schreiner
ProSecure

Smartphone-Based Product Authentication

Opportunities and Challenges of Security Feature Authentication Using Mobile Devices

Content

Executive Summary

The sales process of physical goods has been in a state of transformation for years and the share of online retail keeps growing. Due to the lack of personal contact, it is difficult for customers to judge the trustworthiness of sellers. Criminals increasingly take advantage of this development, feeding fake goods into the supply chain. To minimize risks and losses for themselves and their customers to the greatest possible extent, manufacturers and brand owners have to respond with suitable product protection strategies.

Smartphone-based authentication of products by consumers is an effective product protection concept, presupposing that the products are equipped with suitable security features so that

- the authenticity of a product can be verified by anyone at any time within the supply chain; the possibility of readily and reliably revealing fakes acts as a strong deterrent to counterfeiters, especially in view of the wide-spread availability and use of smartphones today;
- even covert security features can be authenticated; at the same costs, they deliver higher levels of counterfeiting security compared to overt features as well as greater development scope;
- smartphones can be used to achieve “reliable entry into the digital world” from the product perspective; the reason is that only an initial smartphone-based confirmation of a product’s authenticity ensures that the manufacturer’s data and services accessible by smartphone are actually valid for this product as well.

Especially for consumers, it is difficult if not impossible today to judge whether a product they have purchased is an original or fake. The opportunity to use a smartphone for authenticating a product is therefore highly attractive, not least in the interest of consumer protection. The evaluation of whether a product is an original or fake is done automatically, as is capturing a suitable image detail based on powerful algorithms. In addition, customer engagement and loyalty can be generated by an appealing design of the user interface and integrated gamification elements.

However, the achievement of such solutions entails some hurdles. The increasing fragmentation of the variety of smartphone models and the diverse characteristics of smartphone cameras pose exacting demands on the development of a suitable security feature: On the one hand, it must resist tampering attempts and on the other, even the best fakes must be reliably distinguishable from the originals even under a wide variety of picture-taking conditions using different smartphones. This presupposes comprehensive know-how—about the manufacturing processes of security features and their various properties such as print resolution, contrast, and color spaces, and the quality and measuring stability of these properties in relation to the wide variety of existing smartphone models.

This white paper discusses these aspects in greater depth.

1. Introduction

1.1. Vulnerable Sectors

The extent of trade in fake goods has been investigated in countless surveys. The most recent OECD report assesses the share of trade in counterfeit and pirated goods at 3.3%. Accordingly, fake goods valued at 121 billion euros per year (as of 2016) are imported into the European Union, which corresponds to a share of 6.8%; in 2013, the share amounted to only 5%. However, these are just averages and some markets are affected by counterfeits even much more severely. The report mentions a number of sectors where the rate of pirated products is above average, such as perfumes, cosmetics, optical/photographic and medical devices, and watches, plus some where this rate is even in a range between 12% and 23%. They include electrical systems, clothing, leather goods, and shoes (OECD, Trends in Trade in Counterfeit and Pirated Goods, 2019). At these rates, brand owners incur considerable losses that, in the worst case, may jeopardize their economic survival. Consequently, this calls for measures to protect their sales and reputation as well as their rights and intellectual property, depending on individual threat scenarios.

1.2. Lifecycle of Fraud Management

Conceivable protective actions are individual elements of an ideally holistic strategy in the spirit of a Fraud Management Lifecycle designed to protect a business against fraud and losses. Initially, they include establishing and maintaining appropriate conditions and processes to deter and prevent such losses as well as the detection, investigation, containment, and prosecution of fraud (W. Wilhelm, Journal of Economic Crime Management, 2004 2).

A very important and forward-thinking element of such a strategy is the smartphone-based authentication of products that will be discussed in greater depth below. Principally, the Fraud Management Lifecycle can refer not only to tangible objects but also to financial transactions, intellectual property rights, or insurance fraud, for example. However, in the context of smartphone-based authentication, this white paper addresses tangible products.

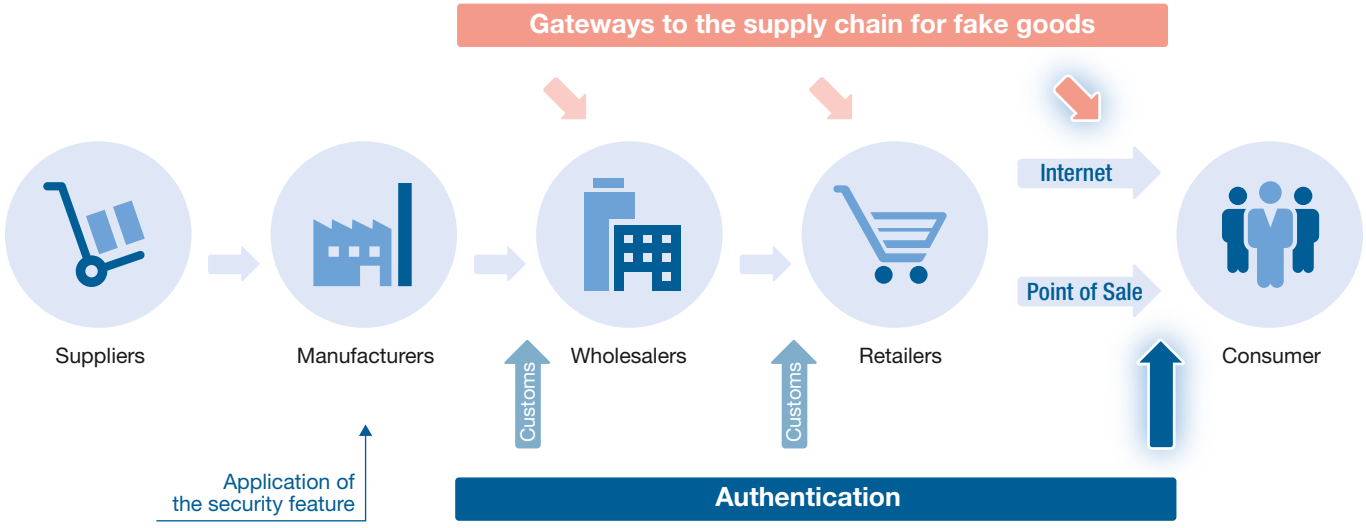

Figure 1: Gateways to the supply chain for fake goods.

1.3. The Trustworthiness Challenge

Fake goods can enter the supply chain in various places (Figure 1). Traditionally, goods used to be distributed via wholesalers to retailers who would sell them to the consumers. Under these conditions, customs inspectors would spot-check the authenticity of products when goods were hauled across international borders. Moreover, buyers were able to personally assess a seller‘s trustworthiness at the point of sale.

This distribution process has changed significantly due to increasing use of the internet and online trade. In Germany, in 2020, the online share of sales amounted to approximately 14% of retail sales. By 2024, further growth to as much as 19.4% is forecast. (IHF Cologne, 2021). However, when purchasing online it is a lot more difficult for consumers to judge a seller‘s trustworthiness. At the same time, the skyrocketing rise of international parcel post reduces the effectiveness of customs inspections. Plus, considering the fact that direct selling via the internet eliminates the risk of a legitimate commercial distributor exposing a product as an imitation or fake, it comes as no surprise that online retail is highly attractive for counterfeiters.

1.4 Motivated Consumers

As a result, the newly emerging flows of goods partly circumvent established checks and, due to online distribution, offer no other points of engagement for inspections either. Hence product authentication by the consumer is the only remaining course of action.

Consumers are indeed ready to actively support this effort. Although there is a 17-percent minority of online buyers who are consciously willing to purchase pirated products (MarkMonitor, Online Barometer, 2017), the vast majority of customers values authentic merchandise.

1.5. Tools for Authentication

Typically, though, simple tools such as magnifying glasses, microscopes, and UV lamps are not readily available to the average consumer, who therefore depends on visual inspections of overt security features such as holograms that can be performed with the naked eye. Yet to be able to reliably identify a fake based on a security feature, the consumer needs to know what characteristics distinguish an original from a counterfeit product.

In this context, smartphones have increasingly become the focus of attention in recent years, as modern image recognition software of AI-based methods, for instance, can be used to authenticate a product.

Remarkable in this context is the fact that a particular manifestation of digitalization—specifically online trade—was one of the causes of the increased incidence of fake products in the first place, whereas another facet of digitalization enables the solution of this problem, namely the now ubiquitous availability of smartphones with which a consumer can verify the authenticity of a branded product.

1.6. Raising Security for Consumers

Smartphone-based product authentication offers several advantages. In the past, for instance, it was necessary to obtain information about a security feature and to memorize the relevant characteristics and manifestations before authenticating a product. By contrast, app-based authentication guides users through the verification process and even relieves them of having to decide whether or not the product is an original because the authentication can be performed automatically. This goes hand in hand with the security feature no longer having to be visible to the human eye when it can be localized and checked by means of the corresponding smartphone app. This is an attractive solution especially for small products/packaging on which there is no space for an overt security feature.

The near-unlimited internet capability of smartphones is another aspect. Feedback on a detected fake can automatically and practically in real time be provided to the manufacturer by smartphone. The follow-up actions—systematic investigation, tracking, and containment of such incidents of fraud—seriously deter potential counterfeiters and spoil their interest in pirating goods that are protected in this way.

Smartphones also pave the way for users' secure entry into the digital world: They provide the connecting link between a product and the digital data and services of a manufacturer related to the product. Only when authentication of the product has ensured that it is a trustworthy original such digital offers are valid for the product as well. Therefore, entering this digital world is truly secure only on the basis of a verified original product.

2. The Smartphone as an Ideal Testing Tool

The key task of smartphone-based product authentication is to enable the reliable distinction of originals from fakes. Therefore, this paper will initially describe the criteria that determine the security level before looking at some of the technical features of smartphones, and subsequently addressing the impact of authentication by the user.

2.1. The Security Level

To assess the increase in security by smartphone-based authentication, the ISO 22380 and ISO 12931 standards can be consulted. The ISO standard 22380 „Security and resilience—Authenticity, integrity, and trust for products and documents" describes general principles for evaluating the risk of product fraud. Accordingly, fraudsters, based on the criminological-sociological theory of rational decision-making, prefer targets that are vulnerable on the one hand and economically beneficial for them on the other. A vulnerability exists when countermeasures are minimal, with four concrete strategies being named for shaping these countermeasures:

- retardation of fraudulent activities, for instance by making reverse engineering more difficult;
- prevention through consumer information;
- ensuring that fakes are detected, for instance by means of authentication;
- deterrence through tracking and investigation of cases of attempted fraud.

Accordingly, the integration of a security feature pursues the goal of detecting counterfeits. In addition, deterrence is reinforced when authentication is smartphone-based because the detection of a fake can automatically be linked to providing feedback to the brand owner so that an investigation and, ideally, the prosecution of a case of attempted fraud can be initiated.

The ISO standard 12931 introduced in 2012 names the performance criteria for authentication solutions to fight counterfeiting of tangible goods and classifies all conceivable applications in the categories of overt and covert (see Table 1). Overt security features enable any user to perform a quick test within ten seconds. Covert features on the other hand are near-exclusively reserved to a limited group of people because, even though consumers can buy commercially available testing tools such as microscopes, magnifying glasses, or UV lamps, it is rather unlikely that they will do so.

Now if consumers can check even covert security features beyond the previously common overt security features, both the frequency and the security level of verifications increases.

	Human senses	Testing tools		Forensic
		Commercially available	Application-specific	
General public	Overt	Covert	–	–
Limited group of people	Overt	Covert	Covert	Covert

Table 1: Categorization of applications according to ISO Standard 12931.

To fully discuss the security level of the security features that can be verified by using a smartphone it is necessary to take a look at the form in which security features are available. Typically, security features are integrated in product labels and packaging. This can be done on the basis of diverse printing technologies such as flexographic printing, screen printing, and inkjet printing as well as by using hot and cold stamping methods, die-cutting techniques, or by laser structuring. In addition, processes with a random component can be used, for instance with paper fibers or by means of a randomized distribution of small but visible pigments in a carrier paint. This approach has the advantage that not even the manufacturer of the security feature can produce a duplicate of such an original.

2.2. Availability of Smartphones

Only the ubiquitous availability of smartphones enables the technical examination of products beyond a purely visual inspection. Worldwide, 5.2 billion people use smartphones. More than half of the entire internet traffic emanates from smartphones even though users are spending only 9 percent of their usage time browsing, while apps for social networks or communication account for the lion‘s share of smartphone usage. Following in third place of the applications are shopping apps with a share of 66 percent, which means that a target group of 3.4 billion people can be supported in their shopping transactions by product authentication (we are social & Hootsuite, Digital 2020: Global Digital Overview).

In the early years of smartphone use, the market structure was still clearer. In the middle of 2012, two thirds of all devices were using iOS from Apple, distributed to the iPhone 3G, 4, and 4s models. By now, the market of smartphone models has become heavily fragmented. At the beginning of 2020, even the top-selling model achieved a market share of merely 2.3 percent and only the models of the top ten managed to jump over the one-percent hurdle at all (Strategy Analytics, April 30, 2020).

2.3. Smartphones as Measuring Instruments

However, a smartphone per se is not adequate for successful use as a means of authenticating products. In addition, it must be suitable for this purpose. The verification process consists of two main steps: First, one or several pictures are taken, followed by image analysis. Particularly for this second part, limitations hardly exist anymore, considering that the computing power of current smartphones achieves the level of a supercomputer twenty years ago. With regard to picture-taking, though, there are no defined minimum quality standards. In this respect, knowledge of what can be expected of smartphones in terms of technology is decisive.

Absolute values can be obtained by means of a measuring instrument designed for this purpose. However, with smartphone-based authentication, this is possible only to a limited extent because the wide variety of smartphone models in use does not allow any reliable conclusion to be drawn about absolute values measured. Neither can smartphones be calibrated because this requires the physical availability of an original sample. Such a sample, however, would have to be distributed to the user, which contradicts the objective of the measuring tool being available to the person performing the authentication without requiring a logistic effort.

In many cases, it is therefore advantageous if, for instance, in a security feature two colors or levels of brightness can be compared with each other, like in the form of two spatially adjacent images, or by looking at the same image from different directions, or by the image actually changing over time—after having been excited by the camera flash of the smartphone, for example. In such a comparison, only a certain minimum difference has to be detected, which is independent of the absolute value.

3. Technical Features of Smartphone Cameras

In a measurement the stability of the measured value is limited either by the variation of the quality of the object to be measured (= security feature) or by the lacking accuracy of the measuring device (= smartphone). When the variations caused by the security feature are small in comparison to the measuring method effects can be observed that describe the limitations which the utilization of a smartphone entails.

Fortunately, for the purpose of developing security features for smartphone-based authentication, the features which the majority of smartphone models offer are sufficient, because particularly good smartphone cameras are not always available whereas only typical smartphone cameras generally are.

3.1. Camera Resolution

For some model ranges since 2016, starting with the iPhone 6s and Samsung Galaxy S7, the format of 4272 x 2848 pixels has become established, which corresponds to a camera resolution of 12.2 megapixels. As of August 2020, 114 smartphone models were available with this camera resolution. However, the Xiaomi Mi 10, Samsung S20 Ultra, and Motorola Edge, which by now achieve 108 megapixels in the form of 12032 x 9024 pixels, are at the high end of smartphone cameras.

3.2. Image Quality

Camera resolution, however, should not automatically be equated to image quality. To date, as a benchmark for image quality, only a proprietary approach developed by the French company DXOMARK has been available, according to which even with a constant camera resolution of 12.2 megapixels the rating of the image quality of the iPhone 7 (market launch in 2016) to the iPhone 11 has increased from 88 to 109 while at the same time the benchmark value from the Samsung S7 Edge (also from 2016) to the Samsung Galaxy S20 Ultra has gone up from 89 to 122.

Technically disclosed has been the IEEE 1858 standard published in 2016 for the image quality of smartphone cameras that is based on the measurement of the spatial frequency response, on color hue and color saturation, color homogeneity, local geometric distortions, texture fringing, and visible noise. However, the factors affecting these measurable characteristics of an image are complex: In addition to the camera‘s resolution, the optical system, image acquisition time, size of the sensor area, autofocus, image stabilizer and, increasingly, image post-processing integrated in image acquisition affect image quality as well.

3.3. Image Definition and Image Contrast

A frequently used measure for characterizing resolution capability is the modulation transfer function (MTF). Figure 2 schematically shows the information it contains. Plotted on the x-axis is the spatial frequency, that is the density of the lines of a test structure. Typically, the unit lp/mm is used for this purpose (lp = line pair: a pair consisting of a dark and a bright line). Plotted on the y-axis is the extent of the brightness contrast between the black areas of the lines and the bright areas between the lines. If the white balance is correct the lines, ideally, are depicted completely black and the spaces between them in pure white, which corresponds to a 100-percent modulation of the brightness value. If the density of the lines is raised the optical system becomes increasingly less capable of depicting the full contrast between the bright and the dark areas. The modulation transfer function describes this fluent transition. The ISO standard 12233 defines image resolution as the line density at which the modulation transfer function exhibits the value of 5 percent. Of interest for the design of security features is the fact that tangentially oriented lines, also referred to as meridional lines, are systematically more critical than radially oriented lines, so-called sagittal lines. Therefore, to achieve an optimal resolution, a security feature should be composed as concentric circles or at least as lines along imagined circular lines.

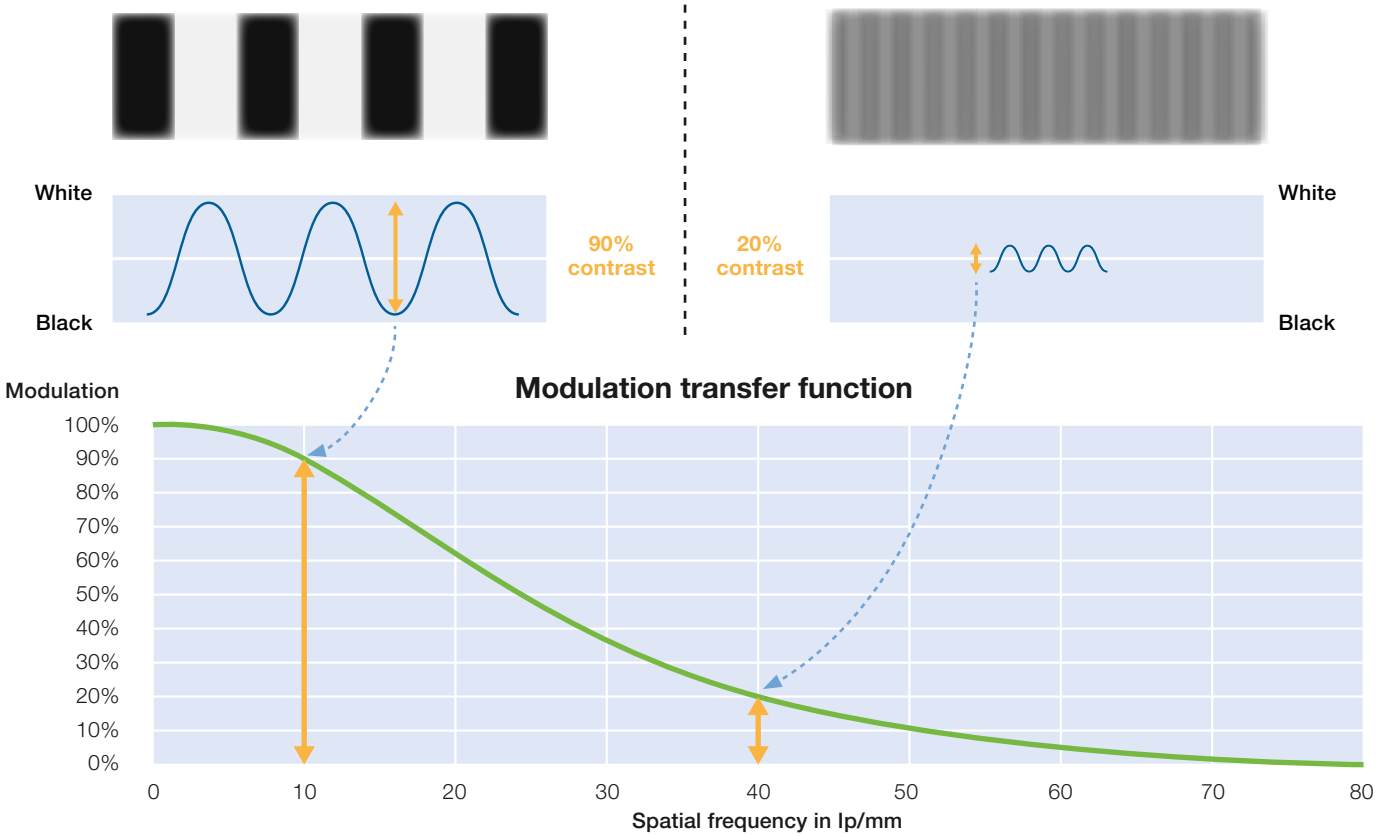

Figure 2: Functional principle of the modulation transfer function using examples with high and low modulation.

3.4. Image Distance and Zoom

The correlation between contrast modulation and line density (Figure 2) initially applies only to the distance with which the relevant picture was taken. When the distance between the camera lens and the object is reduced the image on the camera sensor enlarges proportionally—until the refractive power of the optical system is no longer able to sharply project the object in question on the camera sensor.

Typically, smartphone cameras are able to focus objects up to an image distance of around six centimeters. If the image distance is smaller there will usually be no shutter release. Figure 3 shows how image quality develops during the camera's approach to the object. The upper edge of the measured values depicted shows a clear limit of the maximum image quality that can be achieved for the image distance, which continuously increases for higher image resolutions. Downward there is no clear limit discernible which, for instance, is due to a less than perfectly adjusted focal distance by the autofocus system or focal blur caused by a freehand shot.

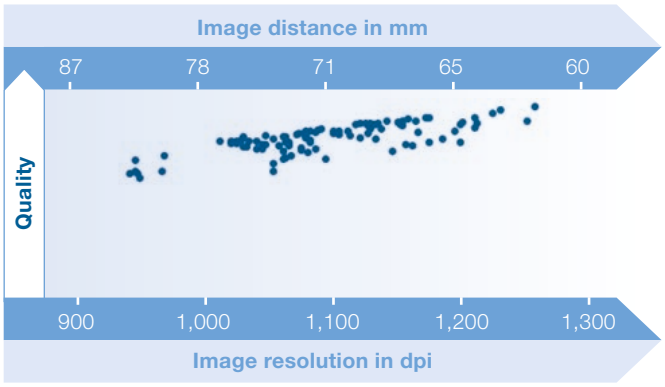

Figure 3: Dependency of image quality on distance between camera and object.

3.5. Image Acquisition Time

A frequent cause of impaired image quality is short image acquisition time. This correlation has been empirically investigated (Figure 4) and proves that these two characteristics compete with each other. Since moving objects are rarely tested, smartphone cameras with strengths in terms of image acquisition time are not helpful in the context of authenticating products because these models consistently entail a lower image quality. Hence high image quality cannot generally be assumed. The lower the requirements of the security feature in terms of image quality, the higher the share of suitable smartphone models.

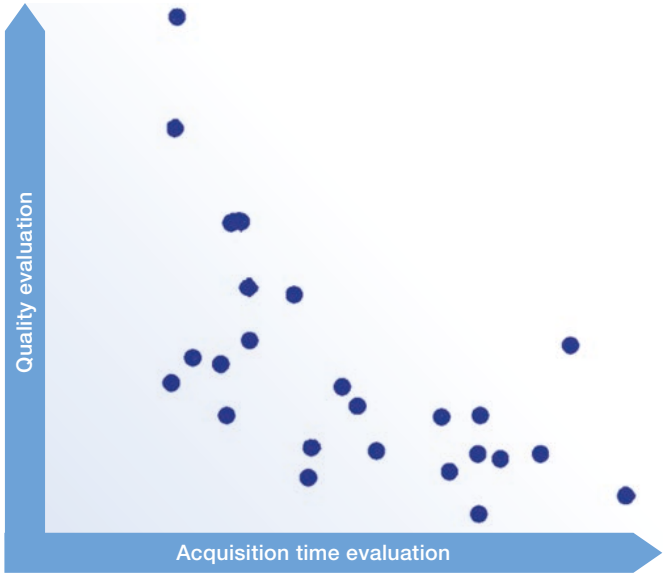

Figure 4: Quality and image acquisition time according to Veli-Tapani Peltoketo, Benchmarking of Mobile Phone Cameras, 2016.

3.6. Lighting Dependency

In the context of product authentication, no active light sources are investigated, but objects to be verified that are exposed to passive illumination. For one, this may be daylight shining, for instance, at a window facing north with indirect lighting by the sun (corresponds to CIE standard lighting D65). Its spectrum exhibits a maximum at around 450 nm and drops just slightly toward either side. For the other, there might be artificial lighting, provided by either a traditional incandescent lamp, where the share of red wavelength dominates, or by fluorescent tubes exhibiting a narrow, albeit very high peak in the red, green, and blue wavelength range, respectively. Accordingly, the actual appearance of images in terms of color varies significantly, depending on the lighting scenario. Of help in this respect is the fact that smartphones with flash LEDs have an integrated lighting unit. Compared to other possible lighting senarios, its emission spectrum is well-defined (Figure 5).

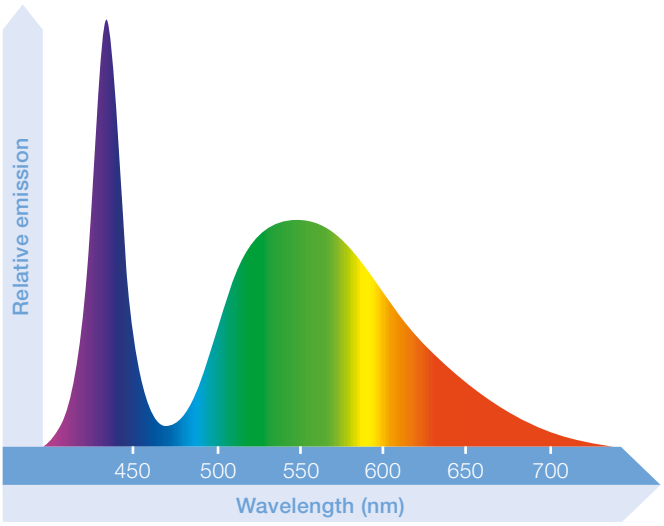

Figure 5: Emission spectrum of a typical flash LED integrated in a smartphone.

3.7. Color Fidelity

The reliable determination of a color depends on the reliability of the color sensitivity of the smartphone camera used. According to ISO standard 17321, the so-called sensitivity metamerism index (SMI) is a measure of how accurately a camera can reproduce colors. This index is defined as SMI = 100 – 5.5 ΔE and, according to the standard, the median color distance is to be determined by averaging the measurements across a complete color chart.

Figure 6 shows the results across a representative selection of smartphone models. All colors exhibit a color distance of approximately 10 to the chromaticity point actually displayed in the color chart. At ±4.6 the standard variation of the color distance across different smartphone models is among the smallest for the natural colors. The standard variation increases the further the color type moves away from the natural colors and with the achromatic grayscale ultimately

reaches the value of ±13.9. Therefore, to obtain a result that is as reliable as possible irrespective of the smartphone model, natural colors should be chosen when the chromaticity point is supposed to be used as a criterion for a security feature.

3.8. Internet Connection

Technically, specific security features are verifiable only with an internet connection and the same applies to feeding back the test result, for instance to the brand owner. There are three approaches:

- Online access is mandatory when an online connection is required for technical reasons, for instance to access a central database in which characteristics of security features etc. are stored that are necessary for authentication.
- Authentication of the security feature can be performed offline, either in the event that no additional information is required for the verification or that the data is stored on the object, for instance as a QR code (= self-authentication). Usability is not limited in the event that no internet connection is required. In that case, however, the brand owner will not receive any feedback about a large-scale incidence of counterfeits or the existence of hot spots. The user cannot access any additional relevant data, for instance about how to use the product.
- Verification as a hybrid solution: Offline authentication is permitted, but occasional feedback to a central server within a defined period of time is mandatory. Otherwise, the verification functionality will be deactivated. The benefits of online and offline use can be combined in this way.

Online access enables another version of authenticating a security feature: verification without an app. This circumvents the hurdle of having to install an app, which increases user willingness to adopt the technology. Depending on the application, user guidance can be designed for practicality even without an app. For instance, a printed QR code can be scanned with a—typically pre-installed—reader app. Subsequently, based on pictures on the related website, the user can perform a comparison with the image at hand consisting, for instance, of randomly arranged fibers.

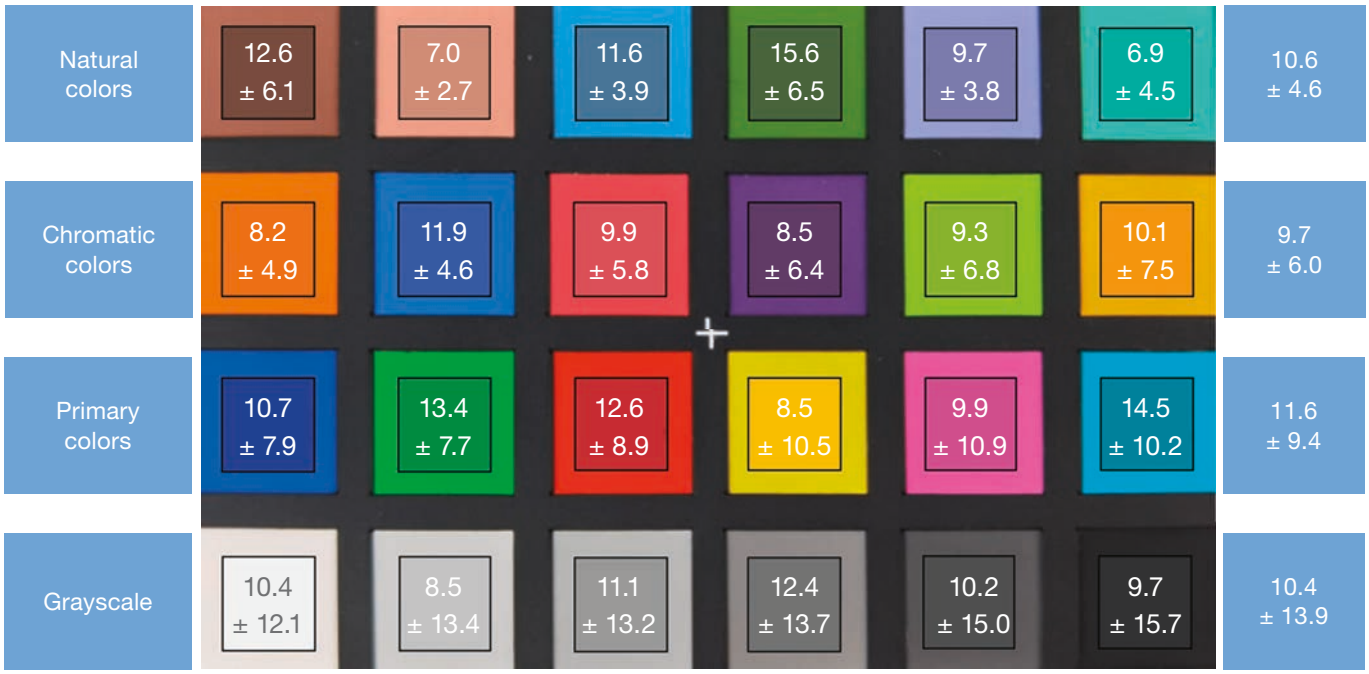

Figure 6: Color reproduction of the ColorChecker test chart from X-Rite for a representative selection of smartphones. The values represent the color distance ΔE between the color measured with a smartphone and the nominal chromaticity point of the test field. On the right-hand side, the median value for the colors of the color group shown in this line is indicated.

4. User Experience

How does a user benefit specifically from smartphone-based authentication? Security features that used to be checked with the naked eye can be verified in an automated process und evaluated by an app-integrated algorithm; in this case, the user no longer requires prior training. The evaluation is less prone to being affected by subjective influences and becomes clearly more reliable.

The verification process can additionally be supported by the app independently causing the picture to be shot. For one, this relieves the user of having to decide whether the image quality in its current form is adequate while ensuring that the authentication only takes as much time as necessary.

This applies particularly in view of the fact that for many security features two images have to be analyzed, because any image can be faked by a corresponding static image created by using conventional printing inks. Only in the case of a specific variation—depending on the security feature at hand—such as a different viewing angle or the time following the activation of the flash—will the security feature change characteristically and uniquely. Especially the automated selection of two or more images that are suitable for the analysis can be of major help for the person performing the authentication.

Some brand owners prefer not to let their customers know that their products are subjected to authentication because this might lead to concerns about their authenticity. In this case, the option of authentication in the background is available. In the case of overt security features, users always have to be informed about what has to be checked. In the case of semi-covert features, they have to be instructed about what testing tools can be used for identifying the security feature or may even have to be provided with a special testing tool. If the feature is a covert one it may have to be sent to a laboratory for verification. By contrast, in the case of security features that can be verified with smartphones, the authentication can take place even without the user being aware of it, for instance when a QR code is scanned or augmented reality is used and the product concerned is acquired by the smartphone‘s camera.

In addition to the practical benefits, the emotional effect on users should be considered: About four in five purchasing decisions are based not on slight appeal or rational agreement, but on strong enthusiam for and fascination with a product or service. An attractively designed app with additional gamification elements such as AR features, progress bars, crosshairs, or interactive displays can support this behavior decisively: it inspires users‘ curiosity and more than likely the authenticated product will have a positive connotation for them as well.

Schreiner ProSecure, a competence center of Schreiner Group
Schreiner Group GmbH & Co. KG · Bruckmannring 22 · 85764 Oberschleissheim · Germany · Phone +49 89 31584-5540
info@schreiner-prosecure.com · www.schreiner-prosecure.com