schreiner
ProSecure

Produktauthentifizierung per Smartphone

Chancen und Herausforderungen der mobilen Authentifizierung von Sicherheitsmerkmalen

Inhalt

Executive Summary

Der Vertriebsprozess physischer Waren befindet seit Jahren im Wandel und der Anteil des Onlinehandels wächst weiterhin stetig. Durch den fehlenden persönlichen Kontakt kann der Käufer die Vertrauenswürdigkeit eines Verkäufers nur schwer einschätzen. Diese Entwicklung nutzen Kriminelle verstärkt aus und schleusen gefälschte Waren in die Lieferkette ein. Um die Risiken und Schäden durch gefälschte Produkte für sich und ihre Kunden soweit wie möglich zu minimieren, müssen Hersteller und Markeninhaber mit geeigneten Produktschutzstrategien reagieren.

Ein wirkungsvolles Produktschutzkonzept ist die Echtheitsprüfung von Produkten per Smartphone durch den Verbraucher/Konsumenten. Voraussetzung dafür ist, dass die Produkte mit entsprechenden Sicherheitsmerkmalen ausgestattet sind, sodass

- die Originalität eines Produktes innerhalb der Supply Chain immer und überall durch jeden überprüft werden kann. Diese Möglichkeit, Fälschungen jederzeit leicht und zuverlässig aufzudecken, stellt eine hohe Abschreckung für Fälscher dar, zumal Smartphones heutzutage flächendeckend verfügbar sind.
- auch verborgene Sicherheitsmerkmale überprüft werden können. Diese bieten bei gleichen Kosten gegenüber offenen Merkmalen eine höhere Fälschungssicherheit und haben einen größeren Entwicklungsspielraum.
- Smartphones genutzt werden können, um einen aus Produktsicht „sicheren Einstieg in die digitale Welt“ zu realisieren. Denn nur, wenn ein Produkt per Smartphone zuerst als Original bestätigt wird, ist sichergestellt, dass auch die zugehörigen, ebenfalls per Smartphone abrufbaren Daten und Dienstleistungen des Herstellers für dieses Produkt tatsächlich gültig sind.

Heute ist es insbesondere für Verbraucher schwer bis unmöglich zu beurteilen, ob es sich bei einem erworbenen Produkt um ein Original oder eine Fälschung handelt. Die Möglichkeit ein Smartphone zur Originalitätsprüfung eines Produktes zu nutzen, erscheint daher auch im Sinne des Verbraucherschutzes hoch attraktiv. Die Bewertung, ob ein Original oder eine Fälschung vorliegt, erfolgt automatisiert; ebenso die Aufnahme eines geeigneten Bildausschnittes auf Basis von leistungsfähigen Algorithmen. Darüber hinaus lässt sich durch eine ansprechende Gestaltung der Benutzerschnittstelle und integrierte Gamification-Elemente Kundenbegeisterung und Kundenbindung erzielen.

Doch es gibt Hürden bei der Realisierung solcher Lösungen: Die zunehmende Fragmentierung verschiedener Smartphone-Modelle und die unterschiedlichen Eigenschaften der Smartphone-Kameras stellen hohe Anforderungen bei der Entwicklung eines geeigneten Sicherheitsmerkmals: Es muss einerseits robust gegenüber Manipulationen sein und und andererseits müssen die besten Fälschungen auch bei unterschiedlichsten Aufnahmenbedingungen mit unterschiedlichsten Smartphones zuverlässig von den Originalen unterschieden werden können. Dies setzt ein umfassendes Wissen voraus – über die Fertigungsprozesse von Sicherheitsmerkmalen und ihre verschiedenen Eigenschaften, wie z. B. Druckauflösung, Kontrast und Farbräume, die Qualität und Messstabilität dieser Eigenschaften in Bezug auf die Bandbreite der existierenden Smartphone-Modelle.

Das vorliegende Whitepaper diskutiert diese Aspekte vertiefend.

1. Einleitung

1.1. Gefährdete Branchen

Es gibt unzählige Erhebungen zum Ausmaß des Handels mit gefälschter Ware. Die jüngste OECD-Studie beziffert den entsprechenden Anteil des Welthandels auf 3,3 %. In die Europäische Union werden demnach jährlich gefälschte Güter im Wert von 121 Milliarden Euro importiert (Stand 2016), was einem Anteil von 6,8 % entspricht; im Jahr 2013 betrug der Anteil noch 5 %. Dies sind jedoch nur Durchschnittswerte und einige Märkte sind noch erheblich stärker von Fälschungen betroffen. So nennt die Studie einige Branchen, in denen die Fälschungsquote überdurchschnittlich hoch ist, wie beispielsweise bei Parfums, Kosmetika, optischen/fotografischen bzw. medizinischen Geräten oder Uhren, und darüber hinaus einige Branchen, bei denen diese Quote sogar zwischen 12 % und 23 % beträgt, dazu zählen elektrische Anlagen, Kleidung, Lederwaren und Schuhe (OECD, Trends in Trade in Counterfeit and Pirated Goods, 2019). In diesem Ausmaß entsteht ein beträchtlicher Schaden für den Markeninhaber, der im schlimmsten Fall existentiell sein kann. Je nach individueller Bedrohung drängen sich für ihn daher Maßnahmen zum Schutz seiner Umsätze und Reputation sowie seiner Rechte und seines geistigen Eigentums auf.

1.2. Lebenszyklus des Betrugsmanagements

Denkbare Schutzmaßnahmen sind individuelle Elemente einer idealerweise ganzheitlichen Strategie im Sinne eines Fraud Management Lifecycles – dem Lebenszyklus des Betrugsmanagements –, durch den ein Unternehmen vor Betrug und Schaden geschützt werden soll. Dazu gehört zunächst die Etablierung und Pflege entsprechender Rahmenbedingungen und Prozesse um vor solchen Schäden abzuschrecken und vorzubeugen, sowie die Erkennung, Untersuchung, Eindämmung und Verfolgung von Schadensfällen (W. Wilhelm, Journal of Economic Crime Management, 2004 2).

Ein sehr wichtiges und zukunftsweisendes Element einer solchen Strategie ist die Authentifizierung von Produkten per Smartphone, die im Nachfolgenden vertiefend behandelt wird. Im Prinzip kann sich der Fraud Management Lifecycle nicht nur auf gegenständliche Objekte beziehen, sondern beispielsweise auch auf Finanztransaktionen, geistige Eigentumsrechte oder Versicherungsbetrug. Im Kontext der Authentifizierung per Smartphone zielt das vorliegende Whitepaper jedoch auf konkrete Produkte.

Abbildung 1: Einfallstore in die Lieferkette für gefälschte Waren.

1.3. Herausforderung Vertrauenswürdigkeit

Gefälschte Ware kann an unterschiedlichen Stellen in die Lieferkette eindringen (Abb. 1). Traditionell wurden Güter über Großhändler an Einzelhändler verteilt und von dort an die Verbraucher verkauft. Unter diesen Bedingungen wurde die Originalität der Produkte durch den Zoll geprüft, der bei grenzüberschreitenden Transporten Stichprobenkontrollen durchführt. Zum anderen konnte der Käufer auch persönlich am Point of Sale die Vertrauenswürdigkeit des Verkäufers einschätzen.

Dieser Vertriebsprozess hat sich durch die zunehmende Nutzung des Internets und Online-Handels jedoch stark gewandelt. In Deutschland wurde in 2020 ein Onlineanteil erreicht, der bei ca. 14 % des Einzelhandelsumsatzes lag. Bis 2024 wird ein weiteres Wachstum auf bis zu 19,4 % prognostiziert. (IHF Köln, 2021). Bei einem Einkauf im Internet gestaltet sich für den Endkunden die Beurteilung der Vertrauenswürdigkeit des Verkäufers jedoch ungleich schwieriger. Gleichzeitig reduziert auch der explosionsartige Anstieg der internationalen Paketpost die Wirksamkeit der Zollkontrollen. Wird dann noch die Tatsache berücksichtigt, dass beim Direktvertrieb über das Internet das Risiko eliminiert ist, dass ein gewerblicher Zwischenhändler ein Produkt als Nachahmung oder Imitat entlarvt, dann wundert es nicht, dass für Fälscher der Online-Handel hoch attraktiv ist.

1.4 Motivierte Verbraucher

Die sich neu entwickelnden Warenströme umgehen damit zum Teil auch etablierte Kontrollen und bieten aufgrund des Online-Vertriebs auch keine sonstigen Angriffspunkte für Kontrollen. Somit bleibt als einzige Möglichkeit, dass die Originalitätsprüfung des Produkts durch den Endkunden durchgeführt wird.

Verbraucher wollen dies auch durchaus aktiv unterstützen. Zwar gibt es eine Minderheit von etwa 17 % der Online-Käufer, die bewusst gewillt sind, Plagiate zu kaufen (MarkMonitor, Online Barometer, 2017), die überwiegende Mehrheit der Kunden hingegen legt Wert auf Originalware.

1.5. Hilfsmittel zur Authentifizierung

Üblicherweise verfügt der „Otto-Normalverbraucher“ jedoch selbst nicht über einfache Prüfmittel wie Lupen, Mikroskope oder UV-Lampen. Dem Verbraucher bleibt daher nur die Sichtprüfung, die über offene, mit dem Auge erkennbare Sicherheitsmerkmale wie beispielsweise Hologramme realisiert werden kann. Doch um via Sichtprüfung ein Imitat anhand eines Sicherheitsmerkmals zuverlässig erkennen zu können, muss der Endkunde wissen, welche Merkmale das Original und eine Fälschung voneinander unterscheiden.

In diesem Kontext rückte in den letzten Jahren mehr und mehr das Smartphone in den Fokus: So können z. B. moderne Bilderkennungssoftware oder KI-basierte Methoden genutzt werden, um die Echtheit eines Produkts zu überprüfen.

Bemerkenswert ist dabei, dass zunächst eine Erscheinungsform der Digitalisierung, nämlich der Online-Handel, überhaupt erst eine der Ursachen für das verstärkte Auftreten gefälschter Produkte war, gleichzeitig die Lösung dieses Problems aber durch eine andere Facette der Digitalisierung ermöglicht wird, nämlich durch die mittlerweile allgegenwärtige Verfügbarkeit von Smartphones, mit denen ein Endkunde die Originalität eines Markenartikels verifizieren kann.

1.6. Mehr Sicherheit für den Verbraucher

Die Produktauthentifizierung per Smartphone bietet mehrere Vorteile. Bisher war es zum Beispiel notwendig, sich vor der Echtheitsprüfung eines Produktes über ein Sicherheitsmerkmal zu informieren und sich die relevanten Merkmale und Erscheinungsbilder zu merken. Eine App-basierte Echtheitspürfung hingegen führt durch die Prüfung und nimmt sogar die Entscheidung über die Echtheit des Produkts ab, da die Authentifizierung vollautomatisch erfolgen kann. Dies geht einher mit der Möglichkeit, dass das Sicherheitsmerkmal nicht mehr zwingend für das menschliche Auge sichtbar sein muss, wenn es mit Hilfe der entsprechenden Smartphone-App lokalisiert und geprüft werden kann. Besonders für kleine Produkte/Verpackungen, die keinen Platz für ein offenes Sicherheitsmerkmal bieten, ist dies eine interessante Lösung.

Ein weiterer Aspekt ist die nahezu uneingeschränkte Internetfähigkeit eines Smartphones. Eine erkannte Fälschung kann automatisch und quasi in Echtzeit per Smartphone an den Hersteller zurückgemeldet werden. Die sich daran anschließenden Maßnahmen – eine zielgerichtete Untersuchung und die Verfolgung und Eindämmung dieser Betrugsvorfälle – schreckt potenzielle Fälscher stark ab und machen eine derart abgesicherte Ware für die Nachahmung uninteressant.

Das Smartphone eröffnet dem Nutzer auch einen sicheren Einstieg in die digitale Welt: Es stellt das Bindeglied zwischen einem Produkt und den mit dem Produkt verbundenen digitalen Daten und Dienstleistungen eines Herstellers dar. Nur wenn über eine Authentifizierung des Produkts sichergestellt ist, dass es sich um ein vertrauenswürdiges Original handelt, sind diese digitalen Angebote auch für das Produkt gültig. Somit ist nur auf Basis eines geprüften Originalprodukts der Einstieg in diese digitale Welt wirklich sicher.

2. Das Smartphone als ideales Prüfmittel

Die Kernaufgabe der Produktauthentifizierung mit einem Smartphone besteht darin, Originale sicher von Nachahmungen unterscheiden zu können. Daher werden im Folgenden zunächst die Kriterien beschrieben, die das Sicherheitsniveau bestimmen, bevor einige technischen Eigenschaften von Smartphones betrachtet werden und abschließend die Wirkung der Authentifizierung auf den Benutzer beleuchtet wird.

2.1. Das Sicherheitsniveau

Um den Zuwachs an Sicherheit durch eine Prüfung mit einem Smartphone abschätzen zu können, kann auf die Normen ISO 22380 und ISO 12931 zurückgegriffen werden. Die im Jahr 2018 eingeführte ISO-Norm 22380 „Sicherheit und Resilienz - Authentizität, Integrität und Vertrauen für Produkte und Dokumente“ beschreibt allgemeine Grundsätze zur Beurteilung des Risikos von Produktfälschungen. Demnach bevorzugen Betrüger gemäß der kriminalsoziologischen Theorie der rationalen Entscheidung solche Ziele, die einerseits verwundbar und andererseits für sie wirtschaftlich lohnend sind. Eine Verwundbarkeit liegt vor, wenn die Gegenmaßnahmen gering ausgeprägt sind, wobei vier konkrete Strategien genannt werden, um diese Gegenmaßnahmen zu gestalten:

- Verzögerung betrügerischer Aktivitäten etwa dadurch, dass Reverse Engineering erschwert wird;
- Vorbeugung durch Verbraucherinformation;
- Sorge tragen, dass Nachahmungen erkannt werden, zum Beispiel durch eine Authentifizierung;
- Abschreckung durch Verfolgung und Aufklärung von Betrugsversuchen.

Die Integration eines Sicherheitsmerkmals verfolgt demnach das Ziel, Fälschungen zu erkennen. Darüber hinaus wird zusätzlich die Abschreckung verstärkt, wenn die Authentifizierung mit einem Smartphone erfolgt; denn mit der Entdeckung kann automatisch die Rückmeldung an den Markeninhaber verbunden werden, sodass die Untersuchung und idealerweise die strafrechtliche Verfolgung eines Betrugsversuchs eingeleitet werden kann.

Die 2012 eingeführte ISO-Norm 12931 benennt die Leistungskriterien für Authentifizierungslösungen zur Bekämpfung der Fälschung von materiellen Gütern und teilt alle denkbaren Anwendungen in die Kategorien offen und verborgen ein (siehe Tabelle 1). Offene Sicherheitsmerkmale ermöglichen jedem Anwender einen Schnelltest innerhalb von zehn Sekunden. Verborgene Merkmale hingegen sind fast ausschließlich einem eingeschränkten Personenkreis vorbehalten, denn obwohl ein Verbraucher durchaus handelsübliche Prüfmittel wie zum Beispiel ein Mikroskop, eine Lupe oder eine UV-Lampe kaufen kann, wird er dies jedoch eher nicht tun.

Wenn die Endkunden nun über die bisher üblichen offenen Sicherheitsmerkmale hinaus zusätzlich auch verborgene Sicherheitsmerkmale prüfen können, dann steigt sowohl die Häufigkeit von Prüfungen als auch das Sicherheitsniveau.

	Menschliche Sinne	Prüfmittel		forensisch
		handelsüblich	anwendungs-spezifisch	
Allgemeine Öffentlichkeit	offen	verborgen	–	–
Eingeschränkter Personenkreis	offen	verborgen	verborgen	verborgen

Tabelle 1: Kategorisierung der Anwendungen gemäß ISO-Norm 12931.

Um das Sicherheitsniveau der mit einem Smartphone prüfbaren Sicherheitsmerkmale vollständig zu erörtern, muss beleuchtet werden, in welcher Form die Sicherheitsmerkmale vorliegen. Typischerweise werden Sicherheitsmerkmale in Produktetiketten und -verpackungen integriert. Dies kann auf Basis unterschiedlicher Druckverfahren erfolgen, beispielsweise Flexodruck, Offsetdruck, Siebdruck und Inkjetdruck, aber auch mit Heiß- oder Kaltprägeverfahren, Stanztechniken oder per Laserstrukturierung. Darüber hinaus können Prozesse mit einer Zufallskomponente genutzt werden, etwa mit Papierfasern oder mittels einer ungeordneten Verteilung kleiner aber sichtbarer Pigmente in einer Trägerfarbe. Der Vorteil dieses Ansatzes ist, dass nicht einmal der Hersteller des Sicherheitsmerkmals selbst ein Duplikat eines solchen Originals anfertigen kann.

2.2. Die Verfügbarkeit von Smartphones

Erst die allgegenwärtige Verfügbarkeit von Smartphones ermöglicht die technische Prüfung von Produkten über die bloße Inaugenscheinnahme hinaus. Weltweit nutzen 5,2 Milliarden Menschen Smartphones. Gut die Hälfte des gesamten Internetverkehrs geht von Smartphones aus, und das, obwohl die Nutzer nur 9 Prozent ihrer Nutzungszeit mit dem Browsen verbringen, der Großteil entfällt auf die Nutzung von Apps sozialer Netzwerke oder zur Kommunikation. Bereits auf Platz drei der Anwendungen folgen Shopping-Apps mit einem Anteil von 66 Prozent, d. h. eine Zielgruppe von 3,4 Milliarden Menschen kann bei ihren Einkaufsvorgängen mittels Produktauthentifizierung unterstützt werden (we are social & Hootsuite, Digital 2020: Global Digital Overview).

In den Anfangsjahren der Smartphonenutzung war die Marktstruktur noch übersichtlicher. Mitte 2012 waren zwei Drittel aller Geräte mit iOS von Apple ausgestattet, die sich auf die Modelle iPhone 3G, 4 und 4s verteilten. Mittlerweile ist der Markt an Smartphone-Modellen stark fragmentiert. Anfang 2020 erreichte selbst das bestverkaufte Modell lediglich einen Marktanteil von 2,3 Prozent und nur die Modelle der Top Ten konnten die Hürde von einem Prozent überhaupt noch überspringen (Strategy Analytics, 30. April 2020).

2.3. Smartphones als Messinstrument

Ein Smartphone an sich ist jedoch nicht ausreichend für den erfolgreichen Einsatz zur Originalitätsprüfung von Produkten, es muss zudem für diesen Zweck geeignet sein. Der Verifikationsprozess besteht aus zwei Hauptschritten: Zunächst erfolgt die Aufnahme eines oder mehrerer Bilder, dann folgt die Bildanalyse. Insbesondere für diesen zweiten Teil gibt es kaum noch Einschränkungen, nachdem die Rechenleistung aktueller Smartphones die Leistungsfähigkeit von einem Supercomputer von vor zwanzig Jahren erreicht. Bei der Bildaufnahme hingegen gibt es keine definierten Mindestqualitätsstandards. Hier ist es entscheidend zu wissen, was aus technischer Sicht von Smartphones erwartet werden kann.

Absolute Werte können mit einem zu diesem Zweck konstruierten Messinstrument ermittelt werden. Bei einer Authentifizierung via Smartphone ist dies nur eingeschränkt möglich, da die Bandbreite eingesetzter Smartphone-Modelle keine verlässliche Aussage über absolute Messwerte zulässt. Auch eine Kalibrierung

des Smartphones scheidet aus, da dafür ein Originalmuster physisch vorliegen muss. Dieses müsste jedoch an den Nutzer verteilt werden, was dem Ziel widerspricht, dass das Messmittel beim Prüfer bereits verfügbar sein soll, ohne dass ein Logistik-Aufwand nötig ist.

In vielen Fällen ist es daher vorteilhaft, wenn in einem Sicherheitsmerkmal zum Beispiel zwei Farben oder zwei Helligkeiten miteinander verglichen werden können, etwa in Form zweier räumlich nebeneinanderliegender Motive oder indem ein und dasselbe Motiv aus unterschiedlichen Richtungen betrachtet wird oder es sich tatsächlich über die Zeit verändert – beispielsweise nachdem es mit dem Blitzlicht des Smartphones angeregt worden ist. Bei einem solchen Vergleich ist nur noch ein bestimmter Mindestunterschied zu detektieren, der unabhängig vom absoluten Wert ist.

3. Technische Merkmale von Smartphonekameras

Bei einer Messung ist die Stabilität des Messwerts entweder durch die Schwankung der Qualität des zu messenden Objekts (= Sicherheitsmerkmal) oder durch die mangelnde Genauigkeit des Messgeräts (= Smartphone) begrenzt. Wenn die durch das Sicherheitsmerkmal begründeten Schwankungen klein sind im Vergleich zum Messverfahren, können Effekte beobachtet werden, die die mit der Nutzung eines Smartphones einhergehenden Einschränkungen beschreiben.

Für die Entwicklung von Sicherheitsmerkmalen zur Prüfung mit einem Smartphone ist es glücklicherweise ausreichend, welche Eigenschaften die Mehrheit der Smartphonemodelle aufweist, da besonders gute Smartphonekameras nicht immer verfügbar sind, sondern im Allgemeinen eben nur typische Smartphonekameras.

3.1. Die Kameraauflösung

Für manche Modellreihen hat sich seit 2016 beginnend mit dem iPhone 6s bzw. mit dem Samsung Galaxy S7 für die Kameraauflösung das Format 4272 x 2848 Pixel etabliert, was einer Kameraauflösung von 12,2 MegaPixel entspricht. Stand August 2020 waren 114 Smartphonemodelle mit dieser Kameraauflösung verfügbar. Die Spitze bilden jedoch das Xiaomi Mi 10, das Samsung S20 Ultra und das Motorola Edge, die mittlerweile 108 MegaPixel in Form von 12032 x 9024 Pixel erreichen.

3.2. Die Bildqualität

Die Kameraauflösung darf jedoch nicht automatisch gleichgesetzt werden mit der Bildqualität. Als Benchmark für die Bildqualität ist bisher einzig ein von der französischen Firma DXOMARK entwickelter proprietärer Ansatz verfügbar, demgemäß auch bei einer konstanten Kameraauflösung von 12,2 MegaPixel die Bewertung der Bildqualität vom iPhone 7 (Markteinführung 2016) bis zum iPhone 11 von 88 auf 109 gestiegen ist, während gleichzeitig der Benchmarkwert vom Samsung S7 Edge (ebenfalls aus dem Jahr 2016) bis zum Samsung Galaxy S20 Ultra von 89 auf 122 geklettert ist.

Technisch offengelegt ist der im Jahr 2016 veröffentlichte Standard IEEE 1858 für die Bildqualität von Smartphonekameras, der auf der Messung des Ortsfrequenzgangs, von Farbton und Farbsättigung, der Farbhomogenität, lokaler geometrischer Verzerrungen, Texturunschärfe und dem sichtbaren Rauschen beruht. Die Einflussfaktoren auf diese messbaren Eigenschaften eines Bildes sind jedoch vielschichtig: In die Bildqualität gehen neben der Kameraauflösung auch Optik, Aufnahmedauer, Größe der Sensorfläche, Autofokus, Bildstabilisator und zunehmend die in die Bildaufnahme integrierte Bildnachverarbeitung ein.

3.3. Bildschärfe und Bildkontrast

Ein häufig genutztes Maß zur Charakterisierung der Auflösungsfähigkeit ist die Modulationstransferfunktion (MTF). In der Abbildung 2 ist schematisch dargestellt, welche Information darin enthalten ist. Auf der x-Achse ist die Ortsfrequenz aufgetragen, d. h. die Dichte der Linien einer Teststruktur. Üblicherweise wird dafür die Einheit lp/mm verwendet (lp = line pair: ein Paar aus einer dunklen und einer hellen Linie). Auf der y-Achse wird aufgetragen, wie groß der Helligkeitskontrast zwischen den schwarzen Flächen der Linien und den hellen Bereichen zwischen den Linien ist. Bei korrektem Weißabgleich werden die Linien idealerweise vollkommen schwarz und die Zwischenräume dazwischen reinweiß dargestellt, was einer Modulation des Helligkeitswerts von 100 Prozent entspricht. Wird die Dichte der Linien erhöht, schafft es das optische System zunehmend nicht mehr, den vollständigen Kontrast zwischen den hellen und den dunklen Bereichen darzustellen. Diesen fließenden Übergang beschreibt die Modulationstransferfunktion. Die ISO-Norm 12233 definiert die Bildauflösung als diejenige Liniendichte, bei der die Modulationstransferfunktion den Wert 5 Prozent aufweist. Interessant für die Konstruktion von Sicherheitsmerkmalen ist, dass tangential ausgerichtete Linien, auch als meridionale Linien bezeichnet, systematisch kritischer sind als radial ausgerichtete Linien, die sogenannten sagittalen Linien. Um eine möglichst gute Auflösung zu erreichen, sollte ein Sicherheitsmerkmal daher als konzentrische Kreise oder zumindest als Linien entlang gedachter Kreislinien aufgebaut sein.

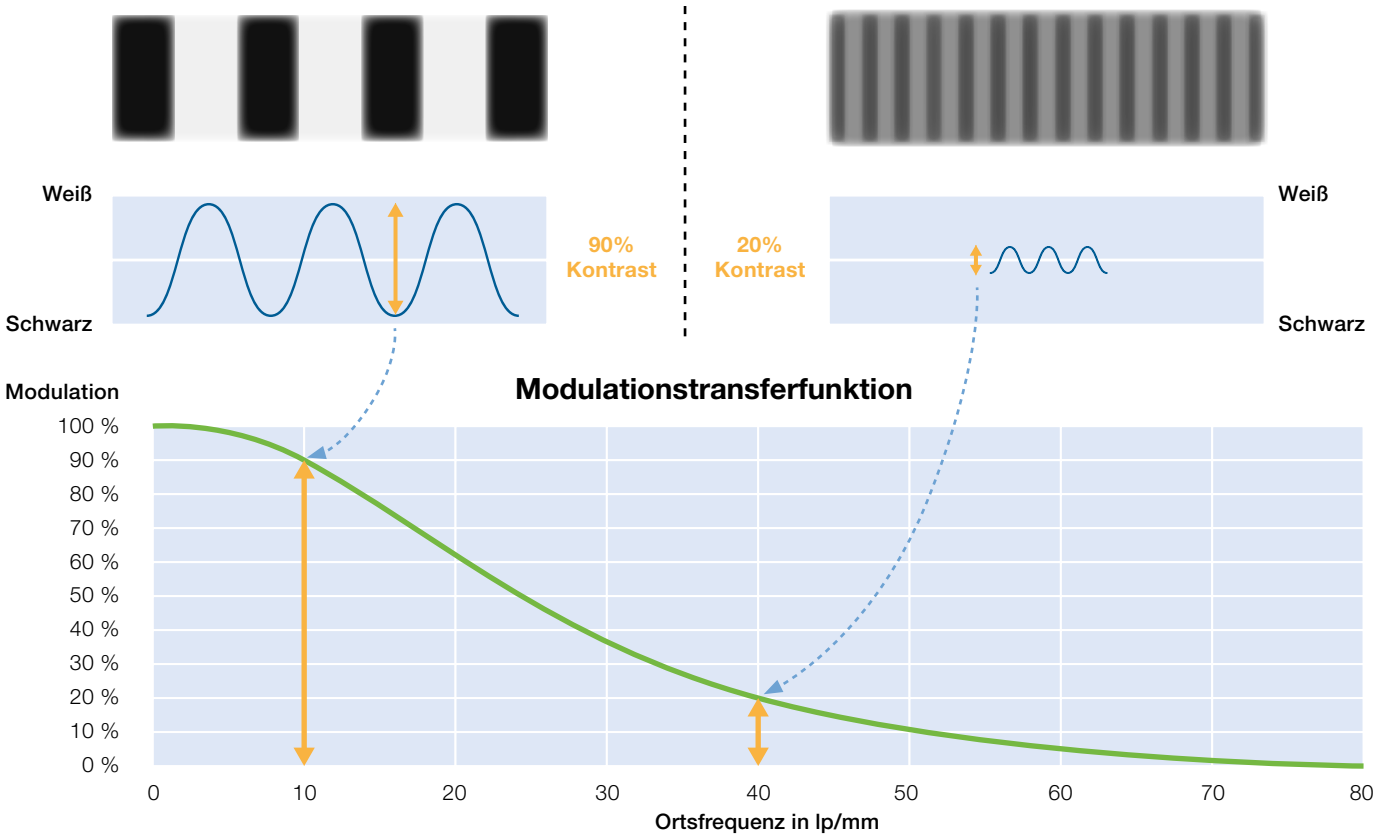

Abbildung 2: Funktionsweise der Modulationstransferfunktion anhand von Beispielen mit einer hohen bzw. einer niedrigen Modulation.

3.4. Bildabstand und Zoom

Der Zusammenhang zwischen der Kontrastmodulation und der Liniendichte (Abbildung 2) gilt zunächst nur für den Bildabstand, mit dem das entsprechende Bild aufgenommen wurde. Wird der Abstand zwischen der Kameralinse und dem Objekt reduziert, vergrößert sich proportional dazu das Abbild auf dem Kamerasensor – so lange, bis die Brechkraft des optischen Systems nicht mehr in der Lage ist, den betrachteten Gegenstand scharf auf den Kamerasensor abzubilden.

Üblicherweise können Smartphonekameras Objekte bis zu einem Bildabstand von etwa sechs Zentimetern scharf stellen. Ist der Bildabstand kleiner, wird meist keine Aufnahme ausgelöst. Abbildung 3 stellt dar, wie sich die Bildqualität bei der Annäherung der Kamera an das Objekt entwickelt. Der obere Rand der dargestellten Messwerte zeigt eine klare Grenze der für den Bildabstand jeweils erreichbaren maximalen Bildqualität, die für größere Bildauflösungen kontinuierlich ansteigt. Nach unten ist keine klare Grenze erkennbar, was zum Beispiel an einem durch das Autofokussystem nicht perfekt eingestellten Fokusabstand liegt oder an einer Bewegungsunschärfe verursacht durch eine Freihandaufnahme.

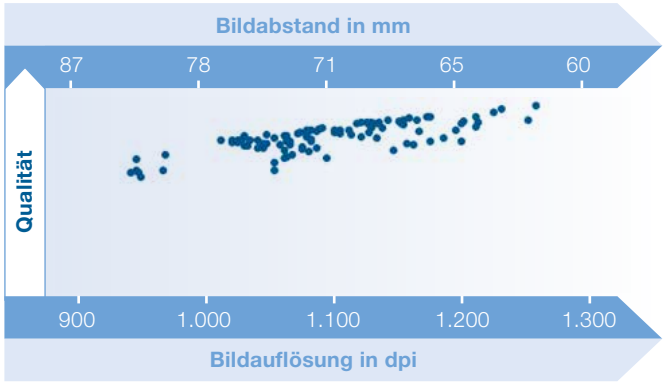

Abbildung 3: Abhängigkeit der Bildqualität vom Abstand zwischen Kamera und Objekt.

3.5. Die Aufnahmedauer

Die Ursache für eine verminderte Bildqualität ist häufig eine geringe Aufnahmedauer. Dieser Zusammenhang wurde bereits empirisch untersucht (Abbildung 4) und belegt, dass diese beiden Eigenschaften zueinander im Wettbewerb stehen. Da selten bewegte Objekte geprüft werden, sind mit Blick auf die Authentifizierung von Produkten die Smartphonekameras mit Stärken bei der Aufnahmedauer nicht hilfreich, da mit diesen Modellen durchweg eine geringere Bildqualität einhergeht. Es kann also nicht generell eine hohe Bildqualität vorausgesetzt werden. Je geringer die Anforderungen des Sicherheitsmerkmals an die Bildqualität, desto größer ist der Anteil an geeigneten Smartphonemodellen.

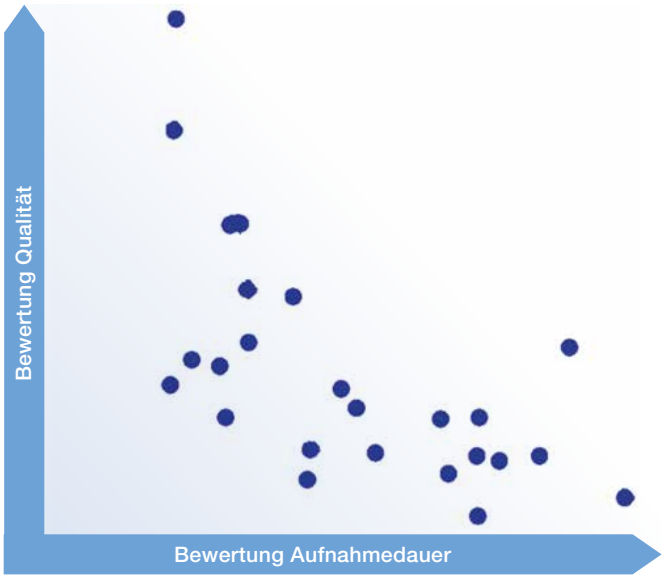

Abbildung 4: Qualität und Aufnahmedauer nach Veli-Tapani Peltoketo, Benchmarking of Mobile Phone Cameras, 2016.

3.6. Die Beleuchtungsabhängigkeit

Im Kontext der Produktauthentifizierung werden keine aktiven Lichtquellen betrachtet, sondern zu prüfende Objekte, die passiv beleuchtet werden. Das kann zum einen Tageslicht sein, das etwa mittags an einem Nordfenster scheint bei indirekter Beleuchtung durch die Sonne (entspricht CIE-Normbeleuchtung D65). Sein Spektrum weist ein Maximum bei etwa 450 nm auf und fällt zu beiden Seiten nur schwach ab. Zum anderen könnte eine künstliche Beleuchtung vorliegen, entweder durch eine traditionelle Glühlampe, bei der die roten Wellenlängenanteile dominieren, oder durch Leuchtstoffröhren, die im roten, grünen und blauen Wellenlängenbereich jeweils eine schmale, dafür aber sehr hohe Spitze aufweisen. Das tatsächliche farbliche Erscheinungsbild von Motiven variiert dement-

sprechend stark mit der Beleuchtungssituation. Hilfreich ist in diesem Fall, dass in Smartphones mit Blitzlicht-LEDs eine eigene Beleuchtung integriert ist. Ihr Emissionsspektrum ist im Vergleich zu den sonst möglichen Beleuchtungssituationen vergleichsweise gut definiert (Abbildung 5).

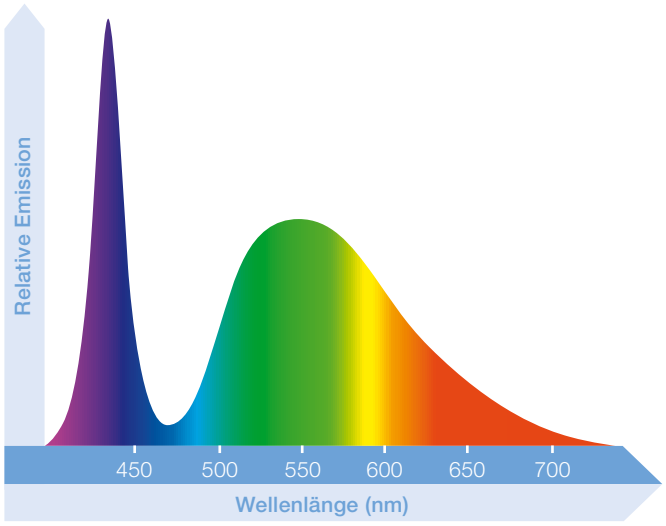

Abbildung 5: Emissionsspektrum einer typischen in einem Smartphone integrierten Blitzlicht-LED.

3.7. Die Farbtreue

Die zuverlässige Bestimmung einer Farbe hängt davon ab, wie verlässlich die Farbempfindlichkeit der verwendeten Smartphonekamera ist. Gemäß der ISO-Norm 17321 ist der sogenannte sensitivity metamerism index (SMI) ein Maß dafür, wie genau eine Kamera Farben reproduzieren kann. Dieser Index ist definiert als SMI = 100 – 5,5 ΔE, wobei gemäß der Norm der mittlere Farbabstand durch eine Mittelung der Messungen über eine komplette Farbtafel zu bestimmen ist.

Die Abbildung 6 zeigt die Ergebnisse über eine repräsentative Auswahl an Smartphonemodellen. Alle Farben weisen einen Farbabstand zum eigentlich auf der Farbtafel dargestellten Farbort von etwa 10 auf. Die Standardabweichung des Farbabstands über unterschiedliche Smartphonemodelle fällt hierbei für die natürlichen Farben mit ±4,6 am kleinsten aus. Die Standardabweichung steigt, je weiter sich der Farbtyp von den natürlichen Farben entfernt und erreicht bei den unbunten Graustufen schließlich den Wert ±13,9. Um unabhängig vom Smartphonemodell ein möglichst belastbares Ergebnis zu erhalten, sollten daher

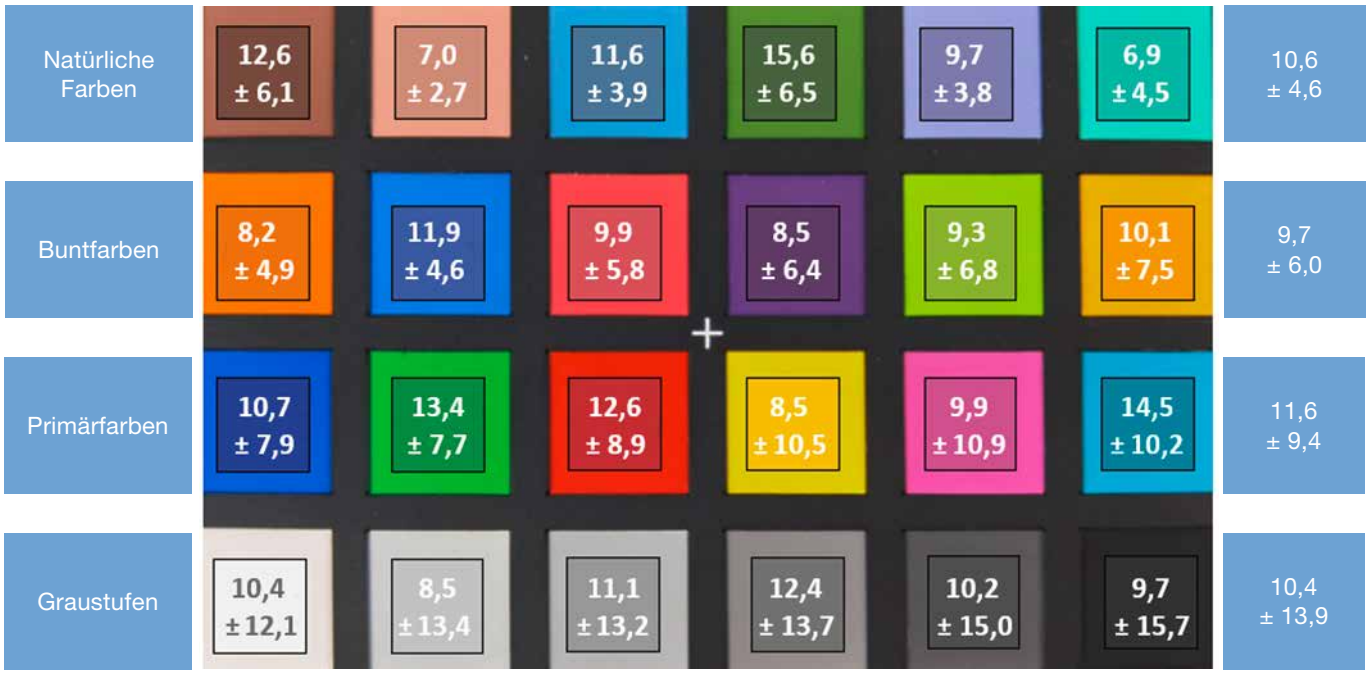

Abbildung 6: Farbwiedergabe des Testcharts ColorChecker von X-Rite für eine repräsentative Auswahl an Smartphones. Die Werte stellen den Farbabstand ΔE zwischen der mit einem Smartphone gemessenen Farbe und dem nominellen Farbort des Testfeldes dar. Auf der rechten Seite ist der Mittelwert für die Farben der in dieser Zeile dargestellten Farbgruppe angegeben.

natürliche Farben gewählt werden, wenn der Farbort als Kriterium für ein Sicherheitsmerkmal verwendet werden soll.

3.8. Die Internetanbindung

Bestimmte Sicherheitsmerkmale sind technisch erst mit einer Internetverbindung überprüfbar, ebenso die Rückmeldung des Prüfergebnisses an beispielsweise den Markeninhaber. Es gibt drei Ansätze:

- Der Online-Zugang wird obligatorisch vorgeschrieben, wenn aus technischen Gründen eine Online-Verbindung erforderlich ist, etwa um auf eine zentrale Datenbank zugreifen zu können, in der zum Beispiel charakteristische Merkmale von Sicherheitsmerkmalen abgelegt sind, die zur Überprüfung benötigt werden.
- Die Authentifizierung des Sicherheitsmerkmals kann offline durchgeführt werden, falls entweder keine zusätzlichen Informationen für die Prüfung benötigt werden oder die Daten beispielsweise als QR-Code auf dem Gegenstand hinterlegt sind (= self authentication). Wenn keine Internetverbindung nötig ist, ist die Nutzbarkeit nicht eingeschränkt. Der Markeninhaber erhält dann jedoch keine Rückmeldung darüber, ob Fälschungen flächendeckend auftreten oder Hotspots existieren. Der Nutzer kann keine zusätzlichen relevanten Daten abrufen, etwa zur Verwendung des Produkts.
- Prüfung als Hybridlösung: Die Offline-Authentifizierung wird zugelassen, vorgeschrieben ist aber eine gelegentliche Rückmeldung an einen zentralen Server innerhalb eines definierten Zeitraums. Andernfalls wird die Prüfmöglichkeit deaktiviert. Auf diese Weise können die Vorteile der Online- und der Offline-Nutzung vereint werden.

Ein Online-Zugang ermöglicht eine weitere Ausprägung der Authentifizierung eines Sicherheitsmerkmals: Die Prüfung ohne App. Damit wird die Hürde umgangen, eine App installieren zu müssen, was die Bereitschaft zur Nutzung erhöht. Je nach Anwendung kann die Benutzerführung selbst ohne App praktikabel gestaltet werden. So kann etwa ein aufgedruckter QR-Code mit einer entsprechenden üblicherweise vorinstallierten Reader-App eingelesen werden. Der Nutzer kann anschließend anhand von Bildern auf der zugehörigen Webseite einen Bildvergleich mit dem vorliegenden Erscheinungsbild durchführen, das zum Beispiel aus zufällig angeordneten Fasern besteht.

4. Die User Experience

Welche Vorteile hat ein Nutzer konkret von der Prüfung mittels Smartphone? Sicherheitsmerkmale, die bisher mit dem bloßen Auge geprüft wurden, können automatisiert geprüft und durch einen in die App integrierten Algorithmus bewertet werden; der Bediener muss in diesem Fall nicht mehr vorab geschult werden. Die Bewertung unterliegt geringeren subjektiven Einflüssen und wird deutlich zuverlässiger.

Der Prüfprozess kann zusätzlich unterstützt werden, indem die App die Bildaufnahme selbsttätig auslöst. Dies entbindet den Nutzer zum einen von der Entscheidung darüber, ob die Bildqualität in der aktuellen Form ausreichend ist und gewährleistet gleichzeitig, dass die Prüfung so wenig Zeit wie nötig in Anspruch nimmt.

Dies gilt umso mehr vor dem Hintergrund, dass für viele Sicherheitsmerkmale zwei Bilder analysiert werden müssen, denn jedes beliebige Erscheinungsbild kann durch ein entsprechendes, in üblichen Druckfarben gefertigtes, statisches Abbild vorgetäuscht werden. Erst bei einer bestimmten – von dem vorliegenden Sicherheitsmerkmal abhängigen – Variation, etwa ein anderer Betrachtungswinkel oder die Zeit nach dem Auslösen des Blitzlichts, verändert sich das Sicherheitsmerkmal charakteristisch und einzigartig. Insbesondere die automatisierte Auswahl von zwei oder mehr für die Auswertung geeigneten Bildern, kann eine große Unterstützung für den Prüfer darstellen.

Manche Markeninhaber möchten ihre Kunden nicht wissen lassen, dass die Produkte auf Echtheit geprüft werden, weil dies eine Besorgnis um die Originalität auslösen könnte. Hier gibt es die Möglichkeit einer Authentifizierung im Hintergrund. Bei offenen Sicherheitsmerkmalen muss der Anwender immer informiert

werden, was zu prüfen ist. Bei halb-verborgenen Merkmalen muss er angeleitet werden, welche Prüfmittel verwendet werden können, um das Sicherheitsmerkmal zu identifizieren oder es muss ihm sogar ein spezielles Prüfgerät zur Verfügung gestellt werden. Ist das Merkmal verborgen muss es mitunter zur Prüfung an ein Labor geschickt werden. Bei Sicherheitsmerkmalen, die hingegen mit einem Smartphone prüfbar sind, kann die Authentifizierung erfolgen, ohne dass es dem Nutzer überhaupt bewusst ist, zum Beispiel, wenn ein QR-Code eingelesen wird oder Augmented Reality eingesetzt wird und das betreffende Produkt dabei mit der Smartphonekamera erfasst wird.

Neben den praktischen Vorteilen ist auch die emotionale Wirkung auf den Bediener zu berücksichtigen: Etwa vier von fünf Kaufentscheidungen gehen nicht auf leichte Sympathie oder rationale Zustimmung zurück, sondern auf starke Begeisterung und Faszination für das Produkt oder die Dienstleistung. Eine ansprechend gestaltete App mit zusätzlichen Gamification-Elementen, wie AR-Features, Fortschrittsbalken, Fadenkreuze oder interaktive Einblendungen, kann dieses Verhalten maßgeblich unterstützen: Sie weckt die Neugier des Nutzers und es ist sehr wahrscheinlich, dass für ihn damit auch das geprüfte Produkt positiv konnotiert ist.

Schreiner ProSecure,
ein Competence Center der
Schreiner Group GmbH & Co. KG
Bruckmannring 22
85764 Oberschleißheim
Deutschland
Telefon +49 89 31584-5540
Fax +49 89 31584-5358
info@schreiner-prosecure.com
www.schreiner-prosecure.com