hund ist 24 Jahre alt und mag Knochen“ entspricht demnach

„MHi24Ja&mK“), im Vergleich zu zufällig generierten Passwörtern getestet [YBAG04]. Diese Studie bestätigt nochmals die bereits erlangten Ergebnisse: Die Erinnerungsfähigkeit der Teilnehmer an aus Anfangsbuchstaben bestehenden Passwörter ist signifikant besser bei gleichbleibend hoher Sicherheit, wie sie bei zufällig generierten Passwörtern gegeben ist. Grundsätzlich scheint in all den Studien Einigkeit darüber zu herrschen, dass einfach zu erinnernde alphanumerische Passwörter den Nachteil haben, dass sie auch einfach zu erraten und demnach auch einfacher zu knacken sind.

Mit den so genannten PassShapes präsentierten Weiss et al. eine neue graphische Authentifizierungsmethode [WDL08]. Die Idee hinter PassShape ist, dass Benutzer eine geometrische Form definieren können, wobei es sich um ein Vieleck oder anderes geometrisches Gebilde mit Kantenkreuzungen handeln darf und aus insgesamt acht Kanten besteht. Für den Authentifizierungsvorgang muss dieses geometrische Gebilde in einem speziellen Interface wiedergegeben werden. Die durchgeführte Studie zeigte, dass die Erinnerungsfähigkeit an PassShapes unter der Voraussetzung besser ist, dass die Teilnehmer die Möglichkeit bekommen, ihr geometrisches Objekt in mehreren Übungseinheiten zu Trainieren. Des Weiteren zeigte die Analyse sogar, dass die Erinnerungsfähigkeit an PassShapes über die Zeit mit jeder Eingabe stieg. Eine ähnliche Studie führten Lin et al. anhand einer leicht abgewandelten Form der „Draw-a-Secret“-Idee, ursprünglich entwickelt von Jermyn et al. [JMM+99], durch. Teilnehmer können ein oder mehrere beliebige Objekte als graphisches Passwort definieren und müssen dieses zur Authentifizierung nachzeichnen. Lin et al. verbesserten dieses System, indem sie eine bessere und sichere interne Repräsentation des graphischen Passworts entwickelten, ohne dabei die Erinnerungsfähigkeit zu verschlechtern [LDOY07].

Die bereits erwähnte Problematik der Erinnerungsfähigkeit an mehrere Passwörter wurde von Moncur et al. in einer Studie in Hinblick auf graphische Passwörter genauer untersucht [ML07]. Insbesondere der Vergleich zwischen mehreren graphischen Passwörtern und mehreren PINs sollte durchgeführt werden. Zudem wurden auch verschiedene Arten von Gedächtnisstützen miteinander verglichen. Die Analysen zeigten, dass die Erinnerungsfähigkeit der Teilnehmer an mehrere graphische Passwörter besser ist als an mehrere PINs. Zudem zeigte sich, dass Eselsbrücken eine effektive Strategie der Gedächtnisstütze darstellen und die Erinnerungsfähigkeit dadurch nochmals verbessert werden kann.

2.1.3. Zusammenfassung

Alle hier vorgestellten Studien beschränkten sich größtenteils auf die Analyse der Erinnerungsfähigkeit an verschiedene Arten vorgegebener graphischer Passwörter im Vergleich zu konventionellen Passwörtern oder PINs sowie Entwicklung von Techniken, die zur Verbesserung der Erinnerungsfähigkeit dienen. Nur bei wenigen der Studien handelte es sich zum Langzeitstudien, welche die Erinnerungsfähigkeit über mehrere Wochen hinweg getestet und gemessen haben, wie beispielsweise von Widenbeck et al. [WWB+05b, WWB+05a] oder De Luca et al. [DLDH09] durchgeführt wurde.

Zwar wurde von Chiasson et al. festgestellt, dass die Auswahl verschiedener Bilder einen Einfluss auf die Erinnerungsfähigkeit der dort getesteten graphischen Passwörter hat [CBO07].

Abbildung 2.1.: Diese Abbildung zeigt die in der ersten Vorstudie als wenig (a), mittel (b) und stark (c) komplex bewerteten Bilder jeweils mit (unten) und ohne (oben) der in Rot visualisierten Saliency Mask.

Jedoch wurde in keiner Studie der Einfluss von Bildern aus verschiedenen Komplexitätsklassen untersucht, in denen die Einteilung der Bilder in die entsprechenden Klassen durch Teilnehmer einer separaten Studie erfolgte. Des Weiteren wurde zwar bereits festgestellt, dass vorgegebene graphische Passwortpunkte, die auf Bildern mit Saliency Mask definiert wurden, sicherer sind [BAS12], allerdings sind hier die Auswirkungen der Saliency Mask auf die Erinnerungsfähigkeit noch unbekannt.

Ziel dieser Studienarbeit ist daher einerseits in einer über mehrere Wochen andauernden Langzeitstudie herauszufinden, ob Bilder aus verschiedenen Komplexitätsklassen einen Einfluss auf die Erinnerungsfähigkeit graphischer Passwörter haben. Andererseits soll in der gleichen Langzeitstudie auch untersucht werden, ob die Saliency Mask einen Einfluss auf die Erinnerungsfähigkeit hat.

2.2. Saliency Mask

Die grundsätzliche Problematik bei der Definition von Passwortpunkten auf einem Bild oder einer Fotografie besteht darin, dass Angreifer davon ausgehen kann, dass Benutzer die Passwortpunkte eher auf hervorstechende und auffallende Bereiche des Bildes setzen. Auf diese Weise wird die Anzahl der Möglichkeiten, die ein graphisches Passwort auf einem Bild theoretisch haben kann, stark eingeschränkt, sodass die Wahrscheinlichkeit, ein Passwort zu erraten, steigt. Diese Annahme wird aus den in der Vorstudie 2 resultierenden Ergebnissen nochmals bekräftigt, siehe Kapitel 3.3.3. Um die Nutzer davon abzuhalten, Passwortpunkte in solche Bereiche eines Bildes zu setzen, besteht die Möglichkeit, diese Bereiche schlicht zu erkennen und zu sperren.

Für die Vorhersage dieser hervorstechenden Bereiche wurde das „Graph-Based Visual Saliency“-Modell (GBVS) von Harel et al. [HKP06] genutzt. Mit GVBS können mit 98% nahezu alle dieser Bereiche innerhalb eines natürlichen Bildes (einer Fotografie) vorhergesagt werden, was einen besseren Wert darstellt, als der originale, von Itti et al. [IKN98] entwickelte Algorithmus. Zur Berechnung der Saliency Mask wurde das ebenfalls von Harel et al. entwickelte Matlab-Skript [Har06] mit den dort vorhandenen Voreinstellungen genutzt – Veränderungen an den Parametern oder am Skript selbst fanden nicht statt. Mit dem GBVS-Algorithmus werden für jedes Bild Heatmaps, repräsentiert durch Graustufenbilder mit Verläufen von Schwarz zu Weiß, der hervorstechenden Bereiche erstellt. Um eine genauere Einteilung zwischen einem hervorstechenden und nicht-hervorstechendem Bereich zu erlangen, wurde die Grenze auf genau $0,5$ festgelegt. Für die in dieser Studie verwendeten Bilder wurde der hervorstechende Bereich bzw. die Saliency Mask in Rot dargestellt, siehe Abb. 2.1.

2.3. Eingereichter Artikel auf Grundlage dieser Studienarbeit

Auf Grundlage der im Rahmen dieser Studienarbeit erlangten entstandenen Ergebnissen wurde ein Artikel erarbeitet und für die *31. SIGCHI International Conference on Human Factors in Computing Systems (2013)* eingereicht. Aus diesem Grund basiert diese Studienarbeit auf dem folgenden Artikel:

Bulling, A., Alt, F., Schneegass, S., Mikusz, M., Schmidt, A., Long-term Memorability of Cued-Recall Graphical Passwords with Saliency Masks. *Submitted to the 31th SIGCHI International Conference on Human Factors in Computing Systems (2013).*

Ferner ist diese Studienarbeit in Zusammenarbeit mit dem *Computing Laboratory*[1] der Universität Cambridge entstanden.

[1] http://www.cl.cam.ac.uk/

3. Vorstudien

Zur Bewertung der Erinnerungsfähigkeit an die bildbasierten Passwörter soll eine Langzeitstudie mit einer Dauer von mehreren Wochen durchgeführt werden. In dieser werden sich die Benutzer in einem Webinterface insgesamt vier mal einloggen und zwei bildbasierte Passwörter sowie eine PIN eingeben müssen.

Vor der Durchführung dieser Hauptstudie hat sich allerdings zur Gewährleistung der Subjektivität die Notwendigkeit für zwei Vorstudien ergeben. Zum einen stellt sich die Frage nach einer korrekten und sinnvollen Bildauswahl. Es sollten Bilder vorhanden sein, die sich von einander ausreichend unterscheiden, damit bei der Auswertung der Hauptstudie auch die Frage beantworten kann, ob die Bilder an sich einen Einfluss auf die Erinnerungsfähigkeit an ein darauf definiertes graphisches Passwort haben haben. Zum anderen soll die Studie möglichst realistisch durchgeführt werden. Dazu gehören insbesondere realistische Bildpasswörter und PINs sowie ein realistisches Vergabeverfahren. Diese beiden Faktoren – die Bildauswahl und PIN-/Bildpasswortvergabe – wurden in zwei separaten Vorstudien untersucht.

3.1. Bilderauswahl

Bei einer bildbasierten Authentifizierung ist es naheliegend, dass die Bildauswahl einen Einfluss auf die auf einem Bild definierbaren Passwörter und somit zumindest auch indirekt einen Einfluss auf die Erinnerungsfähigkeit an solche Passwörter haben kann. Bilder mit sehr vielen Konturen und Kanten bieten mehr Bereiche, Passwortpunkte zu setzen und wiederzufinden, als Bilder ohne klare Formen. Auch die Farben, Größe und Formen in einem Bild können einen Einfluss haben.

Ziel war es daher, zunächst verschiedene Bilder möglichst unabhängig auszuwählen und gleichzeitig garantieren zu können, dass genug verschiedenartige Bilder vorhanden sind. Da allerdings für die Hauptstudie nur wenige Bilder benötigt werden, wurde im zweiten Schritt eine Auswahl dieser Bilder getroffen.

Dazu sollten jeweils ein sehr, mittel und ein wenig komplexes Bild vorhanden sein. Für die Bewertung der Komplexität der Bilder wurden in der Vergangenheit verschiedene Verfahren entwickelt, die alle einem bestimmten Anwendungszweck dienen. Eine Möglichkeit ist beispielsweise die Anzahl der in den Bildern vorhandenen Kanten zu zählen und miteinander zu Vergleichen unter der Annahme, dass viele im Bild vorhandene Kanten auch ein komplexeres Bild darstellen [CDGPT09]. Auch Grauwerte, Kantenlängen, Größen und

Anzahl von Objekten und der Kontrast wurden bereits als Maßeinheit für die Berechnung der Komplexität herangezogen [PIA+90, BCV85].

Bei diesen Studien handelte es sich hauptsächlich um eine automatische Zielerkennung in Bildern – keines behandelte die Komplexität in Hinblick auf die Erinnerungsfähigkeit an Bildpasswörter. Da bei Bildpasswörtern später Menschen mit diesen Bildern arbeiten und darauf Passwörter definieren müssen, ist vor allem bei diesem Einsatzzweck eine subjektive Bewertung durch Menschen interessant. Um eine sinnvolle Bildauswahl garantieren zu können, wurde daher eine Vorstudie zur Bewertung der Bildkomplexität durchgeführt: Voneinander unabhängige Teilnehmer wurden gebeten, die Komplexität der Bilder zu bewerten. Anschließend konnte für die Hauptstudie jeweils ein Bild mit hoher, mittlerer und geringer Komplexität ausgewählt werden.

3.1.1. Zufällige Bilderauswahl

Eine wichtige Aufgabe war zunächst die unabhängige Auswahl möglichst verschiedener Bilder, die später ihrer Komplexität nach bewertet werden sollten. Als Quelle für die Bilder diente Flickr[1].

Für die Auswahl der Bilder wurde ein Python-Skript geschrieben, das über die Flickr-API[2] Zugang zu allen bei Flickr als öffentlich gekennzeichneten Bildern erhalten hat. Ein Abruf beliebiger und völlig zufälliger Bilder wäre naheliegend, ist in der API allerdings nicht vorgesehen. Stattdessen muss für den Abruf von Bildern zumindest eine bestimmte Kategorie oder Schlagwörter angegeben werden. Um eine breite und gleichzeitig auch sinnvolle Auswahl an Bildern zu erhalten, wurden die zu dem Zeitpunkt am meisten genutzten Schlagwörter (siehe A.1) als Übergabeparameter genutzt.

Ein weiteres Kriterium ist die Bildgröße. Wichtig ist, auch auf Hinblick auf die verschiedenen Monitorauflösungen, ein möglichst hoch aufgelöstes Bild sowie, für die homogene und ästhetische Darstellung, Bilder mit einem ähnlichen Bildformat (in etwa 4:3), auszuwählen.

Damit die Bilder später auch in lizenzrechtlicher Hinsicht problemlos für die Vor- und Hauptstudien genutzt werden können, ist ein weiteres Kriterium die Lizenz. Es wurden ausschließlich Bilder mit der „Creative Commons“-Lizenz[3] ausgewählt. Dieses Kriterium konnte direkt über die Flickr-API angegeben werden, sodass eine nachträgliche Überprüfung und Aussortierung unpassender Bilder nicht nötig war.

Die Anzahl der Anforderungen an die Bilder sollten möglichst gering gehalten werden, damit die Bildauswahl so wenig wie möglich eingeschränkt wird und somit so viele verschiedene Bilder gefunden werden.

Um eine möglichst zufällige und unabhängige Auswahl der Bilder garantieren zu können, suchte das dafür genutzte Skript für jedes der 20 Bilder zunächst einen zufälligen Zeitraum

[1] http://www.flickr.com
[2] http://www.flickr.com/services/api/
[3] http://de.creativecommons.org/

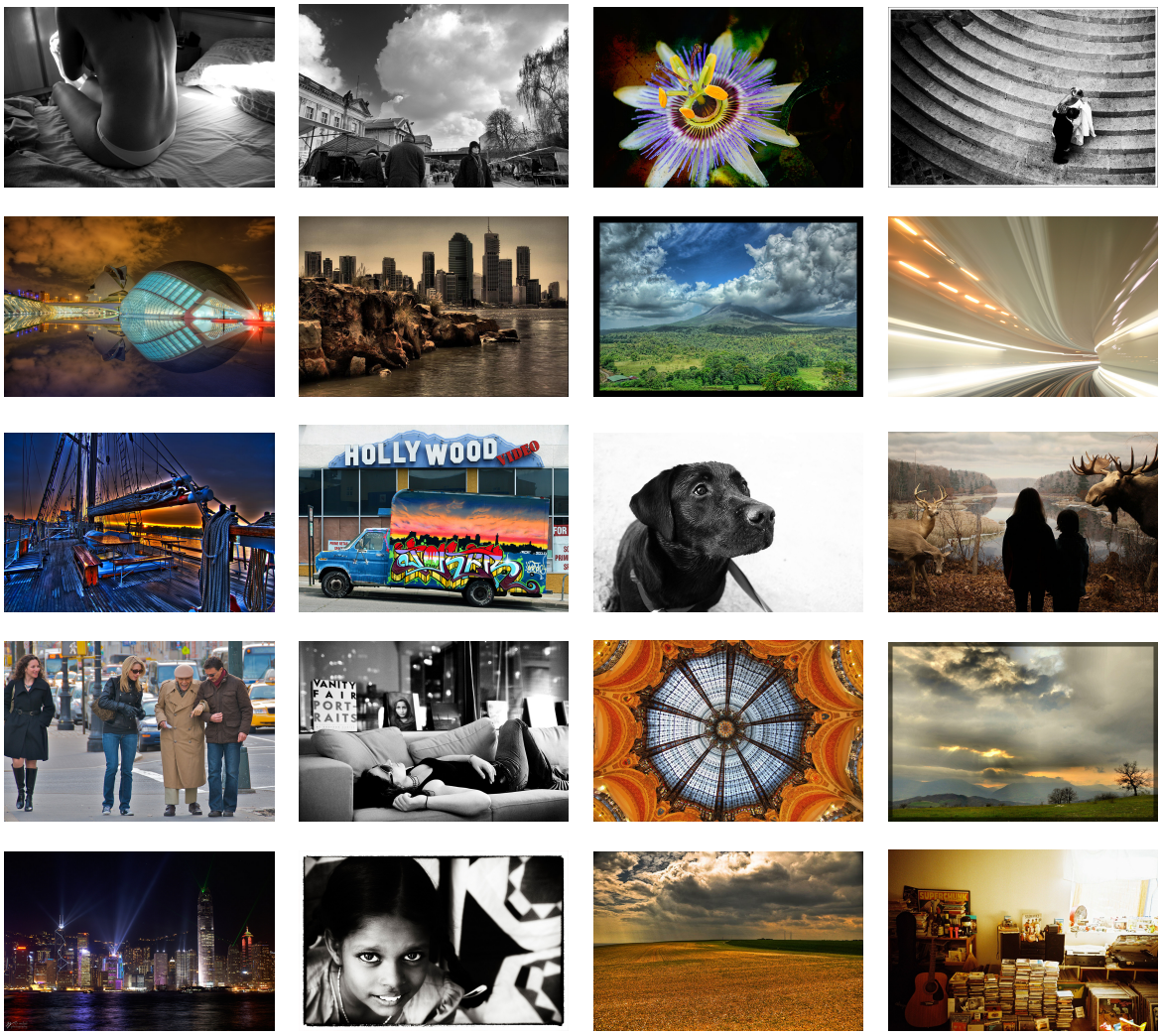


Abbildung 3.1.: Die 20 für die erste Vorstudie zufällig ausgewählten Bilder

von 30 Tagen aus (vom Gründungsdatum des Flickr-Dienstes bis zum heutigen Datum). Anschließend wurden alle Bilder in diesem Zeitraum abgefragt, die zusätzlich die passende „Creative Commons"-Lizenz, Bildgröße sowie Kennzeichnung mit mindestens einem der Schlagwörter aus A.1 enthielten. Die Bilder, die diese Kriterien erfüllten, wurden nach ihrer Beliebtheit bzw. Interessantheit sortiert. Davon wurde das erste und damit interessanteste Bild abgerufen und gespeichert. Anschließend wurde ein neuer zufälliger Zeitraum von 30 Tagen gesucht und das nächste Bild auf diese Weise abgerufen, bis die Gesamtanzahl von 20 Bildern erreicht war. Abb. 3.1 zeigt alle Bilder, die auf diese Weise abgerufen und für die erste Vorstudie wurden.

3.1.2. Diskussion über die Bildkomplexität

Bei Betrachtung der Bilder aus Abb. 3.1 fällt auf, dass sowohl komplexe Formen als auch Bilder ohne erkennbares Muster, mit vielen Verläufen, z.B. ein großer Anteil an Wolken im Bild, vorhanden sind. Auch was die Bandbreite der genutzten Farben angeht, gibt es Unterschiede: Sowohl schwarzweiß- als auch farbige Bilder mit mehr oder weniger intensiven Farben sind vorhanden.

All diese Faktoren können einen Einfluss auf die Gestaltung und Festlegung eines graphischen Passworts haben und damit auch an die Erinnerungsfähigkeit an solch ein Passwort. Denn für das Setzen eines Passwortpunktes, das ein Teil eines Bildpassworts ist, könnte angenommen werden, dass dieser Punkt eher auf einem einfacher wiedererkennbaren und markanten Teil des Bildes gesetzt wird, wie Augen oder Ohren eines Hundes, auf Gesichter von Menschen oder auf den Spitzen der Hochhäuser, statt inmitten einer Wolke bzw. eines Bereichs, ohne wiedererkennbares und markantes Muster.

Ein Bild, das nur wenige oder keine solche Bereiche bietet, und eher aus Verläufen oder, bei einem Landschaftsbild, nur aus Wiesen und Wolken besteht, könnte als Bild mit geringer Komplexität bezeichnet werden. Andere Bilder dagegen, die beispielsweise Silhouetten von Hochhäusern abbilden, enthalten deutlich mehr Kanten und einfacher wiedererkennbare Bereiche sowie markante Muster, sodass die Komplexität höher eingestuft werden könnte. All dies hängt jedoch sehr stark von der Definition der Bildkomplexität selbst und insbesondere dem subjektiven Empfinden eines jeden Benutzers ab.

3.2. Vorstudie 1: Bewertung der Bildkomplexität

Da aus Rücksicht auf die Vergleichbarkeit und Auswertung der Hauptstudie nicht alle diese Bilder verwendet werden können, bestand die Notwendigkeit, alle Bilder als wenig, mittel und hoch komplex zu klassifizieren. Auf diese Weise reicht es aus, wenn für die Hauptstudie nur jeweils ein Bild aus den drei Komplexitätsklassen verwendet werden. Dies ermöglicht einen späteren Vergleich der Erinnerungsfähigkeit zwischen den verschiedenen Komplexitätsklassen und wird zu der Beantwortung der Frage führen, ob graphische Passwörter auf Grundlage von Bildern mit hoher oder geringer Komplexität jeweils mit und ohne Saliency Mask besser, schlechter oder idealerweise gleich gut in Erinnerung behalten werden können.

Für die subjektive Bewertung der Bildkomplexität einzelner Bilder wurde die erste Vorstudie durchgeführt. Möglichst viele Personen sollten in einem eigens dazu entwickelten Webinterface die Komplexität der Bilder bewerten. Damit diese Bewertung immer relativ zu allen anderen Bildern geschieht, es allerdings schwierig für einen Teilnehmer wäre, alle 20 Bilder nebeneinander zu sehen und gleichzeitig bewerten, wurde das Problem wie folgt gelöst: Ein Teilnehmer hat immer zwei Bilder nebeneinander zusehen bekommen und musste auf das aus seiner Sicht komplexere Bild mit der linken Maustaste klicken.

3.2.1. Systemimplementierung

Für die erste Vorstudie musste sowohl ein eigenes Webinterface, das für den Teilnehmer einfach benutzbar und intuitiv verständlich ist, als auch ein dazu passendes und sinnvoll aufgebautes Datenbankmodell entwickelt werden, das zudem entsprechend der Normalformregeln eine Tabellenstruktur hat, die Redundanzen vermeidet. Gleichzeitig sollen in Hinblick auf die Analysen einfache Datenbankabfragen möglich sein.

Webinterface

Das für die Bewertung der Bildkomplexität nötige Webinterface wurde mit einem PHP-Skript realisiert. Da die Bewertung immer anhand zweier Bilder vorgenommen werden sollte, ergab sich nur die Notwendigkeit, zwei Bilder gleichzeitig anzuzeigen und dem Teilnehmer die Möglichkeit zu bieten, das jeweils komplexere der beiden Bilder bewerten zu können. Hierfür wurde zunächst ein zufälliges Bilderpaar, das bisher am seltensten angezeigt wurde, abgerufen und dem Teilnehmer anzeigt. Die Einschränkung, dass es sich um das oder eines der am seltensten angezeigten Bilderpaare handeln muss, garantiert, dass alle Bildpaare über alle Teilnehmer gesehen in etwa gleich oft angezeigt werden. Ein Beispielvergleich ist in Abb. 3.3 zusehen.

Vor Beginn der Vorstudie werden zunächst mit einem HTML-Formular von jedem Teilnehmer die E-Mail-Adresse, das Alter, Geschlecht und die höchste Ausbildung abgefragt. Zudem werden mittels JavaScript und PHP noch folgende Informationen abgerufen und gespeichert: Der vom Teilnehmer aktuell verwendete Browser, Größe des Browserfensters, eingestellte Monitorauflösung sowie IP-Adresse. Nach jeder Registrierung wird eine PHP-Session gestartet und in Cookies gespeichert. Das garantiert während der Teilnahme eine korrekte Zuordnung und hilft danach, zusammen mit der gespeicherten IP- und E-Mail-Adresse, doppelte Teilnahmen einzelner Teilnehmer zu unterbinden.

Datenbankmodell

Bei jedem der durchgeführten Bildvergleiche wurden verschiedene Informationen gespeichert, um eine ausführliche Analyse zu ermöglichen, wie das Datenbankmodell in Abb. 3.2 zeigt. Dazu gehörte die Dauer, die ein Teilnehmer für jeden Vergleich benötigt hat. Mit JavaScript wurde beim Laden des Bildvergleiches der aktuelle Zeitstempel abgerufen und eine Differenz mit der beim Anklicken aktuellen Zeit in der Datenbank gespeichert. Zudem wurde selbstverständlich jedem Bildvergleich die eindeutige Benutzer-ID zugeordnet sowie die Bildpaar-ID, das als komplex und nicht-komplex bewertete Bild gespeichert. Auf diese Weise können bei der späteren Analyse unter anderen die schwierigsten (längsten) Bildvergleiche anhand der Dauer abgerufen werden oder die durchschnittliche Vergleichsdauer pro Bildpaar oder insgesamt berechnet werden.

Um einfachere Abfragen auf der Datenbank zu ermöglichen, wurden mit Hilfe der Tabelle „Bildpaare“ jeder möglichen Kombination zweier Bildpaare eine eindeutige ID zugeordnet.

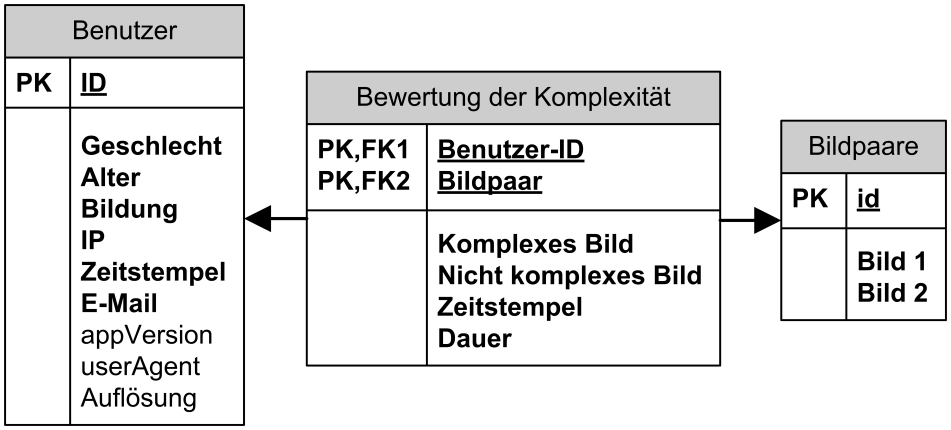


Abbildung 3.2.: Das für die Bewertung der Komplexität (Vorstudie 1) genutzte Datenbankmodell (gekürzte Fassung).

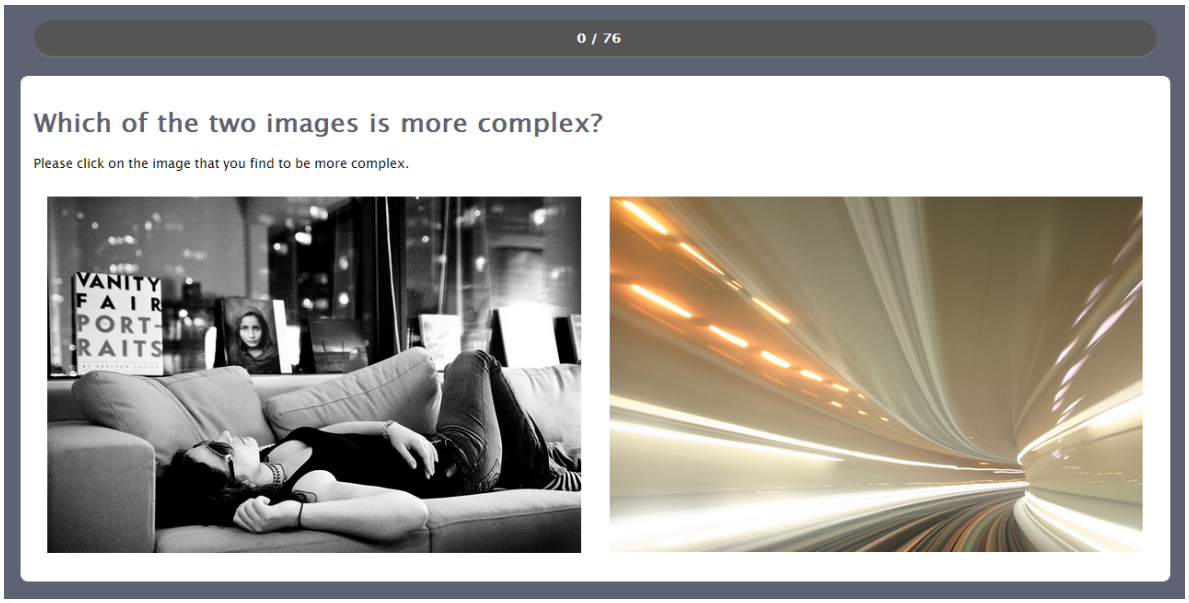


Abbildung 3.3.: Webinterface zur Bewertung der Bildkomplexität. Teilnehmer mussten mit der linken Maustaste auf das aus ihrer Sicht komplexere Bild klicken.

Diese Tabelle wurde im vor der Durchführung der Studie durch ein Skript, das alle möglichen Kombinationen der 20 Bilder berechnete, gefüllt. Nun genügte es, nach der am seltensten (oder gar nicht) vorkommenden Bildpaar-ID zu suchen – außer denen, die ein Benutzer bereits gesehen hat. Die möglichen Bildpaare mussten so auch nicht vom System selbst während der Bewertungsphase kreiert werden.

3.2.2. Durchführung

Die Rekrutierung und Suche nach Teilnehmern erfolgte vor allem durch Verteilerlisten per E-Mail. Um die Teilnehmer nicht zu beeinflussen, wurde zudem absichtlich auf eine Einführung oder Definition der Bildkomplexität verzichtet – es wurden keinerlei weiterführende Informationen hierzu gegeben. Lediglich die Frage, welches der jeweils angezeigten Bilder komplexer sei, wurde gestellt.

Nach einer erfolgreichen Registrierung wurden dem Teilnehmer sofort der erste Bildervergleich angezeigt. Bei 20 Bildern gibt es insgesamt 380 Bildvergleiche, wenn jedes Bild mit jedem verglichen werden soll inklusive vertauschter Positionen (links/rechts). Da 380 Vergleiche sehr viel Zeit in Anspruch nehmen würden, musste jeder Teilnehmer nur 76 Bildpaare vergleichen, was genau 20 % aller möglichen Bildervergleiche entspricht. Dies ist in ca. 5 bis 10 Minuten machbar. Damit die Teilnehmer nicht vorher abspringen, wurde der Fortschritt mit einem Balken visualisiert. Daran konnte erkannt werden, dass innerhalb einer kurzen Zeit ein großer Fortschritt in der Studie machbar ist und insgesamt nur wenig Zeit in Anspruch genommen wird.

Um zu garantieren, dass alle möglichen Bildervergleiche gleich oft vorkommen, wurden vor dem Anzeigen der Bilder zunächst die zwei Bilder rausgesucht, die in einem gemeinsamen Vergleich am seltensten angezeigt wurden und die Bildpaare, die ein Benutzer bisher noch nicht, auch nicht in vertauschter Reihenfolge, gesehen hat. Handelte es sich hierbei um mehr als ein Bilderpaar, wurde daraus ein zufälliges ausgewählt. Auf diese Weise wurden die Bildvergleiche zufällig generiert und es konnte garantiert werden, dass alle möglichen Bildvergleiche insgesamt über alle Teilnehmer in etwa gleich oft bewertet wurden.

Zudem wurden während der 76 angezeigten Bildvergleiche auch drei Testvergleiche zur Messung der Zuverlässigkeit des Teilnehmers gezeigt. Hierzu wurde beim 10., 20. und 30. Vergleich jeweils das erste, zweite und dritte Bildpaar in umgekehrter Reihenfolge, d.h. das vorher links gezeigte Bild war wurde rechts (und umgekehrt), zur Bewertung angezeigt. Dies diente bei der Auswertung als Maß für die Zuverlässigkeit: Wurden jedes mal oder mindestens bei zwei aus drei malen das gleiche Bild als komplexer bewertet, so galt der Teilnehmer als zuverlässig – anderenfalls wurde er als unzuverlässig eingestuft aus der Auswertung ausgeschlossen.

3.2.3. Ergebnisse

Bei dieser Vorstudie haben insgesamt 43 Personen teilgenommen. Davon waren 23 weiblich und 20 männlich und zwischen 20 und 69 Jahre alt ($M = 31.0$, $SD = 8.9$). Von allen 43 Teilnehmern haben 26 Personen alle Kontrollbilder übereinstimmend mit den ersten drei gezeigten Bildern bewertet und haben damit die höchstmögliche Zuverlässigkeit. 15 Teilnehmer haben nur zwei von drei Kontrollbilder korrekt, während zwei Personen nur eines aus drei richtig bewertet haben. Für die nachfolgenden Analysen wurden nur die Daten der Teilnehmer genutzt, die mindestens zwei aus drei Kontrollbilder übereinstimmend

(a) (b) (c)

Abbildung 3.4.: Diese Abbildung zeigt die als am komplexesten (a), als mittel (b) und als am wenigsten komplex (c) bewerteten Bilder, die für die zweite Vorstudie sowie die Hauptstudie ausgewählt wurden.

bewertet haben. Alle nachfolgenden Zahlen und Analysen basieren somit nur noch auf den 41 zuverlässigen Teilnehmern.

Aus den durchgeführten Analysen konnten jeweils das am meisten, mittel und am wenigsten komplexe Bild ausgewählt werden, siehe Abb. 3.4.

Insgesamt wurden von 3268 nur aus den oben beschriebenen Gründen 3116 Vergleiche bzw. Bewertungen betrachtet. Hiervon wurde Bild (a) aus Abb. 3.4 276 mal als das komplexere Bild bewertet, das nächst folgende Bild nur 240 mal. Bild (b) wurde 160 mal und Bild (c) nur 48 mal als das Komplexere bewertet.

Eine Analyse der statistischen Signifikanz zeigt, dass das als am komplexesten bewertete Bild signifikant komplexer ist als die beiden als mittel und wenig komplex bewerteten Bilder: $X^2(1) = 17.00$, $p < .05$, $X^2(1) = 13.24$, $p < .05$. Des Weiteren ist auch das als mittel komplex bewertete Bild signifikant komplexer als das als am wenigsten komplexe Bild: $X^2(1) = 5.94$, $p < .05$.

Eine ausführlichere Analyse der Daten zeigt zudem auch, dass die durchschnittliche Vergleichsdauer über alle Vergleiche 4.07 Sekunden beträgt. Um Ausreißer und ungültige Werte, die diesen Wert verfälschen könnten, wurden alle negativen und Werte über 120 Sekunden ignoriert. In Abb. 3.5 ist der Bildvergleich abgebildet, der mit 12.7 Sekunden durchschnittlich am längsten gedauert hat und damit auch als der Schwierigste bezeichnet werden kann. Insgesamt wurde diese Bildkombination von neun verschiedenen Teilnehmern bewertet. Von diesen neun haben acht Teilnehmer Bild (b) als komplexer bewertet, lediglich ein Teilnehmer entschied sich für (a). Dagegen hat der schnellste Vergleich durchschnittlich nur 1.4 Sekunden gedauert und wurde von sechs verschiedenen Teilnehmern bewertet. Interessanterweise befindet sich in diesem Vergleich das als am komplexesten bewertete Bild, siehe Abb. 3.6. Offensichtlich war dieser Vergleich für alle sechs Teilnehmer auch sehr einfach, denn neben der Schnelligkeit wurde in allen Fällen Bild (a) als das komplexere der beiden Bilder bewertet.

Die getrennte Auswertung der Ergebnisse nach Geschlechtern hat gezeigt, dass sowohl männliche als auch weibliche Teilnehmer übereinstimmend das gleiche Bild als das Komplexeste bewertet haben. Unterschiede gibt es bei dem am wenigsten komplexen Bild. Die weiblichen

(a) (b)

Abbildung 3.5.: Längster Bildvergleich bei der Frage nach der Komplexität. Durchschnittlich hat eine Bewertung dieser Bildkombination 12.7 Sekunden gedauert. Von neun Teilnehmern haben acht Bild (b) als komplexer bewertet, lediglich ein Teilnehmer bewertete (a) als das komplexere Bild.

(a) (b)

Abbildung 3.6.: Kürzester Bildvergleich bei der Frage nach der Komplexität. Durchschnittlich hat eine Bewertung dieser Bildkombination 1.4 Sekunden gedauert. Alle Teilnehmer haben bei diesem Bildvergleich Bild (a) als das komplexere der beiden Bilder bewertet.

Teilnehmerinnen haben übereinstimmend mit dem endgültigen Ergebnis Bild (c) aus Abb. 3.4 als das am wenigsten komplexe Bild bewertet. Unter den männlichen Teilnehmern war dieses Bild lediglich das am zweit-wenigsten komplexe Bild, an erster Stelle landete ein anderes, ebenfalls schwarz-weißes Bild. Bild (b) aus Abb. 3.4, das als mittel komplex bewertet wurde, landete, übereinstimmend mit dem Endergebnis, sowohl bei den männlichen als auch bei den weiblichen Teilnehmern im Mittelfeld. Unterschiede in den Geschlechtern sind somit quasi nur marginal. Für eine endgültige Bestätigung dieser Frage wäre eine Studie mit deutlich mehr Teilnehmern nötig, um Zufall und geschlechtsunabhängige Effekte ausschließen zu können.

Die Bewertung der Komplexität unter den Bildern aus Abb. 3.1 hat zeigt, dass eine Vorhersage eines Endergebnisses schwierig ist. Beispielsweise besitzt das als am wenigsten komplex bewertete Bild (c) aus Abb. 3.4 durchaus sichtbare harte Kanten beim Übergang zwischen Hintergrund und dem Kopf. Dagegen gab es in Abb. 3.1 Bilder mit deutlich weniger Kanten und dafür flüssigen Übergängen, die unter diesem Gesichtspunkt als weniger komplex bewertet worden wären. Bild (a) aus Abb. 3.4 könnte dagegen eher vorhersagbar gewesen sein: Es scheint eine komplexe Form darzustellen mit vielen Kanten und verschiedenen Farben und Bereichen. Es ist allerdings auf den ersten Blick, vor allem bei den mittel und wenig komplexen Bildern, zunächst keine Regel erkennbar, die auf eine andere Bildauswahl übertragen werden könnte. Die subjektive Einschätzung von vielen Menschen scheint derzeit nicht vorhersagbar und daher auch nicht übertragbar auf einen Algorithmus zu sein.

3.3. Vorstudie 2: Definition graphischer Passwörter

Für diese Studienarbeit dienen die PIN und explizit das Szenario des Bankautomaten als Vorbild. In Deutschland wird die PIN für Bankkarten vom jeweiligen ausstellenden Bankinstitut vorgegeben und kann von dem Kunden nicht geändert werden. Da sich die Hauptstudie so weit wie möglich an der Realität orientieren soll, ist daher der Entschluss gefallen, sowohl die PIN, die als Grundlage dient, als auch die graphischen Passwörter vorzugeben. Zudem soll dadurch auch der so genannte „Generation Effect“[4] vermieden werden. Nach [SG78] steigt die Erinnerungsfähigkeit, wenn die Passwörter von den Benutzern selbst generiert werden im Gegensatz zu vorgegebenen Passwörtern, die von den Benutzern nur gelesen werden können. Diese Tatsache spricht ebenfalls gegen die Möglichkeit, den Teilnehmern in der Hauptstudie das Passwort selbst definieren zu lassen. Zwar lassen sich PINs problemlos automatisch kreieren, indem mit einem Algorithmus eine zufällige vierstellige Zahl generiert wird. Jedoch existiert ein solches Verfahren nicht für graphische Passwörter. Bei solchen graphischen Passwörtern ist es wichtig, dass sie einen gewissen Sinn und Bezug auf das jeweilige Bild bieten. Aus diesen Gründen fiel die Entscheidung, durch Menschen generierte graphische Passwörter zu verwenden, wofür die zweite Vorstudie nötig wurde.

[4]Deutsch: Erzeugungseffekt oder Generierungseffekt

3.3.1. Systemimplementierung

Für die Definition der graphischen Passwörter musste ein hierfür neuartiges Webinterface mit einem an ein solches bildbasiertes Authentifizierungssystem angepassten Datenbankmodell entwickelt werden. Der Fokus lag dabei auf einer für den Teilnehmer einfachen und intuitiven Eingabe der Passwortpunkte mit entsprechenden Rückmeldungen über die erfolgte Eingabe.

Webinterface

Die graphischen Passwörter wurden über ein eigens dafür entwickeltes Webinterface gesammelt. Dazu mussten sich Benutzer zunächst registrieren und bestimmte Daten angeben, die für die spätere Analyse und Auswertung herangezogen werden konnten. Dazu gehören die obligatorischen Angaben des Geschlechts, Alters, Ausbildung sowie der Vor- und Nachname und die E-Mail-Adresse. Um mögliche Effekte zu verhindern, die durch die Teilnahme von Benutzern, die bereits an der ersten Vorstudie teilgenommen haben, entstehen könnten, wurde die E-Mail-Adresse mit der Teilnehmerdatenbank der ersten Vorstudie abgeglichen – bei einer Übereinstimmung wurde der jeweilige Benutzer zur Teilnahme nicht zugelassen. Des Weiteren dient die E-Mail-Adresse, gemeinsam mit der gespeicherten IP-Adresse des Teilnehmers und einem Cookie, dazu, mehrfache Teilnahmen eines Benutzers so gut wie möglich zu verhindern. Zusätzlich wurden noch der vom Benutzer verwendete Browser und das Betriebssystem, die Bildschirmauflösung sowie die Größe des Browserfensters gespeichert.

Die Eingabe der graphischen Passwörter erfolgte durch Klicken mit der linken Maustaste. Die Eingabekoordinaten wurden mit Hilfe von jQuery registriert und auf die Bildkoordinaten übertragen. An den entsprechenden Koordinaten wurden mit Hilfe des jsDraw2DX-Pakets[5] JavaScript-Objekte in Form von Kreisen erzeugt, welche die Passwortpunkte darstellten. Zudem wurden die Passwortpunkte untereinander mit Linien-Objekten verbunden, um die Visualisierung geometrischer Objekte, die mit den Passwortpunkten gebildet werden können, zu ermöglichen. Handelte es sich um ein Bild mit Saliency Mask, so musste geprüft werden, ob sich hinter der jeweiligen Koordinate die Saliency Mask befindet. Da der Farbton der Saliency Mask auf allen Bildern einmalig war, konnte dies nur ein einfaches PHP-Skript realisiert werden, das lediglich den Farbton an der anklickten Koordinate mit dem der Saliency Mask abgeglichen hat. Handelte es sich um den gleichen Farbton, so wurde die Eingabe verweigert, ein Passwortpunkt konnte an dieser Stelle nicht gesetzt werden.

[5] http://jsdraw2dx.jsfiction.com/

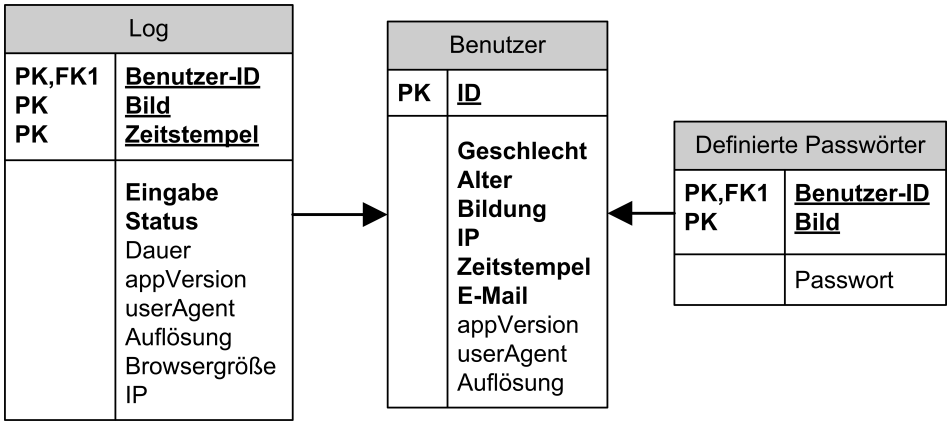


Abbildung 3.7.: Das für die Definition der graphischen Passwörter verwendete Datenbankmodell.

Datenbankmodell

Einen Überblick des für diese Vorstudie genutzten Datenbankmodells bietet Abb. 3.7. Neben der obligatorischen Benutzertabelle für die Speicherung üblicher Daten, insbesondere des Alters, Geschlechts und Bildung, wurden zur Vermeidung doppelter Teilnahmen auch die E-Mail- sowie IP-Adresse gespeichert. Des Weiteren wurden auch bei dieser Vorstudie Informationen über des vom Teilnehmer genutzten Systems gespeichert.

Da ein vom Teilnehmer definiertes graphisches Passworts nur im Falle einer korrekten Verifizierung in die Datenbank geschrieben werden soll, ist der Entschluss gefallen, diese Verifizierung für eine mögliche nachträgliche Auswertung zu speichern. Erst nachdem ein Teilnehmer das jeweilige Passwort korrekt verifiziert hat, wurde dieses in die Tabelle der definierten Passwörter geschrieben. Hier wurde neben dem eigentlichen Passwort bzw. den Passwortpunkten sowie des als Grundlage dienenden Bildes auch die Benutzer-ID des Teilnehmers, der dieses Passwort definiert hat, gespeichert. Durch die gewählte Definition des Primärschlüssels in dieser Tabelle (Benutzer-ID und Bild) wurde bereits durch das Datenbankdesign verhindert, dass ein Teilnehmer versehentlich, bspw. durch mehrmaliges bestätigen oder Neu-Laden des Webinterfaces, ein Passwort mehr als ein mal definiert. Die gewählte Primärschlüsselkombination gewährleistet, dass pro Bild ein Teilnehmer maximal ein graphisches Passwort definieren kann.

3.3.2. Durchführung

Als Grundlage für die Generierung der graphischen Passwörter dienen die in der ersten Vorstudie ausgewählten Bilder mit hoher, mittlerer und geringer Komplexität (Abb. 3.4) jeweils mit und ohne Saliency Mask. Für jedes dieser insgesamt sechs Bilder muss ein Teilnehmer der Vorstudie jeweils ein graphisches Passwort definieren. Für die PINs wurden 10 zufällige Studenten aus dem Universität gebeten, eine beliebige, nicht-triviale vierstellige Zahl

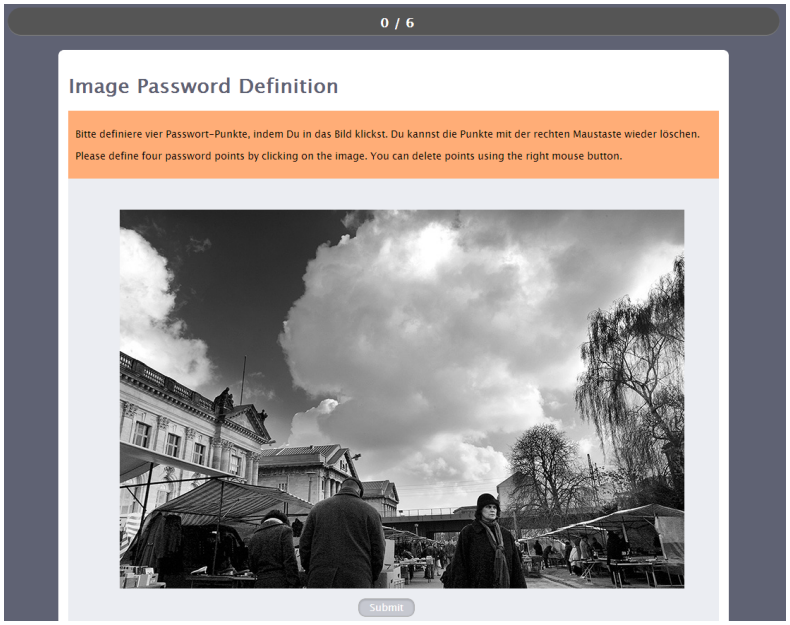


Abbildung 3.8.: Aus den insgesamt sechs Bildern wurde immer ein zufälliges Bild angezeigt, auf dem der Benutzer das graphische Passwort definieren musste – hier handelt es sich um ein Bild ohne Saliency Mask.

aufzuschreiben. Diese PIN durfte nicht aus mehr als zwei gleichen Ziffern hintereinander bestehen.

Die graphischen Passwörter mussten auf dem beschriebenen Webinterface definiert werden. Die Teilnehmer wurden per E-Mail angeschrieben und gelangten durch den versandten Link zunächst auf ein Registrierungsformular sowie kurze Beschreibung der Vorstudie. Nach Abschluss der Registrierung gelangte der Teilnehmer sofort zur Passwortdefinition. Das dafür programmierte Webinterface zeigte immer ein zufälliges Bild an, auf dessen Grundlage noch kein graphisches Passwort von dem jeweiligen Teilnehmer definiert wurde. Die Größe des Bildes orientierte sich immer an der jeweiligen Größe des Browserfensters – das Bild wurde immer so groß wie möglich angezeigt, wie in Abb. 3.8 zusehen ist. Zusätzlich zum Bild wurde immer eine Hinweisbox mit Hilfestellungen zur Benutzung des Webinterfaces angezeigt. Um ein möglichst breites Spektrum an Teilnehmern abzudecken, wurden die Hilfestellungen sowohl in deutscher als auch in englischer Sprache angezeigt.

Die Teilnehmer konnten bei der Passwortdefinition mit der linken Maustaste die Passwortpunkte an einer beliebigen Stelle im Bild setzen. Handelte es sich bei dem jeweiligen Bild um eines mit Saliency Mask, so wurde der gesperrte Bereich auf dem Bild in einem einmaligen, sonst auf nirgends im Bild auftauchenden, roten Farbton angezeigt. In diesem Falle konnte der Benutzer keinen Passwortpunkt in diesen Bereich setzen, siehe Abb. 3.9. Das hinter dem Webinterface stehende Skript prüfte für jede Eingabe, ob der Farbton an dem gesetzten Punkt im Bild dem der Saliency Mask entsprach und akzeptierte oder verweigerte die Eingabe entsprechend. Der gesetzte Passwortpunkt wurde durch einen Kreis visualisiert, in dem

Abbildung 3.9.: In dieser Abbildung wird ein Bild mit Saliency Mask zur Passwortdefinition angezeigt. In diesem Fall kann der Benutzer die roten Bereiche des Bildes nicht anklicken. Zudem wird auch ein angepasster Hinweistext angezeigt, der auf diese Einschränkung hinweist.

zusätzlich durch eine Ziffer die Reihenfolge der gesetzten Punkte angezeigt wurde. Ferner wurden die Passwortpunkte durch eine deutlich sichtbare Linie miteinander verbunden. Hierdurch sollte den Teilnehmern eine Hilfestellung für die Möglichkeit gegeben werden, geometrische Objekte auf den Bildern formen zu können.

Neben dem Setzen von Passwortpunkten konnte der Teilnehmer auch bereits gesetzte Punkte mit der rechten Maustaste löschen. Hierbei wurde immer der jeweils zuletzt gesetzte Passwortpunkt gelöscht – dies konnte so lange wiederholt werden, bis kein Punkt mehr vorhanden war. Auf diese Weise bestand die Möglichkeit, die Eingabe komplett zu löschen und nochmal zu wiederholen.

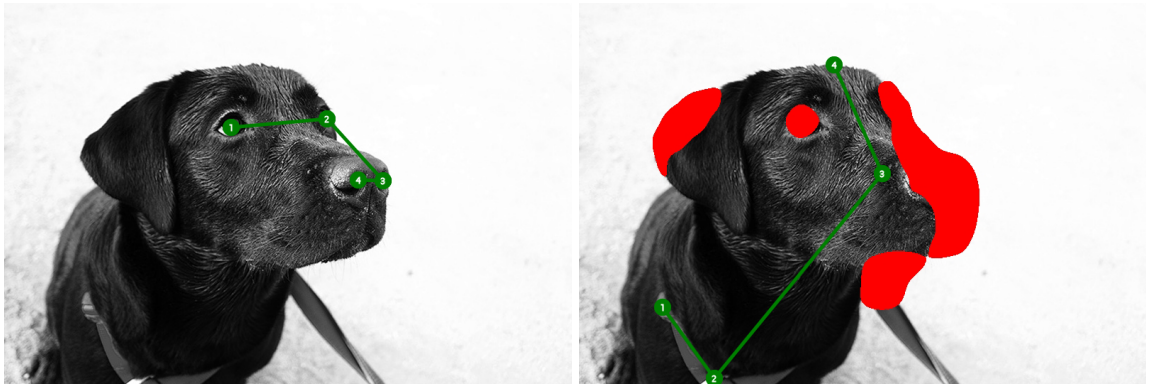
Erst nachdem alle vier Passwortpunkte gesetzt wurden, bestand die Möglichkeit, diese Punkte durch das Klicken auf den vorher deaktivierten Bestätigungsbutton abzuschicken. Anschließend wurde das jeweilige Bild nochmal angezeigt und der Teilnehmer musste durch Eingabe des gerade definierten Passworts genau dieses verifizieren. Schlug die Verifizierung drei mal fehl, so musste das Passwort neu definiert werden und das Prozedere begann von vorne. Das Bildpasswort wurde nur übernommen, wenn der Benutzer es ein mal korrekt verifiziert hat. Auf diese Weise konnte garantiert werden, dass die Teilnehmer sich zumindest etwas Gedanken über das graphische Passwort machen und nicht beliebige, sinnlose Punkte setzen.

Abbildung 3.10.: Das eingegebene Passwort wird durch Linien verbundene Kreise visualisiert – ein Kreis wird nach jedem Klick hinzugefügt. Erst nach der vierten Eingabe wird der Bestätigungsbutton aktiviert.

Ein Zeitfenster oder Limit, innerhalb dem der Teilnehmer ein Passwort definieren musste, gab es nicht. Jeder konnte sich so viel Zeit nehmen, wie nötig. Auch die Anzahl der fehlgeschlagenen Verifizierungen wurde nicht begrenzt, sodass dieses Prozedere von einem Teilnehmer beliebig oft wiederholt werden konnte.

3.3.3. Ergebnisse

Insgesamt haben neun Personen an dieser Studie teilgenommen, davon drei weibliche und sechs männliche. Die Teilnehmer waren zwischen 20 und 48 Jahre alt ($M = 30.0$, $SD = 7.5$). Jeder der Teilnehmer hat sechs graphische Passwörter definiert, für jedes Bild jeweils mit und ohne Saliency Mask eines – niemand hat die Studie vorzeitig abgebrochen. Auf diese Weise wurden insgesamt 54 graphische Passwörter definiert.



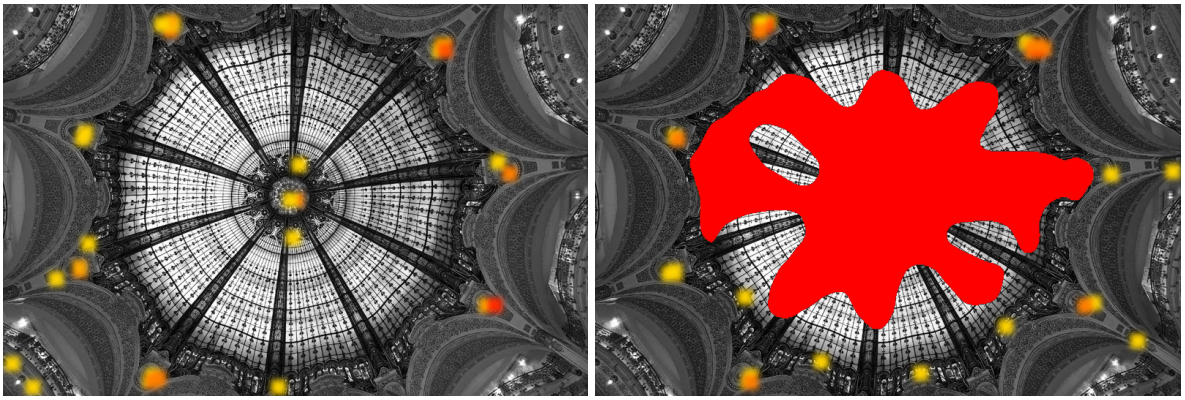
(a) (b)

Abbildung 3.11.: Ein Beispiel eines definierten graphischen Passworts für ein Bild ohne Saliency Mask (a): Der Benutzer orientiert sich an einfach wiedererkennbaren Positionen im Bild, wie in diesem Fall den beiden Nasenlöchern und Augen sowie der im Uhrzeigersinn gesetzten Reihenfolge der Passwortpunkte. Bei dem gleichen Bild mit Saliency Mask (b) waren genau diese Bereiche gesperrt und die Teilnehmer mussten eine andere Strategie wählen.

Erwartungsgemäß hatten alle Passwörter einen gewissen Bezug zum Bild, orientierten sich an bestimmten Punkten oder Objekten. Ein Beispiel eines definierten graphischen Passworts ist in Abb. 3.11 zusehen. Es handelt sich hierbei um das Bild mit der geringsten Komplexität jeweils ohne (a) und mit (b) Saliency Mask. Bei solch einem Bild bietet es sich quasi an, auf Nasenlöcher, Augen, Ohren und andere eindeutige Merkmale die Passwortpunkte zu setzen. Im Beispiel dieses Bildes wurden genau diese Bereiche die Nasenlöcher und Augen genutzt, zudem sind die Passwortpunkte im Uhrzeigersinn angeordnet. Dieses Wissen ermöglicht es definierte Passwörter mit einer höheren Wahrscheinlichkeit zu erraten, was ein erhöhtes Sicherheitsrisiko darstellt. Ein Blick auf Bild (b) verrät, dass genau diese Bereiche der Algorithmus zur Bildung der Saliency Mask korrekt erkannt und deaktiviert hat. Die Teilnehmer mussten bei diesen Bildern eine andere Strategie zur Passwortdefinition und weniger interessante Bereiche im Bild wählen, was ein Erraten des Passworts deutlich erschwert.

Mit Hilfe der Heatmap (Abb. 3.12) lassen sich alle definierten graphischen Passwörter auf einen Blick miteinander auf ihre Ähnlichkeit vergleichen. Die Heatmap visualisiert genau die Bereiche im Bild, die von den Teilnehmern zum Setzen der Passwortpunkte genutzt wurden. Dabei werden alle gesetzten Punkte innerhalb eines Quadrats mit einer Kantenlänge von 50 Pixeln gezählt und farblich kodiert. Gelb bedeutet, dass mindestens ein Passwortpunkt in diesem Bereich gesetzt wurde, Rot steht für sieben Passwortpunkte – der Farbverlauf wurde entsprechend linear berechnet.

Die Heatmap in Abb. 3.12 unterstreicht am Beispiel des am wenigsten komplexen Bildes (c), dass bei der Version ohne Saliency Mask (links) von allen Teilnehmern die Passwortpunkte vor allem im Bereich der Nasenlöcher und Augen gesetzt wurden. Alle Passwörter scheinen



(a)

(b)

(c)

Abbildung 3.12.: Heatmaps der Bildpasswörter des am meisten (a), mittel (b) und am wenigsten komplexen (c) Bildes jeweils ohne (links) und mit (rechts) Saliency Masks. Gelb bedeutet, dass sich zumindest ein, und Rot, dass sich sieben Passwortpunkte innerhalb eines Quadrats mit einer Kantenlänge von 50 Pixeln befinden. Zur besseren Erkennbarkeit der Heatmap wird Bild (a) im Gegensatz zum in der Studie genutzten Original schwarzweiß dargestellt.

hier sehr ähnlich zu sein und sich lediglich durch die Reihenfolge und nur geringfügig abweichende Positionen zu unterscheiden. Dagegen existieren beim gleichen Bild mit Saliency Mask (rechts) eine deutlich größere Bandbreite verschiedener Passwörter, bei denen es fast keine gemeinsamen Punkte gibt. Es existieren lediglich drei Bereiche, die sich mehrere Passwortpunkte reichen. Das bedeutet, dass es, im Gegensatz zu vorher, keine gleichen Passwörter geben kann und sich alle in mindestens einem Passwortpunkt unterscheiden.

Diese Beobachtung kann auch bei dem mittel komplexen Bild (b) getroffen werden. Auch hier wurden die beliebtesten Bereiche durch die Saliency Mask gesperrt. Dazu zählen unter anderem der Kopf der Frau im Vordergrund sowie bestimmte Bereiche der Dächer. Ein Vergleich zwischen links und rechts zeigt, dass genau die Bereiche gesperrt wurden, in denen sich mindestens vier bis sieben Passwortpunkte den gleichen Bereich geteilt haben. Zudem gibt es bei der Version mit Saliency Mask ebenfalls eine deutlich größere Bandbreite an unterschiedlichen Passwortpunkten, bzw. verschiedenen Bereichen, die für das Setzen der Passwortpunkte genutzt wurden.

Etwas anders verhält es sich interessanterweise bei dem komplexesten Bild (a). Sowohl bei der Version mit als auch ohne Saliency Mask scheinen die beliebtesten Bereiche der Passwortpunkte außerhalb des Bereichs der Saliency Mask zu liegen. Die Ursache dafür könnte tatsächlich die hohe Komplexität sein: Überall im Bild, außer in der Mitte, gibt es viele einzelne und kleine Formen bzw. Stellen und Bereiche, die vom Benutzer einfach wiedergefunden werden können, allerdings keine harte Kante darstellen. Daher sind diese Bereiche für den Algorithmus für die Erstellung der Saliency Mask schwer automatisiert zu finden. Es werden somit lediglich Teile des Bildes in der Mitte gesperrt, die allerdings für das Setzen eines Passwortpunktes uninteressant zu sein scheinen.

Auf Grund der Tatsache, dass alle Bildpasswörter von Personen definiert wurden und alle existierenden Einschränkungen durch die Implementierung des Webinterfaces von den Teilnehmern zwingend eingehalten werden mussten, bestand keine Notwendigkeit, die definierten graphischen Passwörter manuell zu überprüfen und ggf. einzelne davon nicht für die Hauptstudie zuzulassen. Bei den zehn durch Studenten der Universität definierten PINs mussten allerdings die zwei folgenden PINs ausgeschlossen werden: „0000“ und „1234“. Auf Grund der vorher gesetzten Beschränkungen, dass es sich um nicht-triviale Zahlenfolgen handeln muss und die gleiche Ziffer nicht mehr als zwei mal aufeinander folgenden darf, wurde dieser Schritt nötig. Für die Hauptstudie wurden daher nur diese übriggebliebenen acht PINs übernommen: „2573“, „3482“, „3721“, „3827“, „6127“, „8144“, „8235“ und „8453“.

4. Hauptstudie

In den durchgeführten Vorstudien wurden eine Reihe von Bildern aus verschiedenen Komplexitätsklassen (Kapitel 3.2) sowie darauf definierte graphische Passwörter und PINs (Kapitel 3.3) gesammelt. Auf Grundlage dieser Daten sollten nun mit der Hauptstudie die Fragen beantwortet werden, ob die Saliency Mask und die Bildkomplexität einen Einfluss auf die Erinnerungsfähigkeit an graphische Passwörter hat und wie sie sich im Vergleich zu PINs verhält, die in der Hauptstudie zudem als Messbasis diente. Konkret wurde hierzu zum einen das Kurzzeitgedächtnis und zum anderen auch das Langzeitgedächtnis untersucht. Jeder Teilnehmer bekam hierzu zwei graphische Passwörter aus zwei unterschiedlichen Bildern sowie eine PIN vorgegeben und musste sich nach bestimmten Intervallen wiederholt damit an einem Webinterface einloggen. Dabei bekam jeder Teilnehmer immer jeweils ein graphisches Passwort eines Bildes mit und ohne Saliency Mask. Das graphische Passwort musste über ein Webinterface direkt auf ein Bild eingegeben werden – die eingegebenen Koordinaten wurden anschließend durch das System mit den vorher definierten verglichen.

4.1. Systemimplementierung

Für die Durchführung der Hauptstudie wurde ein neues Webinterface entwickelt, das sowohl die Eingabe graphischer Passwörter und PINs ermöglicht sowie gleichzeitig auch die Verifizierung der Eingaben übernimmt. Alle Instanzen und Seiten des Webinterfaces wurden komplett zweisprachig sowohl in deutscher als auch in englischer Sprache gehalten, um möglichst vielen Personen die Teilnahme an dieser Studie ermöglichen zu können.

4.1.1. Registrierung

Ein eigenes Interface existierte für die Phase der Registrierung, siehe Abb. 4.4. Die Teilnehmer mussten hierzu Angaben über den Namen, das Alter und Geschlecht sowie den höchsten Bildungsgrad machen, die gemäß des in Kapitel 4.1.4 beschriebenen Datenbankmodells gespeichert wurden. Zudem war die Eingabe der E-Mail-Adresse erforderlich, um das Versenden der Login-Benachrichtigungen nach bestimmten Intervallen zu ermöglichen.

Über PHP und JavaScript wurden noch weitere Informationen über die Teilnehmer bzw. das von ihnen genutzte System abgerufen. Dazu gehören die Attribute „UserBrowser“ und „UserAgent“ zur Extraktion des genutzten Betriebssystems und Browsers. Außerdem wurden die Bildschirmauflösung sowie Größe des Browserfensters und schließlich auch die IP-Adresse und der Zeitstempel der Registrierung abgerufen und zur späteren Analyse

Abbildung 4.1.: Das für die Hauptstudie genutzte Formular zur Registrierung.

sowie im Falle der IP-Adresse zur Vermeidung mehrfacher Registrierungen durch die gleiche Person, in der Datenbank gespeichert.

4.1.2. Eingabe von PINs und graphischen Passwörtern

Die Eingabe der PIN wurde durch ein übliches HTML-Textfeld implementiert, siehe Abb. 4.2. Wie auch bei der Eingabe der graphischen Passwörter, konnten die Teilnehmer die eingegebenen Ziffern während und nach der Eingabe sehen.

Für die graphischen Passwörter wurde ein ähnliches Interface implementiert, wie bereits in der zweiten Vorstudie für das Definieren der graphischen Passwörter (Kapitel 3.3). Hierzu bekamen die Teilnehmer zum Login das jeweilige Bild angezeigt, die Eingabe des graphischen Passworts erfolge mit der Maus, siehe Abb. 4.3 Die Passwortpunkte konnten mit der linken Maustaste gesetzt und mit der rechten Taste konnte der jeweils zuletzt gesetzte Punkt gelöscht werden. Auf diese Weise ermöglichten wir, Eingabekorrekturen durchführen zu können, wie sie auch bei Bankautomaten möglich sind. Ein entscheidender Unterschied zur Vorstudie ist allerdings, dass die Teilnehmer bei der Hauptstudie nicht wussten, ob es sich um ein Bild mit oder ohne Saliency Mask handelt – es wurde immer die Version des Bildes ohne Saliency Mask angezeigt.

Jeder gesetzte Passwortpunkt wurde durch einen Kreis sowie eine Linie zum jeweils vorher gesetzten Punkt visualisiert. Hierbei handelte es sich um JavaScript-Objekte aus dem

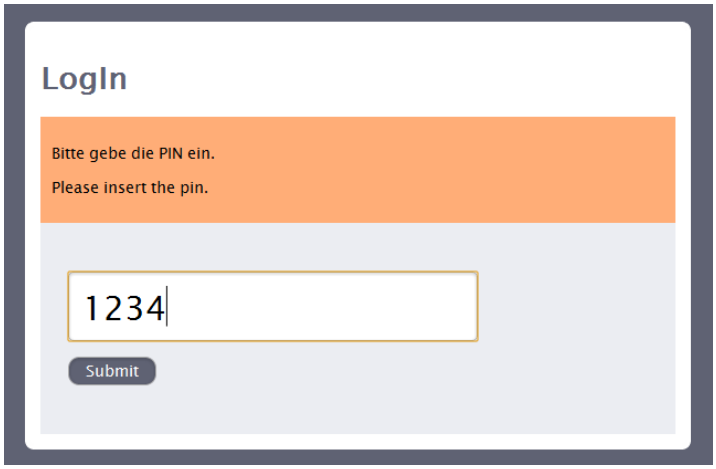


Abbildung 4.2.: Login und Eingabe der vierstelligen PIN. Das Absenden des Formulars war erst nach der Eingabe aller vier Ziffern möglich.

jsDraw2DX-Paket[1]. Jedes dieser Objekte wurde in Arrays gespeichert, um eine Implementierung der Korrekturfunktion zu ermöglichen. Dies bedeutet, dass ein Zugriff auf die Referenz bzw. das Objekt selbst jederzeit möglich war, um dieses bspw. zu löschen. Durch die Verwendung des externen JavaScript-Pakets konnte auf ein bewährtes sowie unter allen gängigen und aktuellen Browser lauffähiges System zurückgegriffen werden, das bereits zeitaufwändige Anpassungen an die verschiedenen Browserengines beinhaltete.

Nach der erfolgten Eingabe und Bestätigung dieser durch eine Schaltfläche im Webinterface, wurden die eingegebenen Koordinaten sofort auf ihre Richtigkeit geprüft. Es musste die Reihenfolge der gesetzten Passwortpunkte übereinstimmen sowie die eingegebenen Koordinaten innerhalb eines Kreises mit einem Radius von 50 Pixeln liegen. Die euklidische Distanz des gesetzten zum definierten Punkt musste somit kleiner oder gleich einem Toleranzwert von 50 Pixeln sein, siehe dazu auch Kapitel 4.4. Es war somit nicht erforderlich, dass die Eingaben exakt auf dem gleichen Pixel liegen, wie die Definition. Dies wäre auf Grund der verwendeten Eingabemethode mit einer Computermaus schlicht zu schwierig oder gar unmöglich gewesen. Ein Beispiel für ein definiertes und vom Benutzer eingegebenes Passwort ist in Abb. 4.1 zusehen. Diese Eingabe wird von dem System nicht akzeptiert, da der dritte und vierte eingegebene Passwortpunkt von der Definition deutlich abweicht, während die ersten beiden Punkte im akzeptierten Bereich liegen. Da mit jedem Login-Versuch die Eingabekoordinaten gespeichert werden, besteht die Möglichkeit, diesen Toleranzwert auch nachträglich zu verändern und eine Analyse mit einer größeren oder kleineren Toleranz durchzuführen.

Für jeden Passworteingabevorgang wird zusätzlich auch die Dauer ab dem Zeitpunkt des ersten gesetzten Passwortpunktes bis zum Absenden der Eingabe gespeichert. Hierzu werden zwei Zeitstempel mit JavaScript abgerufen und anschließend deren Differenz in der

[1] http://jsdraw2dx.jsfiction.com/

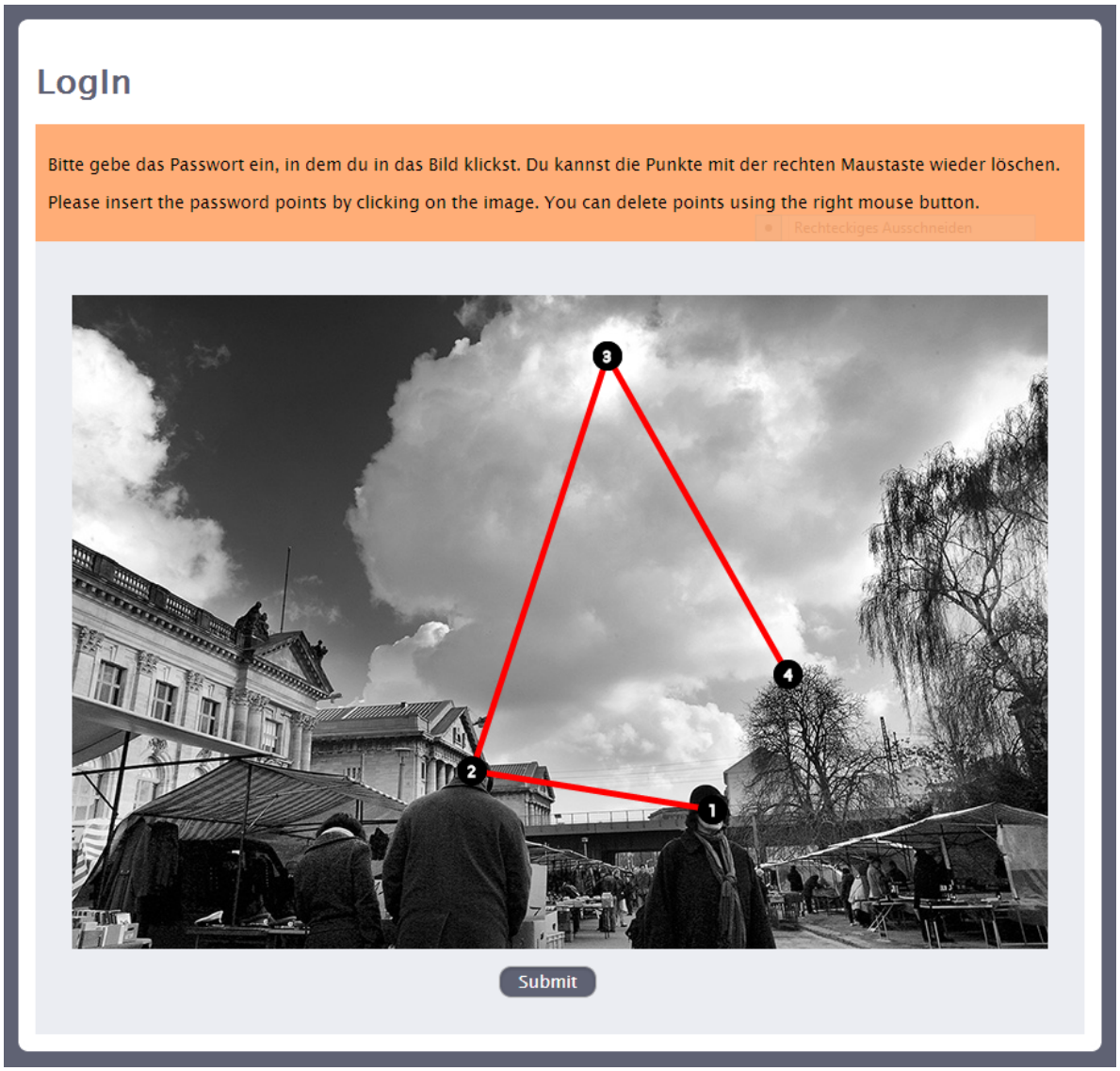


Abbildung 4.3.: Login und Eingabe mit dem graphischen Passwort erfolge mit der linken Maustaste. Die rechte Maustaste konnte für das Löschen des jeweils zuletzt gesetzten Passwortpunktes genutzt werden.

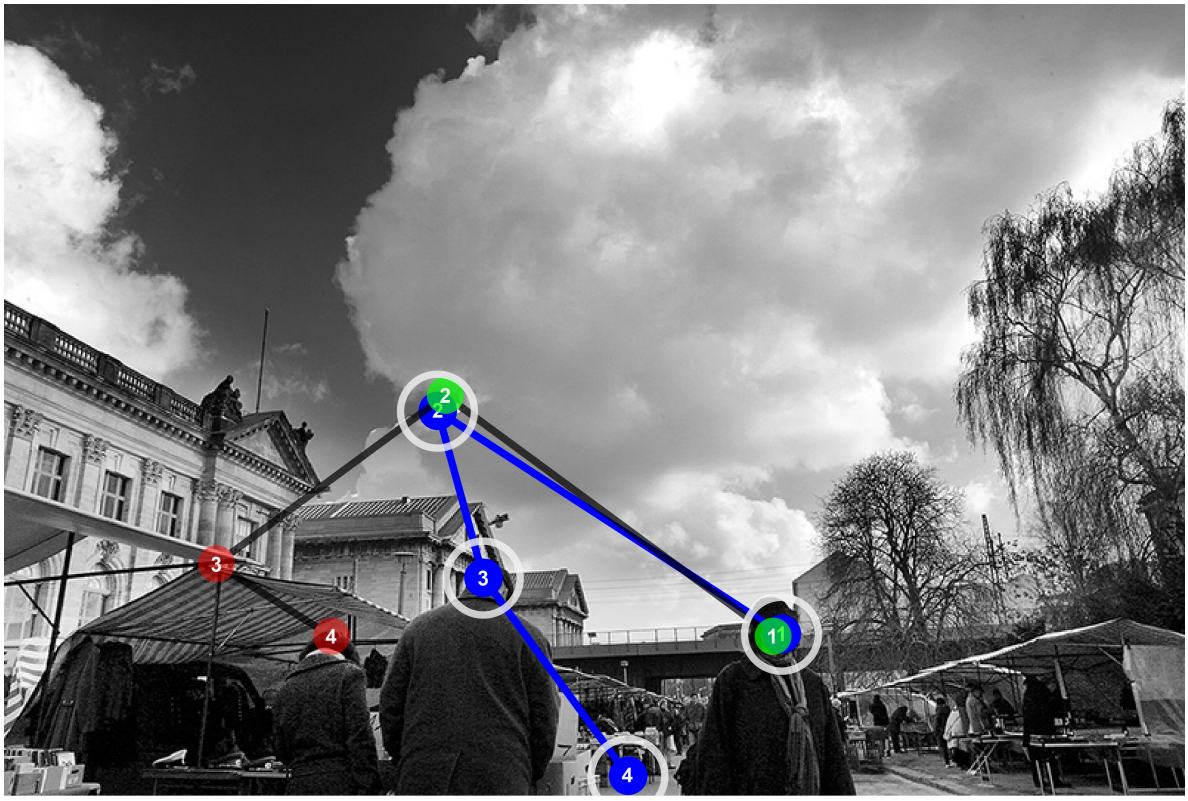


Abbildung 4.4.: Ein Beispiel eines definierten (blau) sowie eingegebenen graphischen Passworts durch einen Benutzer. Die vom System akzeptierten sind Grün, die falschen Eingaben in Rot dargestellt. Die weißen Kreise visualisieren den für jeden definierten Passwortpunkt durch das System noch akzeptierten Eingabebereich.

Datenbank zusammen mit dem jeweiligen Login-Versuch in Millisekunden gespeichert. Wie bei der Registrierung wurden auch mit jedem Login-Versuch der verwendete Browser sowie Betriebssystem, die Bildschirmauflösung und die Größe des Browserfensters gespeichert. Zudem wird selbstverständlich auch die Eingabe selbst in das Log geschrieben: Handelte es sich um ein graphisches Passwort, so werden die vom Teilnehmer getätigten Eingabekoordinaten gespeichert, um eine nachträgliche Analyse zu ermöglichen. Handelte es sich um eine PIN, so wird die eingegebene Ziffernfolge gespeichert.

Um zu gewährleisten, dass nur solche Personen an der Studie teilnehmen, die den Registrierungsvorgang vollständig abgeschlossen haben, wurde erst zum Schluss, nachdem alle nötigen Schritte durchlaufen wurden, das Attribut „Registrierung-Vollständig“ in der Datenbank gesetzt. Nur in dem Fall konnte ein Teilnehmer an den weiteren Phasen der Studie teilnehmen.

4.1.3. Vergabe graphischer Passwörter und Verifizierung

Direkt im Anschluss an die Registrierung folgte die Vergabe des graphischen Passwörter an den Teilnehmer. Um zu gewährleisten, dass alle graphischen Passwörter über alle Teilnehmer möglichst gleichmäßig verteilt sind, werden zunächst aus allen definierten Passwörtern und Bildern so genannte „Bildpasswortpaare“ gebildet, siehe Tabelle „Bilderpaare“ im Datenbankmodell in Abb. 4.5. Dies ermöglicht zum einen eine einfachere Auswertung und Analyse. Zum anderen werden nun unter den am seltensten vergebenen Bildpasswortpaaren ein Bildpasswortpaar zufällig ausgewählt und an den jeweiligen Teilnehmer zugeteilt. Dies führt zu einer möglichst genauen Gleichverteilung aller existierender Bildpasswortpaare über alle Teilnehmer. Es sollte vermieden werden, dass manche Bildpasswortpaare öfter, andere seltener vergeben werden. Da allerdings keine Sicherheit darüber besteht, dass alle Teilnehmer bis zum Ende an der Studie teilnehmen, kann es dennoch passieren, dass am Ende der Studie bei Betrachtung der bis zum Schluss genutzten Bildpasswortpaare eine Ungleichverteilung vorhanden ist.

Im Anschluss an jede Vergabe von Bildpasswortpaaren oder PIN musste eine Verifizierungsphase durchlaufen werden. Hierzu wurde von jedem Teilnehmer das zuvor vergebene Passwort nochmals abgefragt. Implementiert wurde dies durch das beschriebene Interface zur Eingabe von graphischen Passwörtern sowie PINs. Zudem wurde jeder Versuch der Verifizierung bereits intern im Log gespeichert, um eine anschließende Auswertung des Kurzzeitgedächtnisses zu ermöglichen. Schlägt die Verifizierung drei mal hintereinander fehl, so wird das gleiche Passwort nochmals angezeigt – dieses Prozedere wird so lange wiederholt, bis das Passwort ein mal korrekt eingegeben und verifiziert wurde.

Zudem wurden während der gesamten Registrierungs- und Verifizierungsphase auch Tastenkombinationen über JavaScript beobachtet, die zum Erstellen von Screenshots und Kopieren dienen, um so mögliche Strategien der Teilnehmer aufzudecken. Falls eine oder mehrere solcher Tastenkombinationen erkannt wurden, wurde dies ebenfalls in der Datenbank gespeichert. Allerdings konnten auf Grund technischer Beschränkungen nicht alle Tastenkombinationen erkannt werden. Beispielsweise wurde die Drucken-Taste, welche unter Windows für das Speichern des gesamten Bildschirminhalts dient, nicht an den Browser weitergegeben und konnte daher nicht über JavaScript abgefangen werden. Auch das Erstellen von Screenshots mit externen Werkzeugen konnte von dem Webinterface nicht erkannt werden.

4.1.4. Cronjob für Login-Benachrichtigungen und Überwachung der Studie

Um die Studie für den Teilnehmer so angenehm und unkompliziert wie nur möglich zu gestalten und die dauerhafte Teilnahme möglichst aller Personen zu unterstützen, wurden zu den jeweils entsprechenden Zeitpunkten Login-Benachrichtigungen per E-Mail versandt.

Hierfür lief auf dem Studienserver ein Python-Skript, das die Differenz zwischen der aktuellen Zeit und dem Zeitpunkt des letzten Logins überprüfte. Entsprach dieser Zeitraum einem der vor Beginn der Studie definierten Intervalle, so wurde ein einmaliges Token generiert

und eine Benachrichtigung an den jeweiligen Teilnehmer versandt. Der Login war über die gesamte Studie nur mit einem Token möglich, das auch für die Zuordnung des jeweiligen Teilnehmers diente. Bei dem Token handelte es sich um einen MD5-Hash, bestehend aus dem Unix-Zeitstempel zum Zeitpunkt der Generierung des Tokens in Kombination der internen Benutzer-ID. Dieses Token wurde in der Benutzerdatenbank gespeichert. Um sich am Interface einloggen zu können, bekam jeder Teilnehmer per E-Mail einen bereits generierten Link, der als Übergabeparameter dieses Token enthielt. Das Token wurde von dem Webinterface eingelesen und mit der Datenbank abgeglichen. Da es sich durch die Kombination von interner Benutzer-ID und Zeitstempel um ein eindeutigen und einmaligen String handelte, war auf diese Weise eine eindeutige Benutzerzuordnung möglich. So konnten die in der Registrierungsphase an den Teilnehmer vergebenen Bilder und Passwörter abgerufen sowie mit der Eingabe verglichen werden.

Reagierte ein Teilnehmer nicht auf die Login-Benachrichtigung, so wurde nach 24 Stunden eine Erinnerungsnachricht versandt. Falls ein Teilnehmer nach weiteren 24 Stunden auch darauf nicht reagierte, wurde er durch das Python-Skript gesperrt und so von der weiteren Teilnahme an der Studie ausgeschlossen. Hierzu wurde in der Datenbank, wie im nachfolgenden Kapitel genauer beschrieben, eine entsprechende Anmerkung in die Benutzerdatenbank geschrieben, durch die alle nicht mehr an der Studie teilnehmenden Benutzer erkannt werden konnten.

Damit die versandten E-Mail-Benachrichtigungen nicht fälschlicherweise als Spam aussortiert werden, wurde auf das korrekte Setzen des E-Mail-Headers geachtet. Bewährt hat sich dabei dieses Konstrukt: „From: [Absender-E-Mail-Adresse], To: [Empfänger E-Mail-Adresse], Subject: [Betreff], Mime-Version: 1.0 Content-Type: text/plain; charset=ISO-8859-1 Content-Transfer-Encoding: quoted-printable, [Nachrichtentext]“.

4.1.5. Datenbankmodell

Um alle in der Hauptstudie anfallenden Daten sinnvoll zu speichern, wurde das in Abb. 4.5 gezeigte Datenbankmodell entwickelt. Im Wesentlichen bestand dieses aus vier Tabellen. Alle Tabellen wurden in einer gemeinsamen MySQL-Datenbank gespeichert.

Tabelle: Benutzer

Jeder registrierte Teilnehmer wurde zusammen mit seinen in der Registrierungsphase angegebenen und gesammelten Daten in dieser Tabelle einmalig gespeichert. Dabei wurden die Daten auch in die Datenbank geschrieben, wenn der Registrierungsvorgang noch nicht abgeschlossen war. Das für die Teilnahme an der Hauptstudie nötige Attribut „Registrierung-Vollständig“ wurde in dieser Tabelle verwaltet. Erst nach dem Setzen dieses Attributs handelte es sich um einen validen Teilnehmer.

Zudem wurden hier auch die in dem ersten Fragebogen gesammelten Antworten gespeichert. Eine dafür eigenständige Tabelle war nicht nötig, da jeder Teilnehmer diesen Fragebogen nur ein mal auszufüllen hatte.

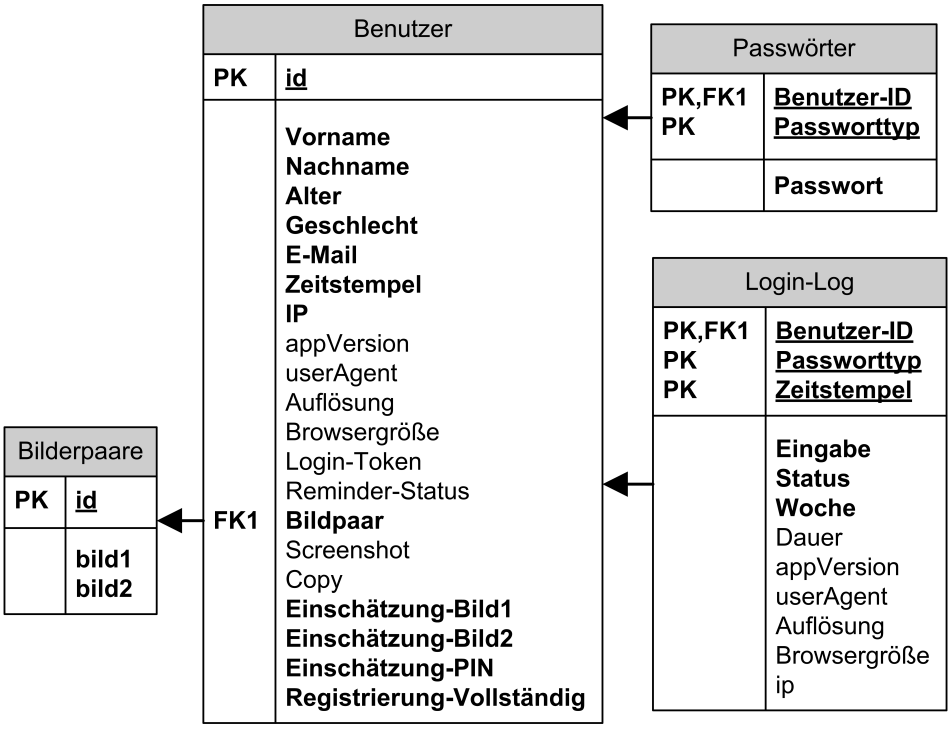


Abbildung 4.5.: Das für die Hauptstudie genutzte Datenbankmodell (gekürzte Fassung).

Die für den Verlauf der Hauptstudie wichtigen Attribute sind „Login-Token“ und „Reminder-Status“. Sollte ein Teilnehmer sich am Interface mit den vergebenen Passwörtern anmelden, so wurde das dafür notwendige Token, das auch zur eindeutigen Zuordnung des Benutzers diente, in dieser Tabelle gespeichert. Erfolgte der Login-Vorgang, so wurde das Token gelöscht und es existierten Login-Logs der entsprechenden Woche in der Tabelle Login-Log. Falls ein Teilnehmer nicht auf die erste E-Mail reagierte, so wurde das Versenden der Erinnerung im Attribut „Reminder-Status“ registriert. War nach insgesamt 48 Stunden das Login-Token immer noch gesetzt, wurde es gelöscht – der Teilnehmer war nun von der Studie ausgeschlossen.

Tabelle: Bilderpaare

Diese Tabelle enthielt alle Kombinationen zwischen Bildern mit und ohne Saliency Mask und wurde vor Beginn der Hauptstudie gefüllt. Während der Studie fanden im Zuge der Passwortvergabe nur lesende Zugriffe darauf statt. Da jeder Benutzer jeweils ein Passwort auf Grundlage eines Bildes mit und ohne Saliency Mask bekam und die beiden vergebenen Bilder zudem ungleich sein sollten, wurde dies in der vorherigen Bildung der Permutationen aller Möglichkeiten der Bildkombinationen ebenfalls berücksichtigt.

Jedem solchen Bilderpaar wurde eine eindeutige Bildpaar-ID zugeordnet. Dies ermöglichte einfache Abfragen nach dem am seltensten vergebenen Bildpaar, das an den Teilnehmer vergeben wurde. Auf diese Weise waren alle Bildpaare und damit Bildreihenfolgen gleich verteilt.

Tabelle: Passwörter

Wurde ein Passwort an einen Teilnehmer vergeben und erfolgreich verifiziert, so wurde zugeordnet zu jedem Benutzer der Passworttyp sowie das vergebene Passwort (die Koordinaten oder die Ziffernfolge der PIN) gespeichert.

Der Passworttyp gab Aufschluss darüber, ob es sich um eine PIN oder um ein graphisches Passwort handelte. Falls letzteres der Fall war, wurde in diesem Attribut der Name des Bildes, auf Grundlage dessen das graphische Passwort definiert wurde, gespeichert. Die dafür nötigen Informationen wurden aus der Datenbank der ersten Vorstudie übernommen, siehe Abb. 3.7. So konnte zu jedem vergebenen Passwort problemlos das dazugehörige Bild mit einer kurzen und schnellen Abfrage abgerufen werden.

Tabelle: Login-Log

Das Login-Log war für fast alle Phasen der Hauptstudie notwendig – sowohl der zur Registrierung gehörenden Verifizierungsphase als auch der Login-Phase. Über das Attribut „Woche“ erfolgte die Zuordnung, ob es sich noch um einen Verifizierungsvorgang (Woche = 0) oder bereits um einen Login-Versuch (Woche > 0) handelt. Zudem wurde die durch das Webinterface vorgenommene Auswertung, ob der Versuch erfolgreich war oder nicht, im Attribut „Status“ festgehalten. So konnte die Anzahl der Versuche eines Teilnehmers pro Passworttyp und Woche gezählt werden – bei einer Anzahl von drei, was drei Fehlversuchen entspricht, wurde das Passwort im Webinterface angezeigt.

Auch die vom Teilnehmer getätigten Eingaben (die eingegebene Ziffernfolge der PIN oder die Koordinaten) wurden festgehalten. Zwar wurde bereits unmittelbar nach der Eingabe eine Auswertung auf Richtigkeit durchgeführt. Durch das Speichern der Eingaben kann allerdings insbesondere bei den graphischen Passwörtern eine nachträgliche Analyse der durchschnittlichen Entfernung eingegebener zu definierter Punkte durchgeführt werden. Zudem kann auf diese Weise nachträglich auch der Toleranzwert vergrößert oder verkleinert werden.

Zusätzlich wurden, wie auch bei der Registrierung, die automatisch erhobenen Informationen über das von dem Teilnehmer zum Login verwendete System für jeden einzelnen Login-Versuch gespeichert, um ändernde Teilnahmeorte ggf. nachvollziehen zu können.

4.2. Gestaltung der Studie

Um möglichst viele Teilnehmer für die Studie zu gewinnen, wurde sowohl über Vorlesungen an der Universität, über interne Mailinglisten als auch über soziale Netzwerke, unter anderem Goolge+ und Facebook, dafür geworben. Es bestand keine allgemeine Teilnahmebeschränkung: Jeder, der nicht bereits bei einer der beiden Vorstudien teilgenommen hat, konnte an der Hauptstudie partizipieren. Um die Studie etwas attraktiver zu gestalten und insbesondere die Motivation an einer konstanten Teilnahme zu fördern, wurden zudem unter allen Teilnehmern, die an der Hauptstudie bis zum Ende teilgenommen haben, insgesamt drei Amazon-Gutscheine im Wert von je 30 Euro verlost.

Die Studie bestand aus einer Verifizierungsphase, in der die Teilnehmer die beiden zugewiesenen graphischen Passwörter sowie die PIN über das Webinterface erfolgreich bestätigen mussten. Anschließend folgten vier Login-Phasen — nach einer (Woche 1), zwei (Woche 2), vier (Woche 4) und acht Wochen (Woche 8) —, in denen die Teilnehmer eine Benachrichtigung per E-Mail erhielten und über das Webinterface jedes der drei Passwörter eingeben mussten. In der Login-Phase gab es, wie auch bei Bankautomaten, drei Login-Versuche pro Passworttyp. Konnte ein Passwort auch beim dritten mal nicht korrekt eingegeben werden, so wurde es den Teilnehmern angezeigt.

Zudem musste sowohl am Ende der Registrierung als auch nach der vierten Woche ein Fragebogen von allen Teilnehmern ausgefüllt werden. Der erste Fragebogen deckte die Selbsteinschätzung der Erinnerungsfähigkeit an die Passwörter durch die Teilnehmer ab. Im Fragebogen wurde unter anderem nach den verwendeten Strategien zum Merken der Passwörter gefragt. Zudem wurde hier nochmals die Frage nach der Bewertung der Bildkomplexität der drei in der Hauptstudie verwendeten Bildern gestellt.

Zu keinem Zeitpunkt haben die Teilnehmer gewusst, ob es sich um ein graphisches Passwort auf Grundlage eines Bildes mit oder ohne Saliency Mask handelt. Bei Passwörtern, die auf Grundlage eines Bildes mit Saliency Mask definiert wurden, wurde die Saliency Mask nicht angezeigt. Zudem wurde den Teilnehmern nicht mitgeteilt, dass es verschiedene Arten von graphischen Passwörtern bzw. Bildern gibt.

4.3. Durchführung

Die Studie bestand aus mehreren verschiedenen Phasen, begonnen von der Registrierungsphase, die auch die Vergabe der graphischen Passwörter sowie deren Verifizierung beinhaltete, über die anschließenden Login-Phasen verteilt über vier Wochen bis hin zum am Ende der Studie durchgeführten Fragebogen.

4.3.1. Registrierungs-, Vergabe- und Verifizierungsphase

Jeder geworbene Teilnehmer bekam zunächst einen Link zu einer Informationsseite, die neben einer Beschreibung und Erklärung der Studie in deutscher und englischer Sprache (siehe Anhang A.2) auch den Link zum Registrierungsformular beinhaltete. Auf der Informationsseite wurden die wesentlichen Ablaufpunkte der Studie erläutert. Neben den Aufgaben wurde insbesondere darauf hingewiesen, dass es sich um eine Langzeitstudie über acht Wochen handelt, die es erfordert, im Laufe dieser acht Wochen mehrmals auf die E-Mail-Benachrichtigungen zu reagieren und an der Studie teilzunehmen. Zudem wurde das Interface zur Eingabe der graphischen Passwörter kurz erläutert.

Direkt im Anschluss an die Informationsseite folgte die Registrierung, in der neben persönlichen Informationen auch Angaben über Geschlecht, Alter und Bildungsgrad gemacht werden mussten. Waren die Angaben vollständig, so begann bereits die Vergabe der Passwörter nach dem in Kapitel 4.1.3 beschriebenen Verfahren. Hierzu wurden jedem Teilnehmer jeweils ein graphisches Passwort auf Grundlage eines Bildes mit und ohne Saliency Mask sowie eine PIN zugeteilt. Bei den Bildern handelte es sich jedoch nie um das gleiche Bild, da jeder Benutzer immer zwei Bilder unterschiedlicher Komplexitätsklassen haben sollte. Zudem war so auch die Unterscheidung der vergebenen graphischen Passwörter möglich – bei zwei gleichen Bildern wäre nicht sofort klar, welches der beiden Passwörter nun gefragt ist. Jedes dem Benutzer zugeteilte Passwort musste ein mal erfolgreich verifiziert werden. Schlug die Verifizierung drei mal fehl, so wurde das Passwort nochmals angezeigt. Die Vergabephase der Passwörter war erst abgeschlossen, nachdem alle drei erfolgreich verifiziert wurden.

Nach der Verifizierung wurden die Teilnehmer nach einer persönlichen Einschätzung über die Schwierigkeit der Erinnerungsfähigkeit an die Passwörter gefragt. Dabei sollten sie sowohl die zwei graphischen Passwörter als auch die PIN auf einer Likert-Skala bewerten. Die Fragen und Antwortmöglichkeiten waren wie folgt formuliert: „Bewerte die folgende Aussage: Ich denke, ich kann mich ohne Probleme an das erste bildbasierte Passwort / zweite bildbasierte Passwort / die PIN erinnern kann“ – 1: „Ich stimme gar nicht zu“ bis 5: „Ich stimme voll und ganz zu“.

Erst nachdem dieser Fragebogen ausgefüllt wurde, war der Registrierungsvorgang erfolgreich abgeschlossen und die Teilnehmer wurden für diese Studie angenommen. Wurde die Registrierungsphase zu irgendeinem Zeitpunkt vorzeitig abgebrochen, bestand keine Möglichkeit an der Teilnahme.

4.3.2. Login-Phase

Nach einer, zwei, vier und acht Wochen erfolgten die Benachrichtigungen mit der Bitte, sich an dem Webinterface mit den vorher vergebenen Passwörtern einzuloggen. Dazu mussten alle drei, sowohl die zwei graphischen Passwörter als auch die PIN, eingegeben werden. Falls die Teilnehmer nicht auf diese E-Mail reagierten, folgte nach 24 Stunden eine Erinnerungsnachricht. Wenn nach weiteren 24 Stunden immer noch keine Login-Versuche am Webinterface erfolgten, wurde der Teilnehmer von der Studie ausgeschlossen. Dies ist nötig, damit es keine Verzerrungen bei der Langzeitstudie gibt: Falls die Teilnehmer nicht genau nach einer, zwei, vier und acht Wochen teilnehmen sondern erst etwas später, ist die Vergleichbarkeit der Ergebnisse untereinander nicht gegeben, da die unterschiedlichen und längeren Zeiträume einen negativen Einfluss auf die Erinnerungsfähigkeit haben können.

Die Reihenfolge der angezeigten Bildern bzw. PIN war bei jedem Login zufällig, um Einflüsse durch die Abfragereihenfolge zu minimieren. Die Login-Eingaben wurden sofort auf ihre Richtigkeit geprüft. Im Falle einer fehlerhaften Eingabe eines der Passwörter, musste es der Teilnehmer nochmals eingeben. Wie bei Bankautomaten üblich gab es auch bei diesem Interface insgesamt drei Eingabeversuche. Nach dem dritten fehlerhaften Eingabeversuch wurde das jeweilige Passwort dem Teilnehmer angezeigt. Auf diese Weise wurde auch bei anderen, ähnlichen Studien vorgegangen [DLDH09, WDL08, WWB+05b], u.a. um das vorzeitige Abspringen von Teilnehmern wegen Frustration zu verhindern. Ob, wann (in welcher Woche) und welches Passwort einem Teilnehmer gezeigt wurde, kann durch das Log in der späteren Analyse jederzeit nachvollzogen werden.

4.3.3. Fragebogen

Nach der vierten Woche wurde ein Fragebogen an alle bis dahin noch aktiven Teilnehmer versandt. Mit diesem Fragebogen wurde sowohl auf die Vorstudien als auch auf die Hauptstudie eingegangen. Bewertet sollte die Komplexität der drei für die Hauptstudie ausgewählten Bildern auf einer Likert-Skala. Hierzu wurden die drei Bilder untereinander angezeigt mit den Bewertungsvorgaben von „1 – wenig komplex“ bis „5 – sehr komplex“.

Der Fokus und Schwerpunkt des Fragebogens lag allerdings auf der Hauptstudie und den dort von den Teilnehmern verlangten Aufgaben. Gebeten wurden die Teilnehmer um eine ehrliche Antwort, mit dem Hinweis dass dies keinerlei Verringerung bei den Gewinnchancen hat, bei der Frage, ob und, wenn ja, welche Hilfsmittel zur Verbesserung der Erinnerungsfähigkeit genutzt wurden. Vorgegeben waren folgende Antwortmöglichkeiten:

- Screenshot
- Passwort kopiert
- Foto gemacht
- Von anderen Personen helfen lassen
- Eselsbrücke (mit einem zusätzlichen Textfeld zur Beschreibung der Eselsbrücke)

- Sonstiges (ebenfalls mit einem zusätzlichen Textfeld zur Beschreibung)
- Keine

Zudem wurde auch direkt auf die vergebenen Passwörter eingegangen. Die Frage: „Gab es bestimmte Elemente im Bild, die dir das Merken des Passworts vereinfacht haben? Wenn ja, beschreibe diese Elemente bitte.“ sollte Aufschluss darüber geben, ob und welche Techniken und Strategien die Teilnehmer zum Merken der graphischen Passwörter genutzt haben, die direkt auf die Bildauswahl zurückzuführen sind. Möglicherweise existieren bestimmte persönliche Verbindungen zu einem Bild, die nur für den einzelnen Teilnehmer sichtbar sind.

Auch die Schwierigkeit sich an die graphischen Passwörter und die PIN zu erinnern, sollte von den Teilnehmern bewertet werden. Die Frage lautete: „Wie schwer war es für dich, das jeweilige Passwort zu merken? Bitte bewerte die Schwierigkeit auf einer Skala von 1 (einfach) bis 5 (schwierig)„. Hierzu wurde zudem das an die Benutzer vergebene graphische Passwort zusammen mit dem Bild angezeigt. Da die Passwörter immer in zufälliger Reihenfolge abgefragt wurden, war dies nötig, um eine eindeutige Zuordnung zu den Passwörtern zu ermöglichen.

Ferner wurde auch gefragt, an welchen Orten die Teilnehmer an der Studie üblicherweise teilgenommen haben, um mögliche durch die Umgebung entstehende Einflüsse zu erkennen. Folgende Antwortmöglichkeiten waren vorgegeben:

- Zuhause
- An der Uni / Arbeit
- In der Straßenbahn
- In der Bibliothek
- Sonstiges (mit einem zusätzlichen Textfeld zur genaueren Beschreibung)

Schließlich wurden die Teilnehmer nach der Anzahl von ihnen im Alltag regelmäßig verwendeten Passwörter gefragt. Dies kann ebenfalls einen Einfluss auf die Erinnerungsfähigkeit haben. Denkbar wäre, dass mit der Anzahl verschiedener Passwörter die Erinnerungsfähigkeit abnimmt oder es andere Einflüsse darauf gibt.

4.4. Datenanalyse

Zur Messung und Feststellung der Erinnerungsfähigkeit eignen sich mehrere Messgrößen und Faktoren, die allesamt in der durchgeführten Studie erhoben wurden. Um die Vergleichbarkeit mit anderen, vorher durchgeführten Studien zu ermöglichen, wurden die in dieser Studie verwendeten Passworttypen untereinander durch die Anzahl der fehlgeschlagenen Login-Versuche verglichen. Ob ein eingegebenes Passwort korrekt bzw. falsch ist und vom System akzeptiert bzw. abgelehnt wird, hängt davon ab, wie groß die euklidische Distanz der eingegebenen Passwortpunkte zu den jeweils definierten Passwortpunkten ist. Akzeptiert

wurde eine Eingabe, wenn die euklidische Distanz aller eingegeben Passworte kleiner oder gleich von 50 Pixeln zu den jeweils definierten Punkten war – alles über diesen Toleranzwert hinaus führte zu einer fehlerhaften Eingabe, die durch das Webinterface abgelehnt wurde.

Der Wert von 50 Pixeln wurde in einer früheren Studie über die Sicherheit vorgegebener graphischer Passwörter mit Saliency Masks [BAS12] ermittelt. Dieser Wert hängt direkt mit der Sicherheit und Benutzbarkeit graphischer Passwörter zusammen – beide Faktoren stehen zudem in einem Spannungsverhältnis zueinander. Wird ein zu großer Toleranzwert gewählt, so wird dadurch die Sicherheit negativ beeinflusst. Mit einem steigenden Wert werden schließlich immer mehr Eingaben akzeptiert, zudem verringert sich hierdurch die Anzahl der möglichen Positionen von Passwortpunkten. Dagegen führt ein zu klein gewählter Toleranzwert dazu, dass die Benutzbarkeit sehr stark leidet, da es sehr schwierig oder gar unmöglich wird, den definierten Punkt auf einem Bild exakt zu treffen. Dies würde zu einer sehr großen Frustration bei den Benutzern eines solches Authentifizierungssystems führen – schließlich würde die Akzeptanz eines solchen Systems sehr stark leiden.

Auf Grund der Tatsache, dass die Wahl des Toleranzwertes, wie beschrieben, einen großen Einfluss auf die Erinnerungsfähigkeit an graphische Passwörter hat, wurde daher in der Auswertung zusätzlich auch die euklidische Distanz der von den Benutzern gesetzten Passwortpunkte zu den jeweils definierten Punkten untersucht. Im Gegensatz zur Untersuchung falscher Login-Versuche, basiert diese Vorgehensweise nicht auf einem vorher festgesetzten Toleranzwert, sondern ist völlig unabhängig davon. Dies erlaubt die Betrachtung der Erinnerungsfähigkeit, ohne mögliche negative Effekte einer falsch (zu groß oder klein) gewählten Toleranz.

5. Ergebnisse

Für die Hauptstudie haben sich 69 Teilnehmer registriert und die Verifizierungsphase erfolgreich durchlaufen, davon 14 weiblich und 55 männlich im Alter zwischen 20 und 48 Jahren ($M = 25.3, SD = 5.1$). Im Laufe der Studie sind bis zur vierten Woche 41, bis zur achten Woche sogar 52 Teilnehmer weggefallen. In Hinblick auf eine statistisch aussagekräftige und verwertbare Analyse, die nur gegeben ist, wenn eine gewisse Mindestanzahl an auswertbaren Ergebnissen vorhanden sind, ist der Entschluss gefallen, die Studie über die Erinnerungsfähigkeit des Langzeitgedächtnisses nur bis zur einschließlich vierten Woche auszuwerten. Bei genauerer Betrachtung der Teilnehmerzahlen (siehe Abb. 5.1) wird deutlich, dass in der vierten Woche mit 26 noch mehr als doppelt so viele Teilnehmer aktiv an der Studie teilgenommen haben als in der achten Woche. Von den 26 Teilnehmern waren sechs weiblich und 20 männlich sowie zwischen 21 und 48 Jahre alt ($M = 26.0$, $SD = 5.9$). In Tabelle 5.1 gibt es zudem einen Überblick aller durch diese Studie erlangten und in den nachfolgenden Abschnitten beschriebenen Ergebnisse.

	Messbasis	**Saliency Mask**	**Bildkomplexität**
Gesamt	$F(2, 50) = .756$	N/A	N/A
Kurzzeit	$F(2, 66) = 29.132$*	$t(68) = -2.160$*	$t(22) = 1.719$ $t(21) = -1.356$ $t(23) = 1.169$
Langzeit	$F(2, 50) = .123$	$F(1, 25) = 1.995$	N/A $F(1, 9) = 1.416$ $F(1, 9) = .738$

Tabelle 5.1.: Übersicht aller durch diese Studie erlangten und berechneten Ergebnisse. Alle statistisch signifikanten Werte sind mit einem * gekennzeichnet. Für die Messbasis diente als Messgröße die Anzahl fehlgeschlagener Logins, während für die Analyse der Saliency Mask und Bildkomplexität die durchschnittliche euklidische Distanz zwischen den eingegebenen und jeweils definierten Passwortpunkten als Messgröße genutzt wurde.

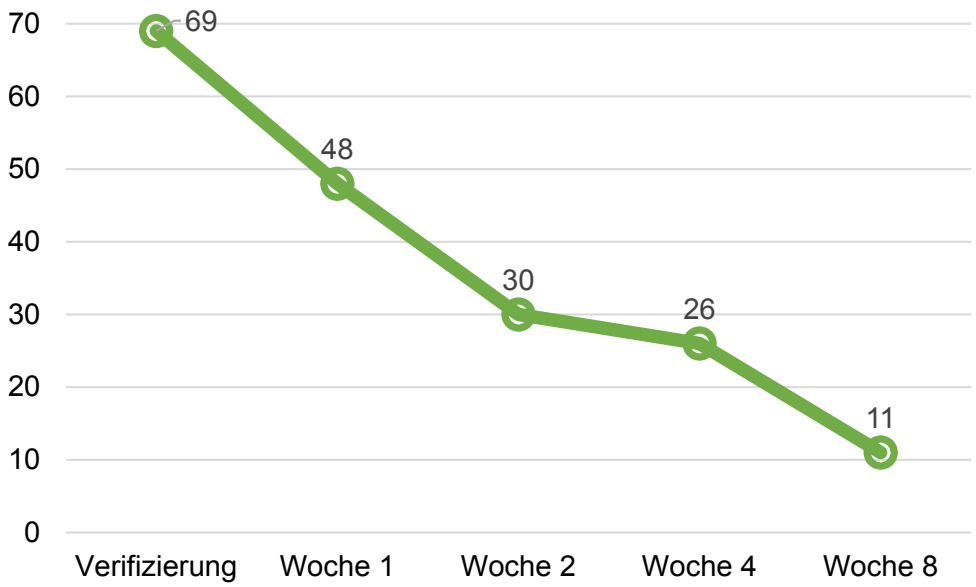


Abbildung 5.1.: Entwicklung der Teilnehmerzahlen über den gesamten Zeitraum von acht Wochen.

5.1. Erinnerungsfähigkeit: Gesamt

Zunächst wurde die Erinnerungsfähigkeit bezüglich der drei in dieser Studie genutzten Passworttypen untersucht: Graphische Passwörter mit und ohne Saliency Mask sowie die vierstellige PIN, die als Messbasis diente. Die zwei Messgrößen, die für die Analyse hauptsächlich genutzt wurden, sind die prozentuale Anzahl erfolgreicher Logins (ein Login ist erfolgreich, wenn einer der drei Login-Versuche für ein Passworttyp vom System akzeptiert wurde), siehe Abb. 5.2, sowie die durchschnittliche Anzahl fehlgeschlagener Login-Versuche, siehe Abb. 5.4. Ferner wurden auch die Anzahl der erfolgreichen Login-Versuche des ersten Versuchs prozentual dargestellt und analysiert, siehe Abb. 5.3. Diese Zahl kann einen Hinweis darauf geben, welche der drei Passworttypen auf Anhieb und ohne Fehlversuche vom Gedächtnis abgerufen werden kann.

Eine Analyse dieser Zahlen zeigt, dass die Erinnerungsfähigkeit der Teilnehmer an alle Passwörter durchweg in der Validierungsphase am besten war ($M = .27$, $SD = .106$). Die durchschnittliche Anzahl fehlgeschlagener Logins ist hier am niedrigsten, dementsprechend ist die Zahl erfolgreicher Validierungen im Vergleich zu den Logins der nächsten Wochen am höchsten. Während nach einer Woche, in der ersten Login-Phase, die durchschnittliche Anzahl der fehlgeschlagenen Logins bei allen drei Passworttypen stieg ($M = 1.62$, $SD = .266$), sank die Zahl in der zweiten Login-Phase nach zwei Wochen wieder ($M = 1.19$, $SD = .271$). Dies kann auf einen gewissen Lerneffekt zurückgeführt werden, der mit der Anzahl der Login-Versuchen entstanden ist. Ein weiterer Grund für diese Entwicklung liegt in dem Design der Studie selbst: Nach drei Fehlversuchen wurde das jeweilige Passwort dem Benutzer angezeigt, sodass dieses nochmals eingeprägt werden konnte. Nach vier Wochen,

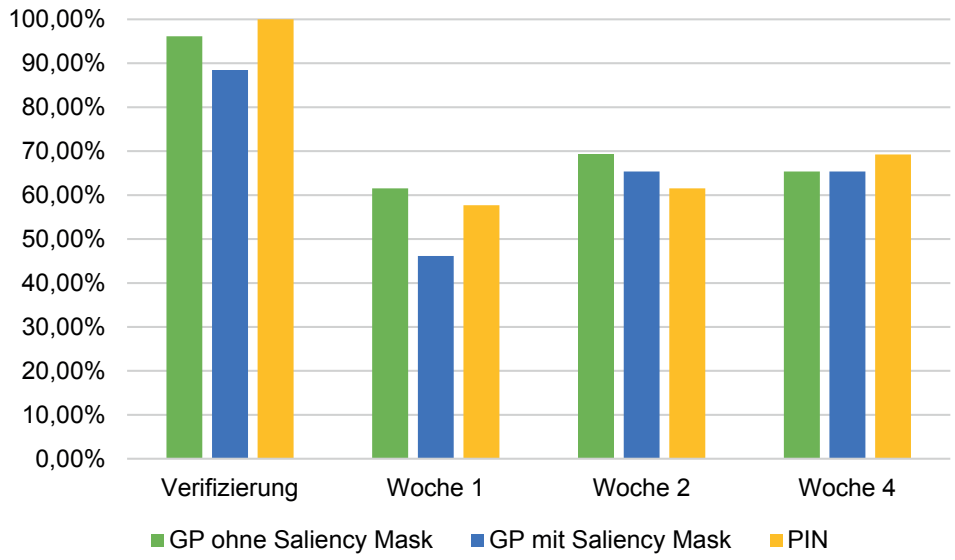


Abbildung 5.2.: Prozentualer Anteil erfolgreicher Logins aller drei Passworttypen gemessen an den 29 Teilnehmern, die bis zur vierten Woche teilgenommen haben.

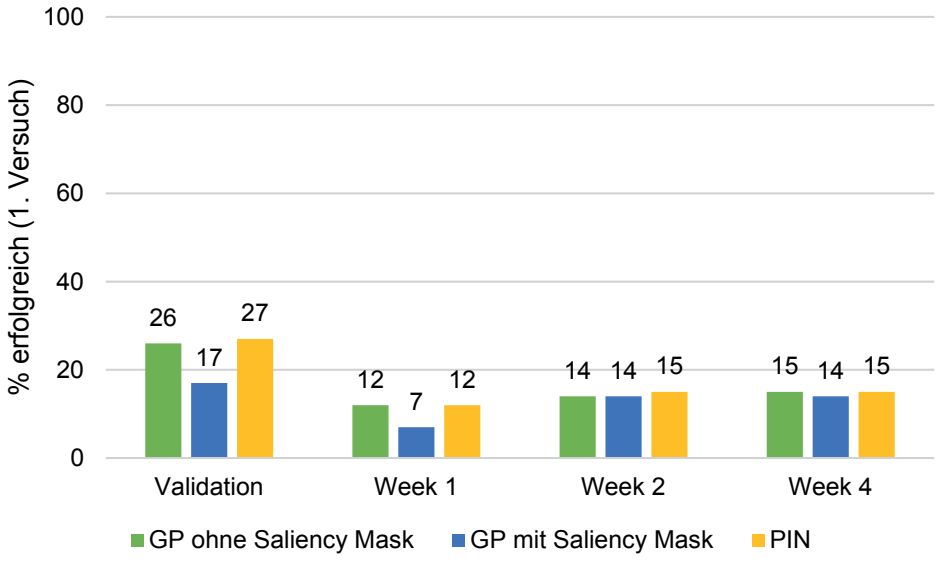


Abbildung 5.3.: Prozentualer Anteil erfolgreicher erster Login-Versuche.

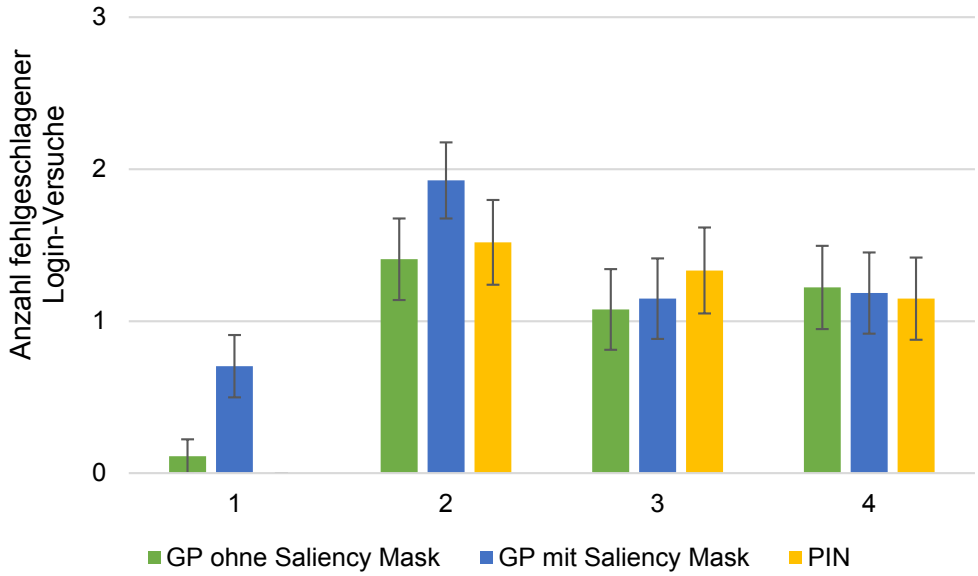


Abbildung 5.4.: Durchschnittliche Anzahl fehlgeschlagener Logins der drei Passworttypen sowie die Standardabweichung über vier Wochen.

in der letzten Login-Phase, gab es keine wesentlichen Veränderungen mehr ($M = 1.187$, $SD = .271$). Zudem wurde mit der Varianzanalyse (ANOVA) getestet, ob die verschiedenen Passworttypen einen Einfluss auf die Erinnerungsfähigkeiten hatten. Die ANOVA ergab, dass es keine statistisch signifikanten Unterschiede zwischen den drei Passworttypen gibt: $F(2, 50) = .756, p = .475$. Auch der Mauchly-Test auf Sphärizität zeigte keine statistisch signifikanten Unterschiede: $X^2(2) = 1.586, p = .452$. Die Effektgröße ist zudem mit $\eta^2 = .029$ sehr klein.

Für eine genauere Analyse der Erinnerungsfähigkeit, insbesondere zur Feststellung von Unterschieden zwischen dem Kurz- und Langzeitgedächtnis, wurde dem von Atkinson und Shiffrin entwickelten Gedächtnismodell [AS68] gefolgt. Demnach fallen Gedächtnisaktivitäten, die innerhalb von 12 bis 30 Sekunden von der Aufnahme bis zum Abrufen erfolgen, in das Kurzzeitgedächtnis. Alles über 30 Sekunden hinaus wird dem Langzeitgedächtnis zugeschrieben. Auf dieser Grundlage wurden die Analysen wie folgt aufgeteilt: Für die Untersuchung des Kurzzeitgedächtnis konnte auf die Daten der Verifizierungsphase zurückgegriffen werden, da jedes gegebene Passwort unmittelbar im nächsten Schritt zur Verifizierung eingegeben werden musste – die Zeitspanne lag bei weniger als 30 Sekunden. Für diese Analyse konnten zudem die Daten aller 69 Teilnehmer genutzt werden, deren Registrierung vollständig war und daher auch die Daten der gesamten Verifizierungsphase vorliegen. Die Daten aus der ersten, zweiten und vierten Woche dagegen dienten für die Analyse des Langzeitgedächtnisses. Um statistisch signifikante und auswertbare Daten zu erhalten, wurden hierfür nur die Daten der Teilnehmer ausgewertet, die bis zur einschließlich vierten Woche aktiv an der Studie teilgenommen haben.

	GP ohne Saliency Mask	GP mit Saliency Mask	PIN
Woche 1	$M = 1.462, SD = 1.392$	$M = 2.000, SD = 1.265$	$M = 1.577, SD = 1.447$
Woche 2	$M = 1.077, SD = 1.354$	$M = 1.154, SD = 1.405$	$M = 1.308, SD = 1.490$
Woche 4	$M = 1.269, SD = 1.430$	$M = 1.115, SD = 1.366$	$M = 1.077, SD = 1.383$

Tabelle 5.2.: Durchschnitt (M) und Standardfehler (SE) der Anzahl fehlgeschlagener Login-Versuche aller Passworttypen nach der ersten, zweiten und vierten Woche.

5.2. Erinnerungsfähigkeit: Kurzzeitgedächtnis

Für die statistische Analyse des Kurzzeitgedächtnisses wurde das ANOVA-Verfahren mit wiederholten Messungen auf Grundlage der Daten aller 69 Teilnehmer aus der Verifizierungsphase genutzt. Die ANOVA wurde auf der Anzahl fehlgeschlagener Login-Versuche bzw., in diesem Fall, der Anzahl fehlgeschlagener Verifizierungsversuche.

Das arithmetische Mittel fehlgeschlagener Verifizierungsversuche über alle 69 Teilnehmer betrug für die verschiedenen Passworttypen folgende Werte:

- PIN: $M_{PIN} = .073$, $SD = .356$
- Graphisches Passwort auf Grundlage eines Bildes *ohne* Saliency Mask: $M_{GP} = .3188$, $SD = .757$
- Graphisches Passwort auf Grundlage eines Bildes *mit* Saliency Mask: $M_{GPsm} = .5507$, $SD = 1.007$

Der Levene-Test zeigte, dass keine Gleichheit der Varianzen vorhanden ist $F(2, 66) = 29.132$. Aus diesem Grund wurde zusätzlich der Hames-Howell Post-hoc-Test durchgeführt um festzustellen, ob zwischen den Passworttypen statistisch signifikante Unterschiede in der Erinnerungsfähigkeit an die Passwörter bestehen. Das Ergebnis wies statistisch signifikante Unterschiede zwischen beiden graphischen Passwörtern und der PIN aus ($p < .05$), allerdings keinen statistisch signifikanten Unterschied zwischen den zwei graphischen Passwörtern und der PIN ($p = .281$).

5.2.1. Einfluss durch die Saliency Mask

Für die Analyse des Einflusses durch die Saliency Mask auf die Erinnerungsfähigkeit an graphische Passwörter im Kurzzeitgedächtnis wurde auf eine Analyse der durchschnittlichen euklidischen Distanz zwischen den gesetzten Passwortpunkten aller Teilnehmer zu den jeweils definierten Passwortpunkten zurückgegriffen, siehe Abb. 5.5. Für die PIN kann eine solche Analyse nicht sinnvoll durchgeführt werden – daher wurde die PIN von diesen Analysen ausgeschlossen.

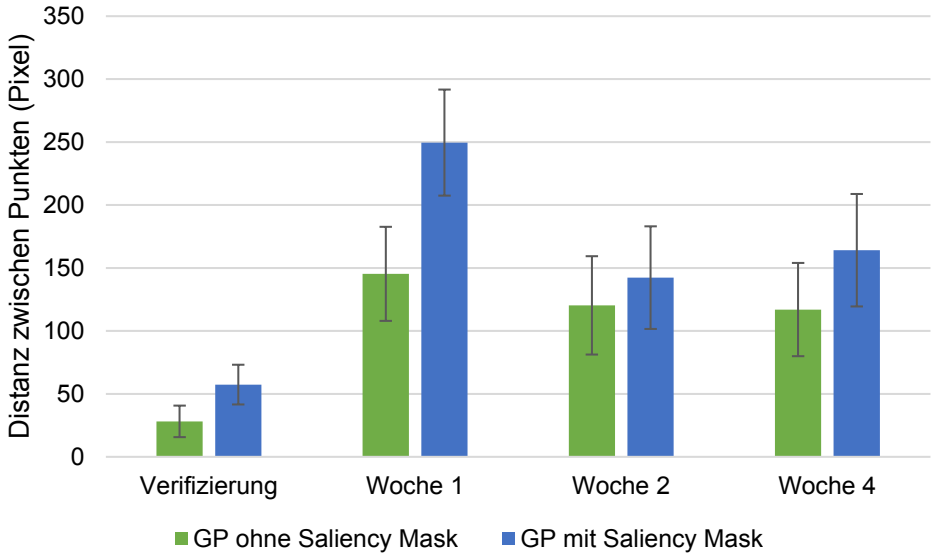


Abbildung 5.5.: Durchschnittliche Distanz zwischen eingegebenen und definierten Passwortpunkten aller 26 Teilnehmer, aufgeteilt nach Bildern mit und ohne Saliency Mask, die für die jeweils als Grundlage für die graphischen Passwörter dienten.

Bereits anhand der Abb. 5.5 lässt sich gut erkennen, dass während der Verifizierungsphase es keine großen Unterschiede zwischen den Passwörtern mit und ohne Saliency Mask gab. Die durchschnittliche Distanz zwischen gesetzten und definierten Passwortpunkten betrug folgende Werte:

- Durchschnittliche Distanz für graphische Passwörter auf Grundlage von Bildern *ohne* Saliency Mask: $57.04px$, $SD = 85.45px$
- Durchschnittliche Distanz für graphische Passwörter auf Grundlage von Bildern *mit* Saliency Mask: $33.16px$, $SD = 55.94px$

Anschließend wurde der zweiseitige Einstichproben-t-Test durchgeführt. Das daraus resultierende Ergebnis zeigte einen statistisch signifikanten Einfluss der Saliency Mask auf die Erinnerungsfähigkeit graphischer Passwörter: $t(68) = -2.160$, $p < .05$. Die Effektgröße war mit $r = .03$ klein. Demnach scheint es schwieriger zu sein, graphische Passwörter, die auf Grundlage von Bildern mit Saliency Mask entstanden sind, im Kurzzeitgedächtnis zu behalten als graphische Passwörter auf Grundlage von Bildern ohne Saliency Mask.

5.2.2. Einfluss durch die Bildkomplexität

Zusätzlich zum möglichen Einfluss durch die Saliency Mask wurde auch der mögliche Einfluss der drei verschiedenen Komplexitätsklassen der Bilder auf die Erinnerungsfähigkeit an graphische Passwörter, die auf Grundlage von Bildern jeweils mit und ohne Saliency Mask

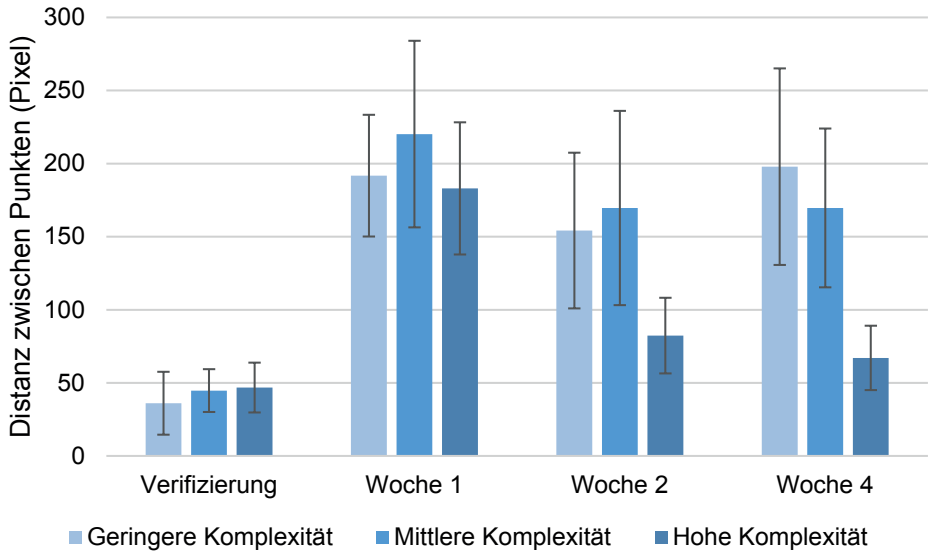


Abbildung 5.6.: Durchschnittliche Distanz zwischen eingegebenen und definierten Passwortpunkten aller 26 Teilnehmer, aufgeteilt nach der Komplexität der Bilder, die für die jeweils als Grundlage für die graphischen Passwörter dienten.

definiert wurden, untersucht. Hierzu wurde ebenfalls einen Vergleich der durchschnittlichen euklidischen Distanz zwischen den von den Teilnehmern eingegebenen Passwortpunkten zu den jeweils definierten Punkten durchgeführt, aufgeteilt in die drei Komplexitätsklassen (gering, mittel und stark), siehe Abb. 5.6. In der Verifizierungsphase ergaben sich, wie bereits die Abbildung erkennen lässt, nur geringfügige Unterschiede:

- Geringe Komplexität: $M_{gering} = 44.74px$, $SE = 11.28px$
- Mittlere Komplexität: $M_{mittel} = 45.24px$, $SE = 9.72px$
- Hohe Komplexität: $M_{hoch} = 45.01px$, $SE = 10.93px$

In diesen Analysen wurde die Bildkomplexität nur mit den zwei graphischen Passworttypen (mit und ohne Saliency Mask) verglichen. Daher wurden zusätzlich mehrere paarweise t-Tests durchgeführt. Hierfür wurde auf die Bonferroni-Methode zur Korrektur der Signifikanz auf $p = (0.05/3 = .016)$ zurückgegriffen.

Daraus entstanden die folgenden Ergebnisse:

- Geringe und mittlere Komplexität: $t(22) = 1.719$, $p = .100$
- Geringe und hohe Komplexität: $t(21) = -1.356$, $p = .189$
- Mittlere und hohe Komplexität: $t(23) = 1.169$, $p = .254$

Es gibt demnach keinen statistisch signifikanten Unterschied in der Erinnerungsfähigkeit des Kurzzeitgedächtnisses an graphischer Passwörter, die auf Grundlage von Bildern beliebiger Komplexitätsklassen entstanden sind.

5.3. Erinnerungsfähigkeit: Langzeitgedächtnis

Wie bei der Analyse des Kurzzeitgedächtnisses auch, wurde bei der Analyse der Erinnerungsfähigkeit des Langzeitgedächtnisses auch auf ANOVA mit wiederholten Messungen zurückgegriffen. Dazu wurde zunächst die Anzahl der fehlgeschlagenen Logins nach der ersten, zweiten und vierten Woche untersucht und unter den drei verschiedenen Passworttypen verglichen, siehe Abb. 5.4. Hierfür wurden die Daten der 26 Teilnehmer betrachtet, die bis zur einschließlich vierten Woche aktiv an der Studie teilgenommen haben. Wie die Abbildungen bereits erahnen lassen, ergab auch die Untersuchung, dass es keine statistisch signifikanten Unterschiede bei der Erinnerungsfähigkeit zwischen den drei Passworttypen gab ($F(2,50) = .123$, $p = .885$). Der Mauchly-Test auf Sphärizität zeigte ebenfalls keine statistisch signifikanten Unterschiede: $X^2(2) = 1.492, p = .474$. Zudem war die Effektgröße mit $\eta^2 = .005$ sehr klein.

Dies lässt darauf schließen, dass die Teilnehmer sich an keines der drei Passworttypen innerhalb der Login-Phasen nach einer, zwei und vier Wochen, signifikant besser erinnern konnten.

5.3.1. Einfluss durch die Saliency Mask

Für die Untersuchung des Einflusses der Saliency Mask auf die Erinnerungsfähigkeit des Langzeitgedächtnisses wurde ebenfalls auf die durchschnittliche euklidische Distanz zwischen gesetzten und definierten Passworttypen zurückgegriffen, siehe Abb. 5.5. Die anschließend auf diesen Daten ausgeführte ANOVA mit wiederholten Messungen zeigte keine statistisch signifikanten Unterschiede zwischen graphischen Passwörtern, die auf Grundlage von Bildern mit und ohne Saliency Mask entstanden sind: $F(1,25) = 1.995$, $p = .170$. Zudem war auch die Effektgröße mit $\eta^2 = .07405$ klein.

5.3.2. Einfluss durch die Bildkomplexität

Ferner wurde auch der Einfluss der drei Komplexitätsklassen (geringe, mittlere und hohe Bildkomplexität) auf die Erinnerungsfähigkeit des Langzeitgedächtnisses an graphischen Passwörter jeweils mit und ohne Saliency Mask untersucht. Hierfür wurde ebenfalls die Maßeinheit der durchschnittlichen euklidischen Distanzen zwischen gesetzten und definierten Passwortpunkten genutzt. Abb. 5.6 zeigt, dass Unterschiede zwischen den drei Komplexitätsklassen innerhalb der Login-Phase (nach ein, zwei und vier Wochen) groß sind.

Während der Registrierung wurden die Bilder und graphischen Passwörter völlig zufällig den Teilnehmern zugeordnet. Daher gab es keine Möglichkeit, darauf einen Einfluss auszuüben. Jedoch kann es insbesondere durch den Wegfall von Teilnehmern im Laufe der Studie zu ungleichen Verteilungen der Bilder bezogen auf die Komplexitätsklassen gekommen sein. Die Kombination zwischen Bildern mit geringer und mittlerer Komplexität war unter den

übrig gebliebenen 26 Teilnehmern nur sechs mal vorhanden, sodass eine statistisch sinnvolle und aussagekräftige Analyse nicht möglich war.

Die ANOVA mit wiederholten Messungen zwischen den anderen beiden Bildpaaren – mittlere und hohe sowie geringe und hohe Komplexität – führte zu keinen statistisch signifikanten Unterschieden:

- Geringe und hohe Komplexität: $F(1,9) = 1.416$, $p = .264$
- Mittlere und hohe Komplexität: $F(1,9) = .738$, $p = .413$

5.4. Auswertung des Fragebogens

An dem im Anschluss an die Login-Phase der vierten Woche durchgeführten Zwischenfragebogen haben von den 26 Teilnehmern, die diese Login-Phase durchlaufen haben, 24 Teilnehmer die Fragen vollständig beantwortet. Davon waren sechs weiblich und 18 männlich. Die Teilnehmer waren zwischen 21 und 48 Jahren Alt ($M = 25.58$, $SD = 6.02$).

5.4.1. Bewertung der Schwierigkeit und Bildkomplexität

Nach der vierten Woche wurden allen Teilnehmern im Rahmen des Fragebogens zunächst jeweils die beiden vorgegebenen graphischen Passwörter sowie die PIN zur Bewertung der Schwierigkeit der Erinnerungsfähigkeit angezeigt, siehe Abb. 5.7. Für die Auswertung dieser Bewertungen wurde der Wilcoxon-Vorzeichen-Rang-Test durchgeführt. Dieser zeigte zwischen den graphischen Passwörtern mit ($Mdn_{GPsm} = 2.5$) und ohne Saliency Mask ($Mdn_{GP} = 3$) keine statistisch signifikanten Unterschiede ($T = 98, p > .05, r = -.005$).

Ferner wurden auch die von den Benutzern abgegebenen Bewertungen der Bildkomplexität der drei im Rahmen der Hauptstudie genutzten Bilder ausgewählt. Hierfür wurde auf den Friedman-Test zur Varianzanalyse zurückgegriffen. Im Kontrast zu den Ergebnissen aus der ersten Vorstudie (siehe Kapitel 3.2.3) ergab die Auswertung des Fragebogens, dass keine statistisch signifikanten Unterschiede in den abgegebenen Bewertungen über die Bildkomplexität zwischen den drei Bildern vorhanden sind ($X^2(2) = .808, p = .668$):

- Bild 1 (hohe Komplexität aus der zweiten Vorstudie): $Mdn = 3$
- Bild 2 (mittlere Komplexität aus der zweiten Vorstudie): $Mdn = 2$
- Bild 3 (geringe Komplexität aus der zweiten Vorstudie): $Mdn = 2$

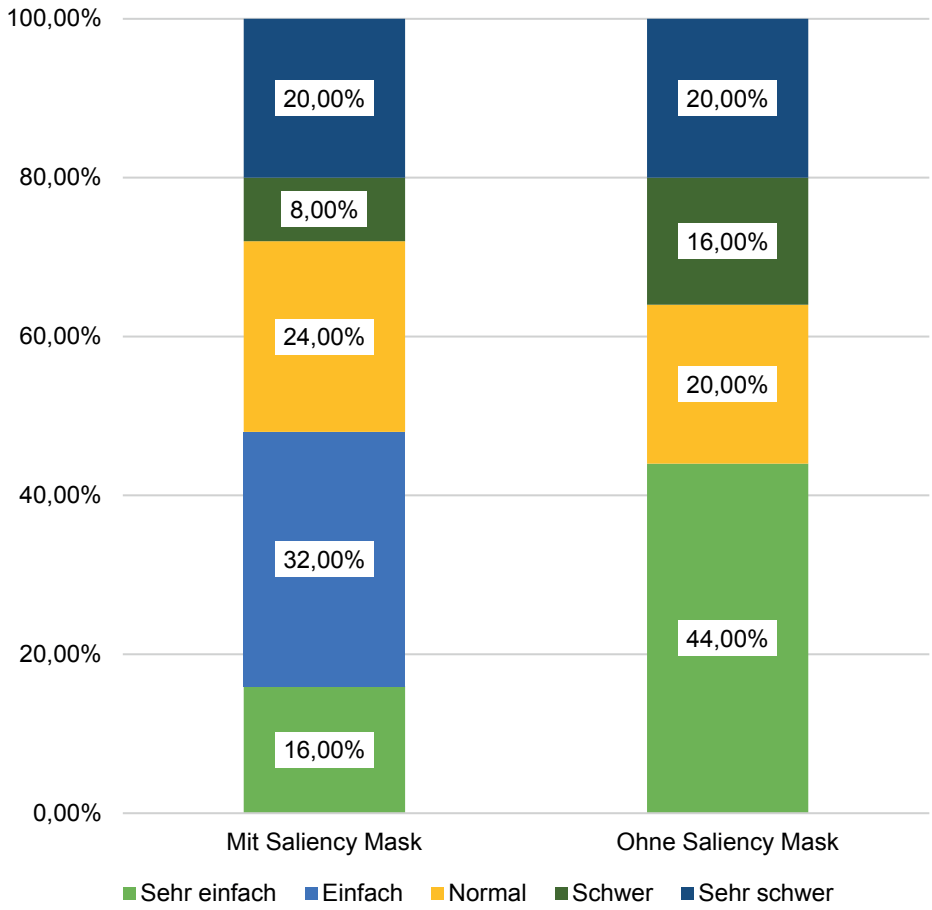
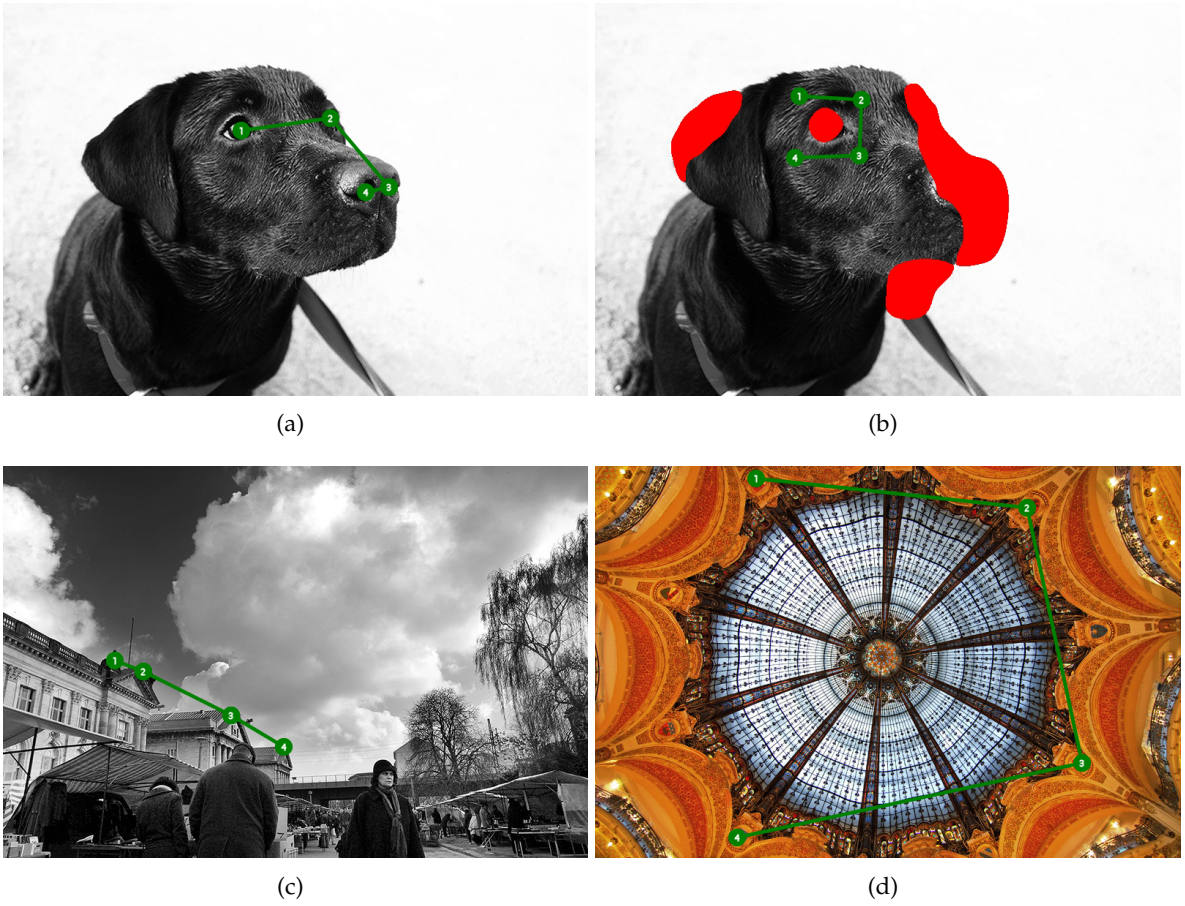


Abbildung 5.7.: Bewertung der Schwierigkeit der graphischen Passwörter, die jeweils auf Grundlage von Bildern mit und ohne Saliency Mask definiert wurden.

5.4.2. Durchführungsorte und Gedächtnishilfen

Im Rahmen des Fragebogens wurde zudem nach dem Ort, an dem die Teilnehmer üblicherweise an der Studie und den Login-Phasen teilgenommen haben, gefragt. Ferner wurde auch nach Gedächtnishilfen, wie beispielsweise Spickzetteln und ähnlichem, gefragt. Dabei wurde explizit darauf hingewiesen, dass die Beantwortung dieser Frage, insbesondere, wenn zugegeben wird, dass Hilfen genutzt wurden, dies keinerlei negative Auswirkungen auf die Gewinnchancen des Gutscheines haben wird. Die Teilnehmer wurden ausdrücklich um ehrliche Antworten gebeten – zudem wurde auf die hohe Relevanz dieser Frage bei der Auswertung dieser Studie aufmerksam gemacht.

Der Großteil der Teilnehmer, 17 der 24, nahm an der Studie überwiegend von zuhause aus teil. Vier Teilnehmer dagegen führten die Logins von der Arbeit aus durch und drei Teilnehmer nahmen von unterschiedlichen Orten aus teil (Zuhause, Arbeit und Uni).



(a) (b)

(c) (d)

Abbildung 5.8.: Verschiedene Strategien, die bei der Definition der graphischen Passwörter genutzt und von den Teilnehmern der Hauptstudie erkannt und übernommen wurden: Nutzung der Augen und Nasenlöcher im Uhrzeigersinn (a); Quadrat um das Auge herum, ebenfalls im Uhrzeigersinn (b); Nutzung der Dachspitzen (c); markante Punkte an den Ecken der Kuppel (d).

15 der Teilnehmer des Fragebogens teilten mit, keinerlei Gedächtnishilfen oder Spickzettel genutzt zu haben. Zwei Teilnehmer gaben zu, das Passwort aufgeschrieben zu haben und sieben Teilnehmer nutzten hauptsächlich Eselsbrücken, die im nachfolgenden Abschnitt ausführlich beschrieben werden.

5.4.3. Strategien und Eselsbrücken

Auf Grund der Tatsache, dass alle in der Studie genutzten graphischen Passwörter von Menschen (während der zweiten Vorstudie) definiert wurden, lagen diese Passwortpunkte erwartungsgemäß in einem sinnvollen Zusammenhang zu dem Bild bzw. auf einfach zu erinnernden Stellen im Bild. Manche Teilnehmer der zweiten Studie definierten durch die

vier Passwortpunkte beispielsweise ein Quadrat um ein Kopf oder Auge herum oder haben ausschließlich die Passwortpunkte auf die Augen und Nasenlöcher gesetzt, siehe Abb. 5.8.

Interessanterweise wurden diese Strategien, die während der Passwortdefinition genutzt und ausgedacht wurden, von Teilnehmern der Hauptstudie korrekt erkannt und auch als Gedächtnisstütze oder Eselsbrücke genutzt. Unter anderem war die Symmetrie des graphischen Passworts bzw. des daraus entstandenen geometrischen Gebildes eine Hilfe (Antwort von zwei Teilnehmern: *"Bei dem Hund war ich mir nicht immer sicher, konnte mich aber an das visuelle Muster unabhängig von den Dingen auf dem Bild erinnern und dann rekonstruieren."* und *„Die Perspektive. Es muss ein Viereck ergeben, wobei die Kanten mehr oder weniger parallel zu den Bildkanten sind."*). Bei einem Teilnehmer spielte auch die Symmetrie eine Rolle (*„Die Symmetrie – einmal rund im Kreis, ein mal auf einer Linie"*). Grundsätzlich scheint wohl die Assoziation des graphischen Passwortes mit einem durch die Passwortpunkte gebildeten geometrischen Objekt ein brauchbares Hilfsmittel zu sein. Auch persönliche Elemente bzw. ein persönlicher Bezug zum Bild scheinen eine große Gedächtnishilfe gewesen zu sein (*„Das Bild des Hundes hat zu mir direkten Bezug. Hatte selbst mal einen. Das war sofort gespeichert."*).

Für die PIN wurde ebenfalls die Frage nach möglichen Gedächtnishilfen und Strategien zur besseren Erinnerungsfähigkeit an die vierstellige Zahlenfolge gestellt. Manche Teilnehmer konnten zu den Ziffernfolgen einen persönlichen Bezug herstellen, in einem Fall entsprachen die Ziffern beispielsweise einem Geburtsdatum (*„Hintere beiden Ziffern sind mein Geburtstags falsch herum und die ersten beiden sind fortlaufend, beginnend mit dem Nachfolger der 4. Ziffer."*). Ein weiterer Teilnehmer griff auf eine mathematische Eselsbrücke zurück und merkte sich nur die Summe der letzten beiden Ziffern (*„3 und 7 gemerkt und der Rest ergab in der Addition 3 (2 und 1)"*). Ähnlich wie bei den graphischen Passwörtern, konnten auch bei der vierstelligen PIN geometrische Objekte, die sich durch die Eingabereihenfolge auf einer numerischen Tastatur ergeben, als Gedächtnishilfe genutzt werden (*„Für die Zahlenkombination habe ich mir die Abfolge visuell auf dem Numpad gemerkt."*).

6. Zusammenfassung und Ausblick

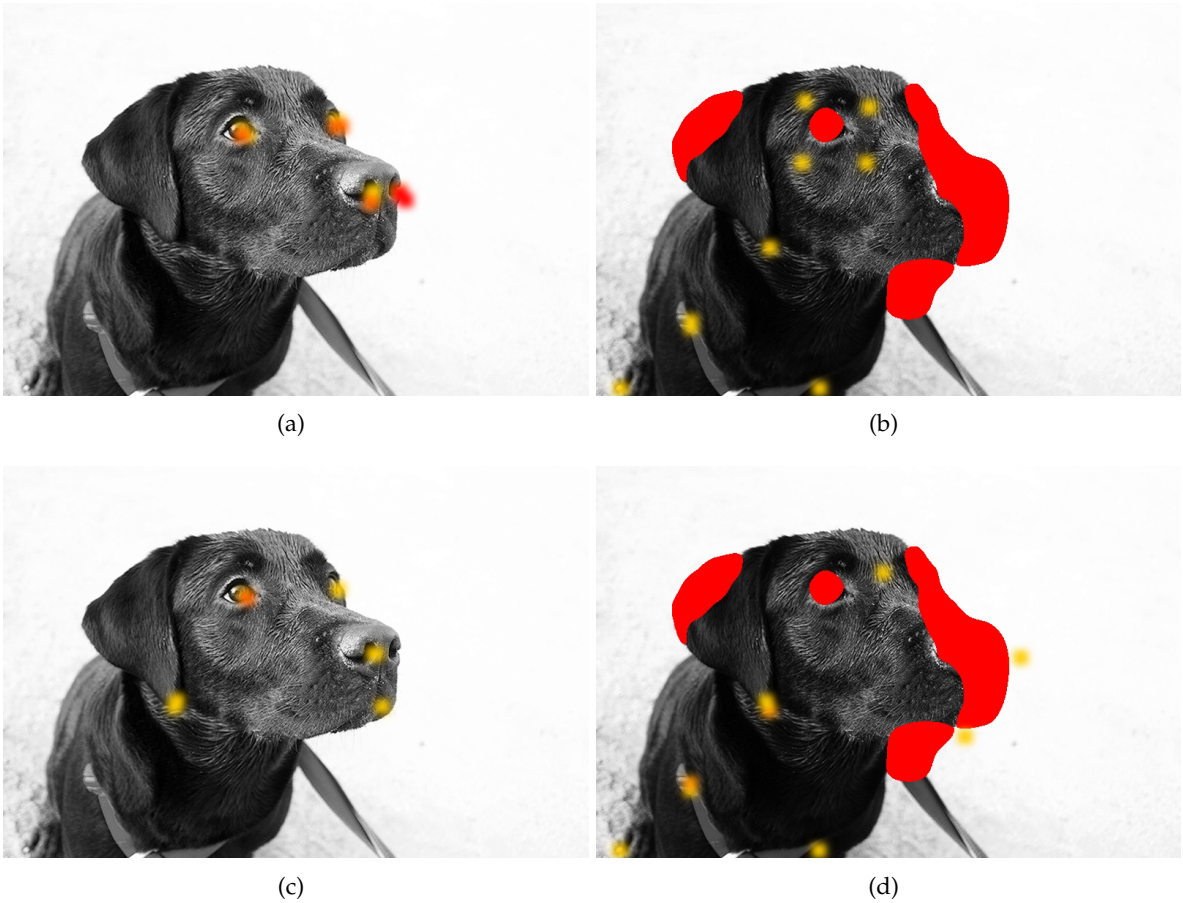
6.1. Zusammenfassung der Ergebnisse

In Bezug auf Hypothese 1 (siehe Kapitel 1.2) ergaben aus der Studie erlangten Ergebnisse sowie die darauf folgende Analyse, dass die Saliency Mask keinen statistisch signifikanten Einfluss auf die Erinnerungsfähigkeit an vorgegebene graphische Passwörter über einen längeren Zeitraum hat. Diese Erkenntnis konnten durch die Untersuchung der Anzahl fehlgeschlagener Login-Versuche insgesamt als auch bei der detaillierten Analyse des Langzeitgedächtnisses erlangt werden, siehe Abb. 5.4 sowie Kapitel 5.3.

Zudem haben die Analysen bestätigt, dass auch die Bildkomplexität keinen Einfluss auf die Erinnerungsfähigkeit an graphische Passwörter, jeweils mit und ohne Saliency Mask, zu haben scheint, siehe Abb. 5.6. Damit konnte Hypothese 2 ebenfalls bestätigt werden.

Im Rahmen der Analyse wurden in dieser Studie zwei verschiedene Messverfahren genutzt: Die Anzahl fehlgeschlagener Login-Versuche sowie die Distanz zwischen eingegebenen und jeweils definierten Passwortpunkten. Interessanterweise ergaben beide Messverfahren ein übereinstimmendes Ergebnis bezüglich der Erinnerungsfähigkeit des Langzeitgedächtnisses in der ersten, zweiten und vierten Woche. Dagegen gab es bei der Analyse des Kurzzeitgedächtnisses, für das die Daten der Verifizierung aller 69 registrierten Teilnehmern die Grundlage bildeten, unterschiedliche Ergebnisse. Die Analyse der Anzahl fehlgeschlagener Login-Versuche ergab in Hinblick auf die Erinnerungsfähigkeit keine statistisch signifikanten Unterschiede zwischen den zwei graphischen Passwörtern (jeweils mit und ohne Saliency Mask), während die Distanzanalyse ergab, dass die Erinnerungsfähigkeit über einen kurzen Zeitraum an Passwörter basierend auf einem Bild mit Saliency Mask besser ist, als ohne. In wie weit die verschiedenen Ergebnisse aus beiden Messverfahren zu interpretieren sind und welcher Zusammenhang hierbei zwischen den beiden Messverfahren besteht, muss durch eine separate Studie und eine detaillierte Untersuchung beider Messverfahren beantwortet werden.

Es wurde erfolgreich von den Möglichkeiten Gebrauch gemacht, durch verschiedene Strategien die Erinnerungsfähigkeit an graphische Passwörter sowohl auf Grundlage von Bildern mit als auch ohne Saliency Mask zu verbessern. Dies wurde von den Teilnehmern der zweiten Vorstudie zur Definition der graphischen Passwörter genutzt und von den Teilnehmern der Hauptstudie wiederverwendet. Die gestellte Frage nach der Schwierigkeit der Passwörter im Fragebogen ermöglichte die Einordnung in einfach und schwierig zu erinnernde graphische Passwörter. Aus diesen Passwörtern wurde, am Beispiel des am wenigsten komplexen Bildes, eine Heatmap nach dem gleichen Prinzip wie bereits in Kapitel 3.3.3 erstellt. Je mehr Passwortpunkte sich innerhalb eines Quadrats mit einer Kantenlänge von 50 Pixeln befinden,



(a) (b)

(c) (d)

Abbildung 6.1.: In dieser Abbildung werden die Heatmaps der als einfach (oben) und schwierig (unten) bewerteten Passwörter jeweils ohne (links) und mit (rechts) Saliency Mask.

desto dunkler die Farbe. Die daraus resultierende Heatmap (siehe Abb. 6.1) bestätigt die bereits in der Vorstudie erlangen Erkenntnisse: Obwohl die Definition von Passwörtern erschwert war und das Setzen der Passwortpunkte auf Augen und Nasenlöcher nicht mehr möglich war, konnten die Teilnehmer Strategien entwickeln, die dazu führten, dass die Erinnerungsfähigkeit an Passwörter mit Saleincy Mask nicht schlechter wurde, siehe in Abb. 6.1 (a) und (b). Die beiden Bilder stellen alle als einfach bewerteten graphischen Passwörter, jeweils mit (a) und ohne (b) Saliency Mask, dar.

Im Kontrast hierzu gelang es scheinbar nicht allen Nutzern, solche Strategien zu finden. Der Vergleich zwischen Abb. 6.1 (b) und (d) offenbart, dass scheinbar das Setzen von einzelnen Passwortpunkten in einen weniger markanten, beispielsweise in den komplett weißen Bereich, die Schwierigkeit deutlich erhöht hat. Ähnliches lässt sich auch bei den graphischen Passwörtern auf Grundlage es Bildes ohne Saliency Mask beobachten. Die Passwörter aus Bild (a) und (c) unterscheiden sich lediglich an einer Stelle, die offensichtlich dazu führt, dass

die Erinnerungsfähigkeit an das Passwort deutlich schwerer wird. Demnach scheinen bereits geringe Unterschiede zwischen verschiedenen Passwortpunkten die Erinnerungsfähigkeit an ein solches Passwörter stark zu beeinflussen.

6.2. Einschränkungen

Die durchgeführte Studie beinhaltete mehrere Einschränkungen. Zunächst wurde nur eine Begrenzte Anzahl an Bildern genutzt. Zwar ergab die Untersuchung, dass die Bildkomplexität keinen Einfluss auf die Erinnerungsfähigkeit der darauf definierten graphischen Passwörter hat, allerdings besteht die Möglichkeit, dass es durchaus bestimmte Elemente in einem Bild gibt, die einen Einfluss auf den Nutzer haben können. Dies könnte beispielsweise der Fall sein, wenn ein Benutzer sich das Bild selber aussuchen kann und es nicht, wie in dieser Studie, durch einen Zufallsgenerator vorgegeben bekommt.

Eine weitere Einschränkung bestand in der Anzahl der aktiv an der Studie teilgenommenen Personen. Bereits die Zahl der 69 vollständig registrierten Teilnehmern war gering – die Zahl der aktiv bis zum Ende der Studie teilgenommenen Personen sank noch deutlich. Dies führt zu der Frage, ob die erlangen Ergebnisse allgemein gültig sind und sich auch auf andere, eventuell weniger Computer-affine Benutzer, übertragen lassen. Insbesondere die stark sinkende Anzahl der Teilnehmer wirft die Frage auf, in wie weit die Teilnehmer in Zukunft besser an eine Studie gebunden und für eine aktive Teilnahme motiviert werden können, um solche Probleme zu vermeiden.

Die dritte Einschränkung bestand in der begrenzten Dauer der Studie. Zwar war die Gesamtdauer auf acht Wochen veranschlagt, hiervon waren allerdings nur vier Wochen statistisch auswertbar. Interessant wäre die Frage nach einer deutlich längeren Studie, mit einer Dauer von mehreren Monaten. Beispielsweise werden PINs von Bankkarten üblicherweise über mehrere Jahre nicht verändert und konstant genutzt. Ein vergleichbares Ergebnis, zumindest über viele Monate, wäre daher sicherlich interessant.

In dieser Studie wurde die Eingabe mit der Computermaus durch Klicken auf das Bild genutzt. Es kann grundsätzlich angenommen werden, dass die Eingabemethode keinen großen Einfluss auf die Erinnerungsfähigkeit hat. Allerdings wäre es in Hinblick auf die Benutzbarkeit und die damit verbundene Frage, in wie weit Teilnehmer mit einer alternativen Eingabemethode zurecht kommen, eine weitere Studie wert. Die Frage, ob die Eingabe durch Augengestik statt mit der Computermaus einfacher oder schwieriger bzw. komfortabler oder anstrengender ist, konnte demnach in dieser Studie nicht beantwortet werden.

6.3. Ausblick

Das im Rahmen dieser Studienarbeit genutzte Authentifizierungssystem ist nicht auf bestimmte Anwendungszwecke sowie Eingabemethoden beschränkt. Dies ermöglicht den Einsatz dieses Systems vielen verschiedenen Bereichen, wie beispielsweise im Web als Online-Login, an Bankautomaten, am Smartphone oder Tablet und auch auf Notebooks. Offen ist hierbei allerdings die Frage, wie dieses System implementiert werden muss, um die nötigen Sicherheitsanforderungen, insbesondere bei Bankautomaten, ausreichend zu erfüllen. Hierbei handelt es sich vor allem um die Fragen nach der Bildgröße, um genug Möglichkeiten für das Setzen sinnvoller Passwortpunkte zu sehen, die richtige bzw. sicherste Konfiguration des Saliency-Mask-Algorithmus sowie auch um die Eingabemethode. An Bankautomaten könnte der Login durch Augengestik erfolgen, was mehr Sicherheit gegen die Gefahren des „über die Schulter schauen“ oder Abfilmen der Passworteingabe bietet. Ferner stellt sich die Frage, ob die Bild- und Passwortauswahl durch den Benutzer vorgenommen werden darf, oder es sich ausschließlich um vorgegebene Bild-Passwort-Kombinationen handeln sollte. Bei vorgegebenen Passwörtern muss allerdings untersucht werden, ob nicht ein Sicherheitsrisiko dadurch entsteht, dass die Passwörter ursprünglich durch Menschen definiert wurden und es sich nicht um zufällig generierte Passwörter handelt.

Aus diesem Grund gibt es noch einen weiteren, bisher nicht erforschten Bereich: Die automatische und vom Zufall abhängige Generierung graphischer Passwörter. Für PINs und konventionelle Passwörter gibt es bereits Passwortgeneratoren, die teilweise auch einfacher zu merkende Passwörter generieren, beispielsweise die jeweils ersten Buchstaben eines Satzes. Für graphische Passwörter ist bisher unbekannt, nach welchem Muster ein solcher Generator arbeiten muss, um sinnvolle graphische Passwörter, die einen Bezug zum Bild haben und damit auch einfacher zu erinnern sind, zu generieren. Vor allem sollte ein solcher Generator auch gewisse Gedächtnishilfen generieren können, wie beispielsweise das Setzen der Passwortpunkte auf markante Bereiche im Uhrzeigersinn.

Ferner gibt es auch im Online-Bereich interessante Einsatzmöglichkeiten graphischer Passwörter. Möglich wäre, Login-Seiten, welche die Eingabe normaler Passwörter oder PINs erforderlich machen, komplett durch die Eingabe graphischer Passwörter zu ersetzen. Als Eingabeinterface kann größtenteils das im Rahmen dieser Studienarbeit entwickelte Webinterface genutzt werden. Die Nutzung graphischer Passwörter auf bekannten und oft besuchten Internetplattformen könnte zudem dazu führen, dass eine großflächige Benutzerstudie mit deutlich mehr potenziellen Nutzern durchgeführt werden könnte. Eine weitere Möglichkeit bietet sich durch „Text 2.0“[1]. Dieses System ermöglicht die Verbindung einer Blickerfassungshardware über ein entsprechendes Webkit-Plugin mit einem kompatiblem Webbrowser. Dies kann für die Eingabe graphischer Passwörter durch Augengestik für den Login über den Webbrowser genutzt werden. Im Gegensatz zur Eingabe mit der Computermaus eignet sich diese Methode nicht für eine großflächige Studie. Neben der Voraussetzung, dass entsprechende Hardware vorhanden sein muss, besteht zudem die Notwendigkeit, dass die Hardware korrekt kalibriert und an das jeweilige Webinterface durch entsprechende

[1] http://text2o.net/

Schaffung von Schnittstellen angepasst ist. Daher eignet sich diese Eingabemethode derzeit nur für stationäre Studien.

Die interne Repräsentation von Passwortpunkten ist ebenfalls ein noch offener Bereich. Im Gegensatz zu PINs oder Passwörtern, die vom Teilnehmer exakt wiedergegeben werden müssen und es daher ausreicht, die Eingabe mit einem intern gespeicherten Hash abzugleichen, müssen bei graphischen Passwörtern die definierten Passwortpunkte wegen des Toleranzbereichs bei Abgleich mit der Eingabe bekannt sein. Dies könnte ein eventuelles Sicherheitsrisiko darstellen: Ein Angreifer, der in den Besitz der Passwortdatenbank gelangt, würde auf diese Weise in den Besitz aller Passwörter gelangen. Daher sollten zumindest die Zuordnungen von Passwörtern zu Bildern separat und sicher gespeichert werden. Ferner kann dieses Risiko dadurch minimiert werden, dass der die Passwortdatenbank bzw. der für die Speicherung genutzte Server sicher und aufwendiger gegen Angriffe geschützt wird.

Zudem wurde bereits in den Analysen darauf hingewiesen, dass es für graphische Passwörter zwei verschiedene Messverfahren gibt: Zum einen die Distanzanalyse zwischen eingegebenen und jeweils definierten Passwortpunkten. Zum anderen ist auch das Messverfahren nach der Anzahl fehlgeschlagener Login-Versuche denkbar. Die Analysen des Langzeitgedächtnisses in dieser Studie ergaben eine Übereinstimmung, während die Analysen des Kurzzeitgedächtnisses unterschiedliche Ergebnisse zwischen den beiden Messverfahren offenbarten. Für eine mögliche zukünftige Studie wäre daher die Frage nach dem Zusammenhang dieser beiden Messverfahren interessant. Eine detaillierte Untersuchung würde unter anderem auch Aufschluss darüber geben, wie unterschiedliche Ergebnisse aus beiden Verfahren interpretiert werden können.

6.4. Fazit

Zusammengefasst bestätigen die Ergebnisse das Potenzial vorgegebener graphischer Passwörter, die auf Grundlage von Bildern mit Saliency Mask definiert wurden. Diese zeichnen sich durch die Kombination aus höherer Sicherheit und gleich bleibender Erinnerungsfähigkeit aus. Es kann somit die Aussage getroffen werden, dass eine Saliency Mask keinen statistisch signifikanten Einfluss auf die Erinnerungsfähigkeit hat, das darauf generierte graphische Passwort jedoch sicherer ist. Ferner ist die Erinnerungsfähigkeit an graphische Passwörter nicht schlechter, als an die als Messbasis dienenden vierstelligen PINs. Demnach ist die Entwicklung eines benutzbaren Authentifizierungssystems gelungen, dass die Vorteile der besseren menschlichen Erinnerungsfähigkeit an Bilder und geometrische Objekte ausnutzt und mit einer erhöhten Sicherheit kombiniert.

A. Anhang

A.1. Die beliebtesten Schlagwörter von Flickr

2005, 2006, 2007, 2008, 2009, architecture, art, australia, baby, barcelona, beach, berlin, birthday, blackandwhite, blue, bw, california, cameraphone, canada, canon, car, cat, chicago, china, christmas, church, city, clouds, concert, dog, england, europe, family, festival, film, florida, flower, flowers, food, france, friends, fun, garden, geotagged, germany, girl, green, holiday, italy, japan, landscape, live, london, macro, mexico, museum, music, nature, new, newyork, night, nikon, nyc, paris, park, party, people, photo, photography, portrait, red, rock, sanfrancisco, sea, seattle, show, sky, snow, spain, spring, street, summer, sunset, taiwan, texas, tokyo, travel, trees, trip, uk, urban, usa, vacation, washington, water, wedding, white, winter, zoo

Stand: April 2012

A.2. Erklärungstext der Hauptstudie

Die Hauptstudie wurde allen Teilnehmern vor der Registrierung mit diesem Begrüßungs- und Hinweistext (in deutscher und englischer Sprache) erklärt:

> Vielen Dank für Dein Interesse an unserer Studie!
>
> In dieser Studie geht es darum, verschiedene Möglichkeiten der Passworteingabe über einen längeren Zeitraum zu testen. Dazu wirst du im Folgenden aufgefordert, drei vorgegebene Passwörter einzugeben und zwar:
>
> 1) eine vierstellige PIN, 2) ein Passwort, bestehend aus vier Passwortpunkten, welches durch Klicken mit der Maus auf ein Bild eingegeben wird, 3) ein zweites Passwort, bestehend aus vier Passwortpunkten, welches durch Klicken mit der Maus auf ein anderes Bild eingegeben wird.
>
> Nachdem ihr euch einmal erfolgreich eingeloggt habt, werdet ihr in bestimmten Zeitabständen per E-Mail benachrichtigt und gebeten, euch erneut mit dem vorgegebenen Passwort einzuloggen. Insgesamt werdet ihr euch fünf Mal über einen Zeitraum von 8 Wochen einloggen. Nach Ablauf der 8 Wochen verlosen wir unter allen Teilnehmern, welche die komplette Studie durchgeführt haben, drei Amazon Gutscheine im Wert von jeweils 30 Euro. Falls Ihr euch an ein Passwort

einmal nicht erinnern könnt, wird euch dieses angezeigt und ihr könnt weiterhin an der Studie teilnehmen.

Die Eingabe der drei Passwörter wird jedesmal maximal 5 Minuten dauern.

Eure eingegebenen Daten werden vertraulich behandelt und nicht an Dritte weitergegeben. Außerdem werden alle nicht studienbezogenen Daten (z.B. eure E-Mail Adresse) nach Ablauf der Studie gelöscht.

Bitte klicke hier, um an der Studie teilzunehmen

A.3. Alle definierten graphischen Passwörter

Alle im Rahmen der zweiten Vorstudie (siehe 3.3) durch Benutzer definierten graphischen Passwörter jeweils für das komplexeste (Abb. A.1), mittel (Abb. A.2) und am wenigsten komplexe (Abb. A.3) Bild. Mehrfach vorhandene gleiche oder ähnliche Passwörter sind darauf zurückzuführen, dass verschiedene Teilnehmer zufällig ein nahezu gleiches Passwort definiert haben.

A.4. Zwischenfragebogen

In Abb. A.4 wird der an alle Nutzer versandte Zwischenfragebogen dargestellt. Die Inhalte des Zwischenfragebogens waren für jeden Teilnehmer unterschiedlich und passten sich den jeweils genutzten Bildern und Bildpasswortkombinationen an. Zur Teilnahme war ein eindeutiges Token nötig, das zur Identifikation der Nutzer diente.

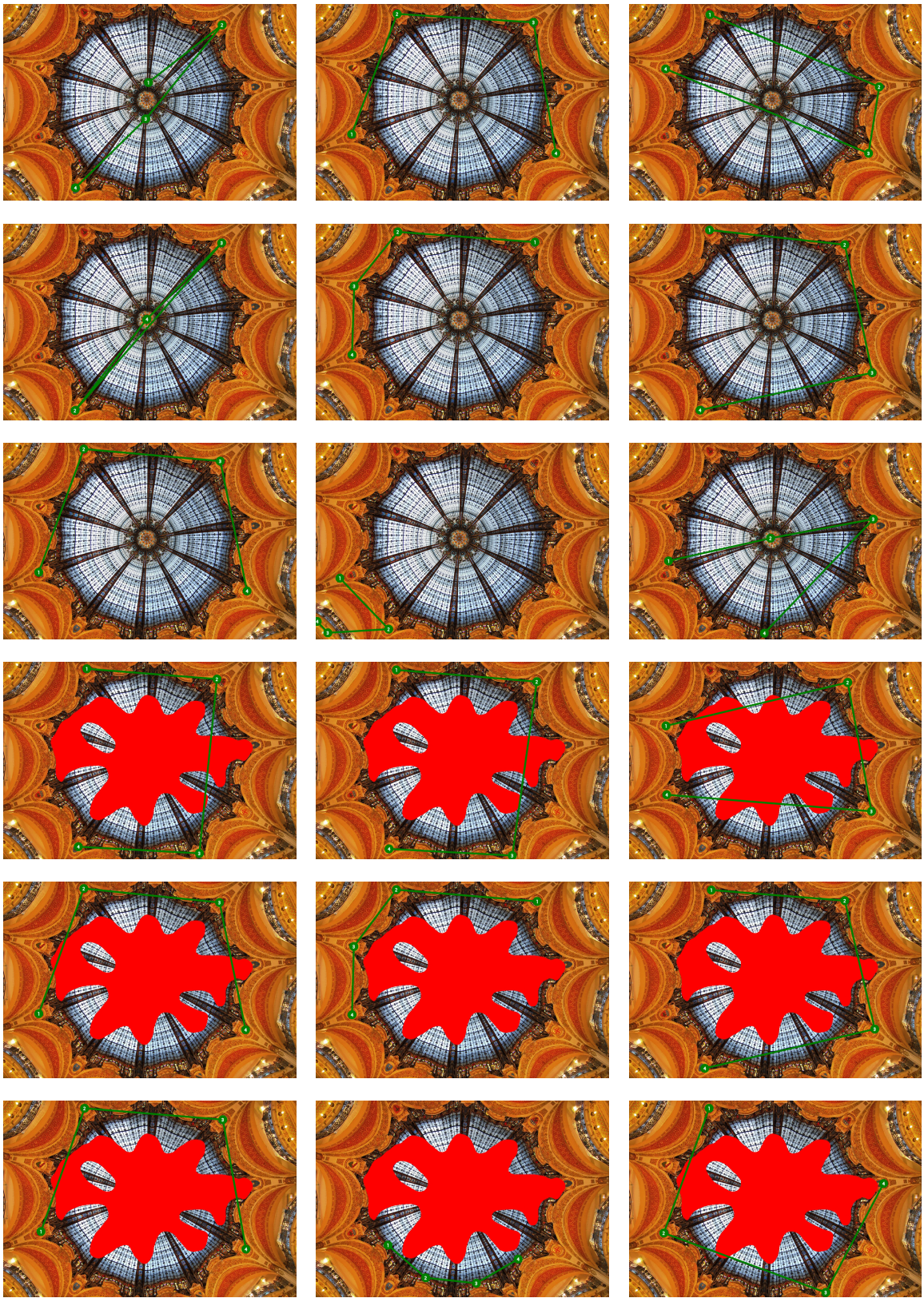


Abbildung A.1.: Alle Bildpasswörter des komplexesten Bildes.

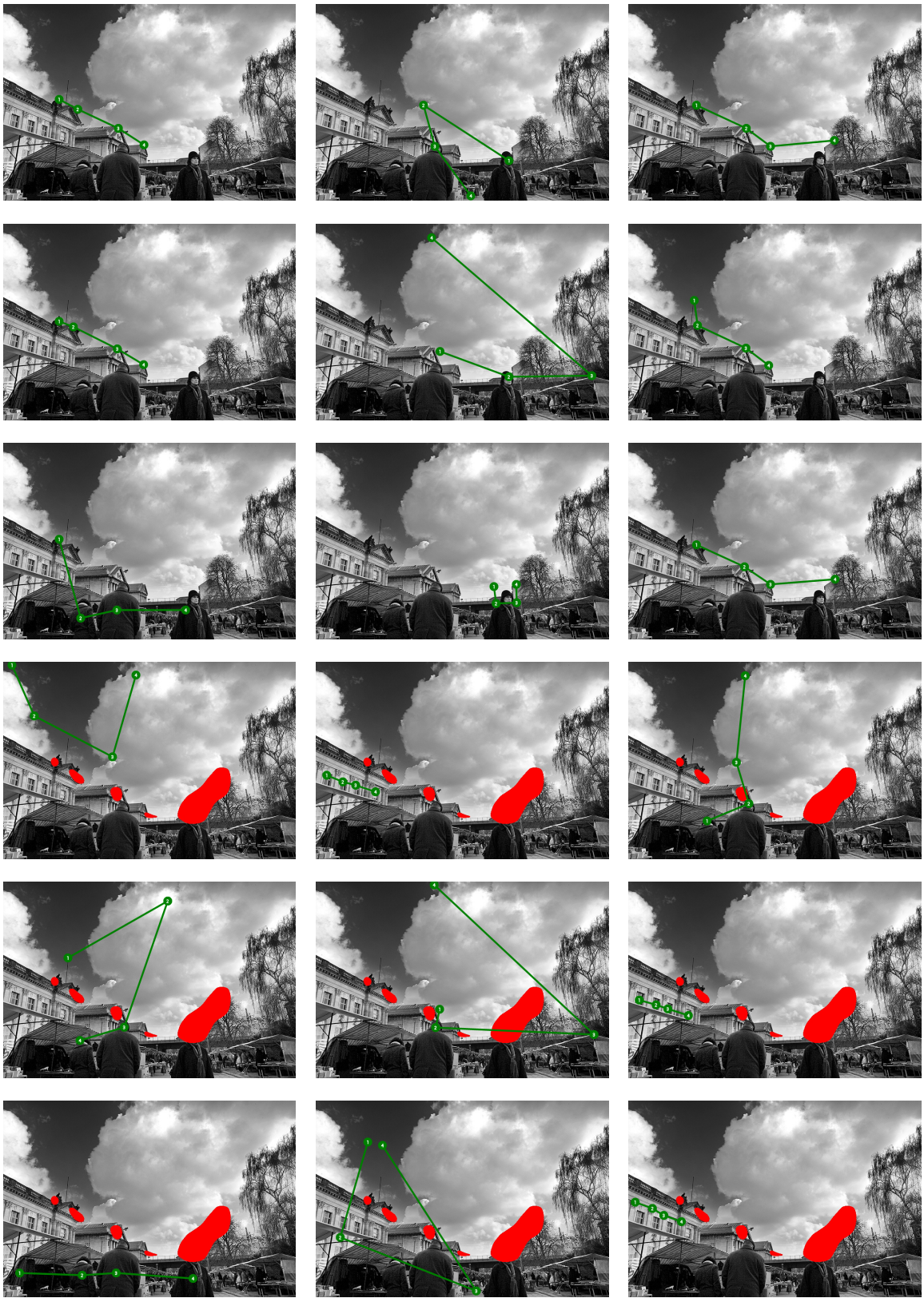


Abbildung A.2.: Alle Bildpasswörter des mittel komplexen Bildes.

Abbildung A.3.: Alle Bildpasswörter des am wenigsten komplexen Bildes.

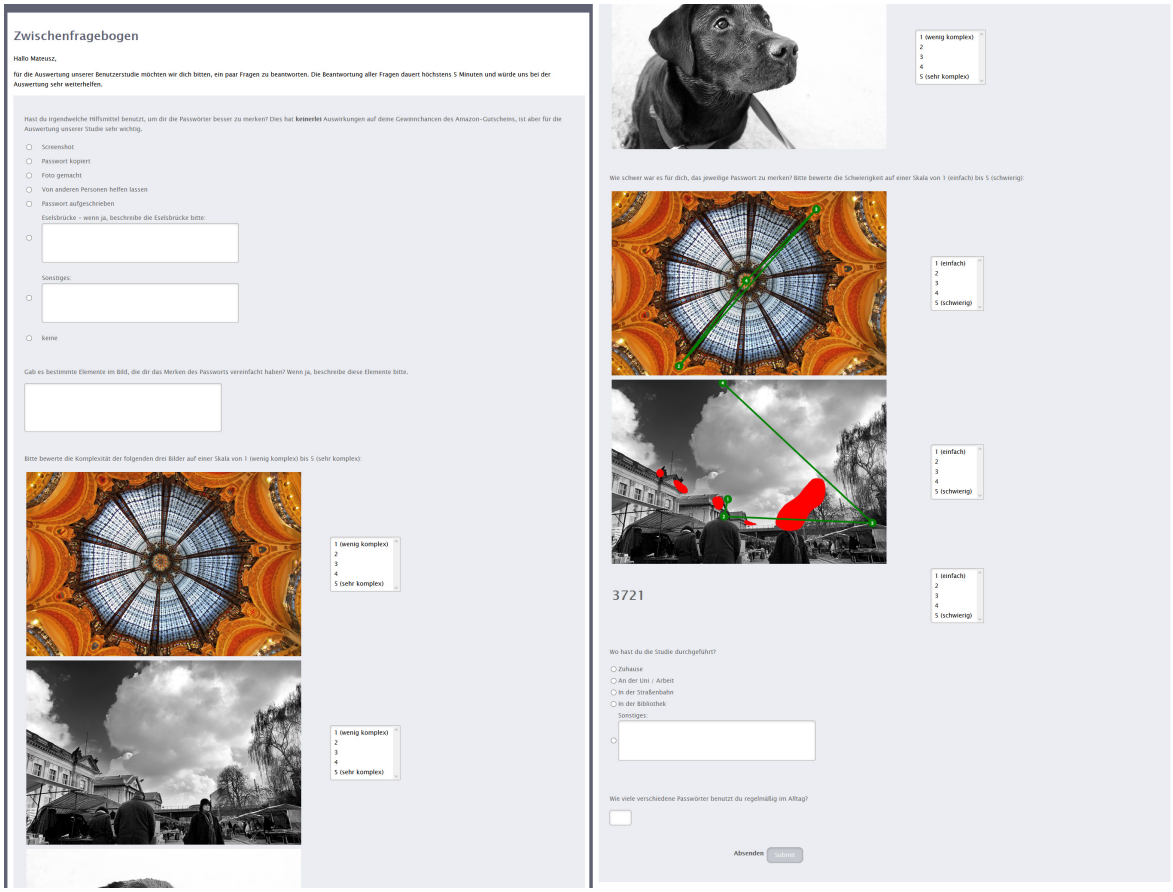


Abbildung A.4.: Screenshot des Zwischenfragebogens

Literaturverzeichnis

[AS68] R. Atkinson, R. Shiffrin. Human memory: A proposed system and its control processes. *The psychology of learning and motivation: Advances in research and theory*, 2:89–195, 1968.

[AS99] A. Adams, M. A. Sasse. Users are not the enemy. *Communications of the ACM*, 42(12):40–46, 1999. doi:10.1145/322796.322806. URL http://doi.acm.org/10.1145/322796.322806.

[BAS12] A. Bulling, F. Alt, A. Schmidt. Increasing the security of gaze-based cued-recall graphical passwords using saliency masks. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems*, CHI '12, S. 3011–3020. ACM, New York, NY, USA, 2012. doi:10.1145/2208636.2208712. URL http://doi.acm.org/10.1145/2208636.2208712.

[BBZD04] A. S. Brown, E. Bracken, S. Zoccoli, K. Douglas. Generating and remembering passwords. *Applied Cognitive Psychology*, 18(6):641–651, 2004. URL http://dx.doi.org/10.1002/acp.1014.

[BCV85] J. Beard, L. Clark, V. Velten. Characterization of ATR Performance in relation to image measurements. *ATRWG Report, AFWAL/AARF, Wright Patterson AFB, OG*, 45433, 1985.

[BCVO12] R. Biddle, S. Chiasson, P. Van Oorschot. Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys*, 44(4):19:1–19:41, 2012. doi:10.1145/2333112.2333114. URL http://doi.acm.org/10.1145/2333112.2333114.

[BS00] S. Brostoff, M. A. Sasse. Are Passfaces More Usable Than Passwords? A Field Trial Investigation. In *Proc. of HCI 2000*, S. 405–424. 2000.

[CBO07] S. Chiasson, R. Biddle, P. C. van Oorschot. A second look at the usability of click-based graphical passwords. In *Proc. of the 3rd Symposium on Usable Privacy and Security*, S. 1–12. 2007. doi:10.1145/1280680.1280682.

[CDGPT09] M. Cardaci, V. Di Gesù, M. Petrou, M. E. Tabacchi. A fuzzy approach to the evaluation of image complexity. *Fuzzy Sets Syst.*, 160(10):1474–1484, 2009. doi:10.1016/j.fss.2008.11.017. URL http://dx.doi.org/10.1016/j.fss.2008.11.017.

[COB07] S. Chiasson, P. C. van Oorschot, R. Biddle. Graphical Password Authentication Using Cued Click Points. In *Proc. of the 12th European Symposium On Research In Computer Security*, S. 359–374. 2007.

[DACJR05] A. De Angeli, L. Coventry, G. Johnson, K. Renaud. Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*, 63(1-2):128–152, 2005. doi:10.1016/j.ijhcs.2005.04.020. URL http://dx.doi.org/10.1016/j.ijhcs.2005.04.020.

[DLDH09] A. De Luca, M. Denzel, H. Hussmann. Look into my eyes!: can you guess my password? In *Proceedings of the 5th Symposium on Usable Privacy and Security*, SOUPS '09, S. 7:1–7:12. ACM, New York, NY, USA, 2009. doi:10.1145/1572532.1572542. URL http://doi.acm.org/10.1145/1572532.1572542.

[DMR04] D. Davis, F. Monrose, M. K. Reiter. On user choice in graphical password schemes. In *Proc. of the 13th USENIX Security Symposium*, S. 11–11. 2004. URL http://dl.acm.org/citation.cfm?id=1251375.1251386.

[DP00] R. Dhamija, A. Perrig. Déjà Vu: a user study using images for authentication. In *Proceedings of the 9th conference on USENIX Security Symposium - Volume 9*, SSYM'00, S. 4–4. USENIX Association, Berkeley, CA, USA, 2000. URL http://dl.acm.org/citation.cfm?id=1251306.1251310.

[EBFK09] K. M. Everitt, T. Bragin, J. Fogarty, T. Kohno. A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09, S. 889–898. ACM, New York, NY, USA, 2009. doi:10.1145/1518701.1518837. URL http://doi.acm.org/10.1145/1518701.1518837.

[Har06] J. Harel. Graph-Based Visual Saliency Toolbox for MATLAB, http://www.klab.caltech.edu/ harel/share/ gbvs.php, 2006. URL http://www.klab.caltech.edu/~harel/share/gbvs.php.

[HKP06] J. Harel, C. Koch, P. Perona. Graph-Based Visual Saliency. In *Proceedings of the 20th International Conference on Neural Information Processing Systems*, S. 545–552. 2006.

[IKN98] L. Itti, C. Koch, E. Niebur. A Model of Saliency-Based Visual Attention for Rapid Scene Analysis. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(11):1254–1259, 1998.

[JMM+99] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin. The design and analysis of graphical passwords. In *Proc. of the 8th USENIX Security Symposium*. 1999.

[LDOY07] D. Lin, P. Dunphy, P. Olivier, J. Yan. Graphical passwords & qualitative spatial relations. In *Proc. of the 3rd Symposium on Usable Privacy and Security*, S. 161–162. 2007. doi:10.1145/1280680.1280708.

[ML07] W. Moncur, G. Leplâtre. Pictures at the ATM: exploring the usability of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '07, S. 887–894. ACM, New York, NY, USA, 2007. doi:10.1145/1240624.1240758. URL http://doi.acm.org/10.1145/1240624.1240758.

[PIA+90] R. A. Peters, II, R. Alan, P. Ii, R. N. Strickland. Image Complexity Metrics for Automatic Target Recognizers, 1990.

[SG78] N. J. Slamecka, P. Graf. The generation effect: Delineation of a phenomenon. *Journal of Experimental Psychology: Human Learning and Memory*, 4(6):592–604, 1978. doi:10.1037/0278-7393.4.6.592.

[SZO05] X. Suo, Y. Zhu, G. S. Owen. Graphical Passwords: A Survey. In *Proceedings of the 21st Annual Computer Security Applications Conference*, ACSAC '05, S. 463–472. IEEE Computer Society, Washington, DC, USA, 2005. doi:10.1109/CSAC.2005.27. URL http://dx.doi.org/10.1109/CSAC.2005.27.

[WDL08] R. Weiss, A. De Luca. PassShapes: utilizing stroke based authentication to increase password memorability. In *Proceedings of the 5th Nordic conference on Human-computer interaction: building bridges*, NordiCHI '08, S. 383–392. ACM, New York, NY, USA, 2008. doi:10.1145/1463160.1463202. URL http://doi.acm.org/10.1145/1463160.1463202.

[WWB+05a] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, N. Memon. Authentication using graphical passwords: effects of tolerance and image choice. In *Proc. of the 1st Symposium on Usable Privacy and Security*, S. 1–12. 2005. doi:10.1145/1073001.1073002. URL http://doi.acm.org/10.1145/1073001.1073002.

[WWB+05b] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, N. Memon. PassPoints: design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1-2):102–127, 2005. doi:10.1016/j.ijhcs.2005.04.010. URL http://portal.acm.org/citation.cfm?id=1090412.1090418.

[YBAG04] J. Yan, A. Blackwell, R. Anderson, A. Grant. Password memorability and security: empirical results. *IEEE Security Privacy*, 2(5):25 –31, 2004. doi:10.1109/MSP.2004.81.

[ZLAZ09] J. Zhang, X. Luo, S. Akkaladevi, J. Ziegelmayer. Improving multiple-password recall: an empirical study. *European Journal of Information Systems*, 18(2):165–176, 2009. doi:10.1057/ejis.2009.9.

Alle URLs wurden zuletzt am 28. 11. 2012 geprüft.

Erklärung

Hiermit versichere ich, diese Arbeit selbständig verfasst und nur die angegebenen Quellen benutzt zu haben.

(Mateusz Mikusz)