Innovations in Biometric Printing

Moataz Shazli Khalil, B.Eng. and Prof. Dr. Volker Jansen

Keywords: biometric, security, NIR visible ink, document security, encrypted data, imaging

Abstract

Current official identity documents such as passports and driving licenses rely on complex security features to prevent unauthorized alteration and replication of the documents. When a document is a suspect of forgery, the complex security features require time-consuming and resourceful verification.

The aim of the work is to develop a new concept to improve the efficiency and security of official documents by investigating and addressing the most common and effective types of forgery related to official documents and by addressing and finding solutions to current issues crippling the verification process done by the authorities.

The idea behind a new concept is using smartphone technology to make the verification and recognition of official documents quicker and easier. It is to utilize smartphones equipped with near-infrared setups along with the relevant encryption and decryption software, the usage of an appropriate workflow for variable data processing and the use of digital printing presses in combination with suitable printing inks that rely on infrared radiation for their functionality to address the issues.

The work discusses the approach of the concept and addresses its feasibility and the advantages it brings to current verification methods used. It examines the status quo of document verification and the building blocks of the concept, and addresses the requirements and the points that have to be addressed for the successful realization of the concept.

Hochschule der Medien

Introduction

According to Rolf Fauser (2021), Chairman of the European Network of Forensic Science Institutes, at the State Bureau of Investigations, Forensic Institute in Germany (Landeskriminalamt), a significant issue involving the detection and recognition of falsified documents is the lack of ability, time, and equipment at the scene to verify the documents on hand. This shortcoming is due to the complexity of the security features embedded into the documents. Such features include various types of invisible inks, guilloches of different patterns as well as engravings, and microchips. Such complex features require special equipment and sufficient training and know-how to detect any falsifying (Fauser 2021).

According to information provided by State Bureau of Investigations, Forensic Institute in Germany, criminals rely on mere similarities in the looks of the facial features to deceive law enforcement personnel into thinking that the criminal is someone they are not. Such impersonation can be done where the forger uses the identification document, for example, a passport of a person that looks similar to themselves.

Forgers use impersonation as a technique to deceive law enforcement, especially when the candidate for counterfeiting looks similar to another person whose passport or identity document was stolen or acquired by the counterfeiter. The State Bureau of Investigations asserts that impersonation is more effective in cross-border checks when law enforcement officers encounter individuals with facial features that are unusual to law enforcement officers.

Another approach is to forge part of the document. Fauser (2021) declares that

> '[…] due to the great complexity of existing security features, falsifying whole documents becomes be a significant challenge. Instead, forgers rely on substituting a layer that contains the name and the picture or, in some cases, just the picture. Such a forgery process is effective since only a few parts of the document are altered, which leaves a smaller room for error and a greater abundance of time for the forgers to focus on the smallest of details. The partial alteration usually leaves disruptions in the patterns, such as inconsistent reflections or a distortion of the fibers of the substrate, for example. Depending on the skill and the techniques used by the forger, the damage could be minimal, and the detection could need trained personnel and equipment'.

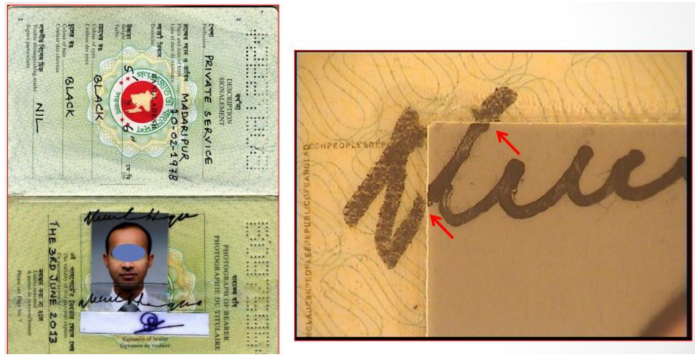

Fig. 1: *A forged passport (Esteves 2012)*

The figure above (Fig. 1) shows a passport that has been forged by replacing the original photograph with the photo of the person receiving the forged passport. Upon close inspection figure 1 shows that the texture of the writing on the photo looks different from the original writing on the passport.

.

According to Fauser (2021), "Interpol manages databases that contain information such as names and fingerprints related to crime and criminals as well as information about stolen property such as passports. The website also mentions that national police can access and search these databases for information […]". He refers to the Interpol databases and asserts that it is not always possible to compare the names and biometric data on official documents such as passports, as the Interpol databases only contain information on a specific group of people. Most of them are connected with crime. The databases are available online; therefore, referring to them for verification of information could not always be possible due to the instability or unavailability of the internet connection.

According to the Forensic Institute (2021) police officers are not equipped with specific equipment such as magnifying glasses, UV light or other helpful tools that would enable the verification of identification documents on the field. A suspect document will have to be submitted to specialists or laboratories specialized in verifying and detecting forgery. Rendering suspicions documents to specialists and laboratories is a time-consuming process (Fauser 2021). Instead, the idea of this work is to address the problem by relying on smartphones. According to the Forensic Institute the German police personnel have access to a police smartphone (2021). The police assert on their websites in Nordrhein-Westfalen: "Police officers have access to a police smartphone. The smartphone is often shared with other police officers. The police of Nordrhein-Westfalen as of March 2020 counted 22000 police smartphones and purchased additional 7000 smartphones, that shall by 2021 enable each police officer on active duty to have his or her own smartphone" (GdP 2020). In order to achieve the objective of the present analysis, the concept involves the usage of a specific smartphone software that captures guilloches or patterns printed on the document and superimposes them to form an image of the fingerprint of the

owner of the document. These patterns represent the characteristics of individual fingerprints; therefore, the guilloches can be encrypted and converted into secure data before being printed on the official document.

Materials and Methods

The work on which this paper is based was carried out in collaboration with Hewlett Packard, its research department in Israel and the Landeskriminalamt (Forensic Institute) in Germany, where HP provides the facilities and technology to carry out the tests and experiments necessary to assess the feasibility of the concept. At the same time, the Forensic Institute provide guidance on what issues and use-cases the concept must address to prove usefulness and feasibility.

The concept is based on the following methodology: Secure biometric data is scanned using the smartphone then a specially designed software compares the collected biometric data against those of the individual. The fingerprints of the individual are scanned using the same software on the smartphone. The software can utilize the built-in fingerprint sensor or the camera. The software compares the fingerprint captured on the document and compares it with the imagery captured by the fingerprint sensor to deliver a match or no-match. Very similar to how fingerprint-secured smartphones work. A multifunctional software will be required to capture the biometric data and decrypt it.

The encrypted image data of the fingerprint is divided into several segments, whose size is changed and manipulated with effects such as mirroring, rotating and scaling. The data is converted into printing elements that are applied to the document, covering person-specific data. These patterns are printed across the passport photo on the document to ensure that manipulation can be detected if the photo was replaced or manipulated. The superimposition of the pattern is required as Fauser (2021) states: “Forgers rely on replacing parts of the passport picture, such as the chin or the eyes. This technique is used since forgers try to minimize the amount of alteration they take on when falsifying a document. It is done to help the imposter avoid detection via altering the image of the original owner of the document to contain features of the imposter”. He claims that forgers aim for as little manipulation or intervention as possible to minimize anomalies, which lead to the detection of forgery.

Printing guilloches or encoded data using pigments that emit light in the visible spectrum over the document holder’s image is problematic because the printed elements (the guilloches or encoded data) can hide details and features of the printed image or personal data (date of birth, name, etc.). The printed elements must be visible to the smartphone camera during the scanning process. This requires a high contrast between the printed elements and their background. The need for high contrast between the printed elements and their background requires the use of inks

that contrast appropriately with the colors of the image. Inks that are transparent or highly translucent in the visible range but reflective or fluorescent in the infrared or ultraviolet range of the spectrum are suitable for the purpose because these inks have sufficient contrast when viewed with an IR or UV sensitive camera and do not obscure details of the document behind the elements printed with them.

As the approach aims to allow law enforcement personnel to rely solely on smartphones for screening, the use of such inks presents another challenge, as smartphones have limited ability to detect light that is below or outside the visible spectrum. Therefore, a careful examination of the capabilities of modern smartphones could reveal features that could be used to realize such a use case.

The printing process is carried out using variable data printing technology as available on the HP Indigo and the corresponding software. When the individualized document is checked for authenticity, a smartphone carrying specially programmed software scans the document and recognizes the printed guilloches or the encrypted data. The software then restitches the scanned pieces of the printed guilloches or encrypted data together by reversing the manipulation done to the single pieces. The pieces are then fit together to provide the data and the shape of the fingerprint, which is then used for verification with the fingerprint scanned from the carrier of the document. When the software fits the pieces together to form the guilloche or the encrypted data, then the first level of verification is successful, and the software moves to the second step of verifying that the printed fingerprint is matching to the scanned fingerprint of the individual. If that is also successful, an identity match is confirmed.

Figure 2 to 4 demonstrate the advantages of the concept as it offers the possibility to maintain simplicity by relying on the abstract patterns of the fingerprint, which are used as a secure and verifiable security feature that is hidden in plain sight i.e. the green dots are not viable to the human eye. In addition, various features can be included in the print of the patterns to enhance security. To achieve the goal, the fingerprint data is printed in several places on the document in different orientations and transformed by resizing and mirroring.

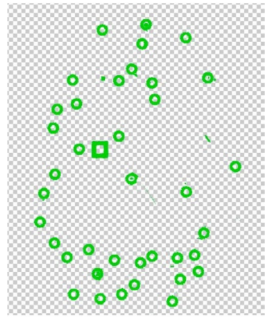

Fig. 2: *Random fingerprint data*

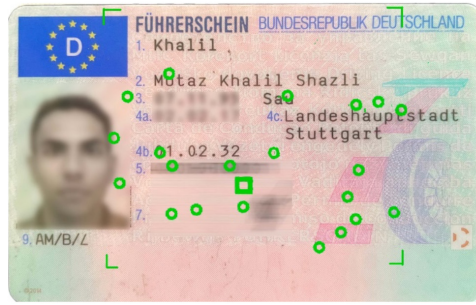

Fig. 3: *German driving license (Front)*

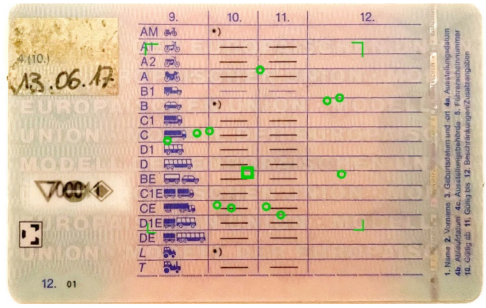

Fig. 4: *German driving license (Back)*

In figure 2 the elements in green resemble data extracted from a fingerprint. The data is first split into two parts, moved, and then rotated and finally mirrored. The elements are then printed on the front and the back as shown in figure 3 and 4. This means the data is converted into printing elements that are applied to the document, covering person-specific data. During the scanning process, the software on the smartphone is programmed to realign and transform the printed patterns in a way that reproduces the original fingerprint data. The work investigates specific patterns, which, when run through an algorithm, provides specific features to the result. For instance, the algorithm encrypts fingerprint patterns and makes visual recognition or detection of the original fingerprint impossible. Converting the data back into an image requires a decrypting software.

The codes or patterns are printed across the photograph and name on the document to ensure that manipulation can be detected if the photograph was replaced or manipulated. The need for high contrast between the printed elements and the background would make the use of inks necessary that offer an appropriate contrast to the colors of the image and cannot be seen by the human eye on identification elements. All the same, the printed elements must to be visible to the smartphone's camera during the scanning process. Inks are required that are transparent or highly translucent in the visible spectrum but reflective or fluorescent in the infrared or the ultraviolet range of the spectrum which can be viewed using an IR or UV sensitive camera and will not hide details of the document. The approach aims to allow the law enforcement personnel to solely rely on smartphones for the verification process.

Results and Discussion

Several different processes can be used to identify and match fingerprints. For example, "Correlation-based matching" relies on the correlation between pixels when images of two fingerprints are superimposed for comparison. Or "Non-minutiae feature-based matching," this method is usually used in the case of the unavailability of high-quality images of the fingerprints (Maltoni et al. 2016, 42–43).

"Minutiae-based matching" is the most common method for fingerprint matching (Maltoni et al. 2016, 177). This is due to its strict analogy with how fingerprints are compared by forensic experts and its wide acceptance in courts in most countries. It relies on the recognition and comparison of fingerprints by describing each minutiae by a number of attributes such as its location on the fingerprint's image, its orientation as well as its type. Minutiae-based matching process relies on the recognition and comparison of fingerprints by describing each minutia by a number of attributes such as its location on the fingerprint's image, its orientation as well its type. The most commonly used minutiae matching algorithms refer to each minutia with a set of data. mi = {xi,yi,_θi} Where x and y indicate the coordinates of the minutia on a 2-dimensional axis and θ _indicating the orientation of the minutia. (Jampour et al. 2010, 294). Further testing would be required to assess the efficiency and reliability of different methods when taken in the context of printing. To establish the concept using fingerprints encrypted for Minutiae-based matching imposes some challenges. The police will need a smartphone equipped with facial recognition systems. It requires an App with a reading, decrypting and matching software. And finally, it requires a hygiene routine to avoid the risk of bacterial or viral transmission through direct contact with the fingerprint sensors.

Smartphone cameras utilize complementary metal oxide semiconductor sensors or CMOS for short. Cameras utilizing these CMOS sensors are fitted with IR blocking filters. According to various IR cut-filter manufacturers more than 90% percent of the IR spectrum is blocked by the filter. However, a residue of IR radiation still passes through the filter. Although the IR radiation transmitted through the filter is relatively small, it can be used to detect IR radiation. Smartphones we tested in their capacity to detect IR radiation emitted from an infrared diode.

The imaging of the IR radiation became more apparent when placing an R72 filter in front of the lens. Such a capability of smartphones could be combined with the use of IR ink to allow the detection of the printed pattern by using a device capable of detecting IR radiation.

It is projected that all smartphones will be equipped with Biometric facial recognition set up by the year 2024. This biometric facial recognition process requires an IR set up on the screen side of smartphones. These built-in IR setups are available from Apple and Android manufactures. Leading smartphone manufacturers such

as Google and Huawei have implemented facial recognition utilizing a setup containing an IR sensor and an IR flood illuminator in some smartphones.

Invisible security inks such as IR inks that rely on their translucence in the visible spectrum between 420 and 780 nm are suitable for the use. Hence, the pigment used in the printing inks must comply with the capabilities of the setup. The requirements are due to the flood illuminator and the sensor, which work in the near-infrared spectrum (NIR) of $\lambda = 940$nm, as well as the dot projector, which works at 850nm. Therefore, suitable inks, which reflect electromagnetic radiation in the range of $\lambda = 850\text{-}940$nm and are transparent or highly translucent to the visible range of the electromagnetic spectrum, have to be made available.

The concept relies on the unique capabilities of three key components that are currently a part of the facial recognition systems—namely, the infrared sensor, the flood illuminator, and the dot projector. Depending on the ink used, one, two, or all of the components could be used simultaneously to enhance the performance. Each of the components offers individual capabilities that could potentially play a role in the verification process. How each individual component would contribute to the concept is explained in the following sections.

The flood illuminator creates a flat-top infrared illumination pattern for applications in structured light, stereo vision or time-of-flight sensors, and video light enhancement applications. The devices are optimized to deliver best-in-class performance in 3D sensing applications on a variety of platforms such as mobile, IoT, and robotics. This feature will be applicable for the reading of IR ink encrypted bio data.

The dot projector is designed to project a matrix of dots on the face of the user during the verification and unlocking of the smartphone. This process is first done during the initialization phase when using facial recognition for the first time. The dot matrix is projected on the face. The NIR sensor analyses the reflected NIR light and produces a distance map of the face.

In the application of this project, we will be relying purely on capturing the details of a fingerprint utilizing the features offered on smartphones sporting facial recognition capabilities. This is particularly useful since verification using facial recognition technology primarily relies on a built-in IR sensor and an IR flooding device setup, which could then be used in the scanning of the printed fingerprint.

In the case of the iPhone, the dot projector emits near infrared radiation or NIR in short with a wavelength of 850nm projecting 30,000 dots (see figure 6). The dot projector utilizes four significant components to produce the dot projection. These components include the ceramic electronic chip package, a two wafer-level lenses

optic, and a diffractive optical element. The most relevant element for the concept is the Vertical Cavity Surface Emitting Laser diode or VCSEL in short.

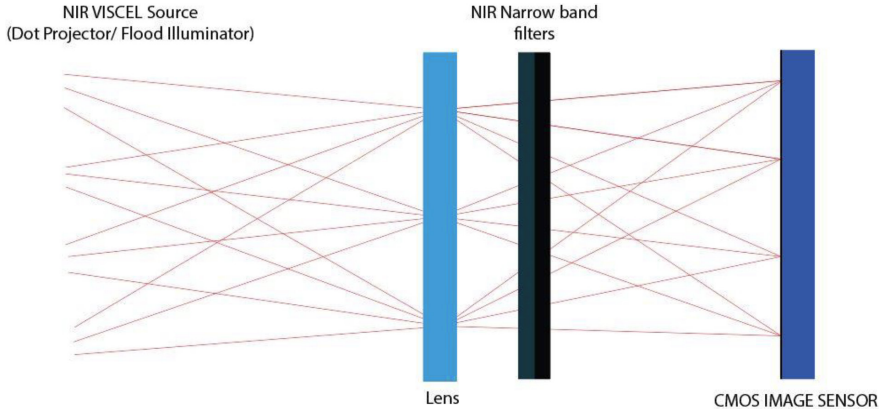

Fig. 5: *Components of the NIR sensor based on (Bae et al. 2021, 2)*

Unlike the flood illuminator, the dot projector relies on a high-powered VCSEL diode to emit the NIR dot projection (Future Think Tank 2020). The high-power output of the diode included in the NIR dot projector could be particularly useful. This is due to a possible lack of output power when relying solely on the flood illuminator (LDP LLC 2021).

Fig. 6: *Projected dots during the unlocking of an iPhone (ardo111 2017)*

The capturing process of the fingerprints must be a quick and accurate process that also guarantees a high-quality image of the fingerprint. The captured image must retain all the small details of the captured fingerprint so that a comparison with the printed biometric data is reliable and quick.

For reading the fingerprint correctly a specific recognition software is required. The software must recognize and extract the relevant biometric data sets required for the verification process. It must be programmed to automatically focus and take continuous pictures of the fingers. This would be required for high density resolution

(HDR for short) and to simultaneously focus on the different fingers and take sharp in-focus pictures of them. The software should be able to apply the appropriate post-processing algorithm to enhance the details and increase the contrast between the valleys and elevations in the captured images. This is necessary for efficient and successful recognition and extraction of biometric data sets.

The software must be programmed to recognize and extract the relevant biometric data sets required for the verification process and should be able to decrypt the encryption applied when the biometric data sets are printed. It has to have the capability to apply the verification process comparing the data biometric data sets collected from the fingerprints as well as the decrypted biometrics collected from the document.

Devices used to scan fingerprints in the offices of the German government have to meet the standards of the "Bundesamt für Sicherheit in der Informationstechnik" or BSI for short. All devices have to be certified by the BSI. According to a report issued by the BSI, "Fingerprint scanning devices have to meet strict criteria to be applicable for certification and the use in passport authorities. The devices have to meet the image quality of at least level 31 of the [ISO_FINGER] which defines the Image Acquisition Requirements of the devices (Bundesamt für Sicherheit in der Informationstechnik 2010: 7). Level 31 corresponds to a scan resolution of at least 500 pixels per inch. The report also mentioned that the passport authorities use optical sensors exclusively these sensors are also referred to as live scanners (Bundesamt für Sicherheit in der Informationstechnik 2010: 8). Depending on the data relevant for the printing and verification, existing optical sensors currently in use in government offices and passport authorities are required to provide sufficient data for the fingerprint recognition and matching process.

Additional features could also be added to the software, for example, the ability to refer to the corresponding databases of the authorities. This could, for example, help with verification as an extra layer of security or as a standalone verification method in the case of the absence of a document. The app's design should have a verification button that starts the verification process on demand. The verification process has to go through various steps. First, switches on the back camera then the smartphone is pointed at the four fingers of a given suspect. The software then extracts the distinct features of the fingerprint. The extracted features are then stored temporarily for comparison in the next step. Second, the software switches to the appropriate front camera and controls the appropriate IR transmitters. The identification document has then to be held in front of the camera for scanning. The app scans the printed biometrics and shows a confirmation message. Third, the software starts comparing the data extracted from the first and second steps of the procedure. The matching of fingerprints can be done in various ways depending on which fingerprinting matching process is used in the final design of the concept.

The software either shows confirmation that both sets of data are matching or shows a mismatch indicating possible forgery.

For scanning and printing biometric data a suitable infrared absorbing pigment is supplied by Llewellyn Data Processing. The pigment works to the concept of IR absorbing inks. Where the ink is translucent under visible light but absorbs NIR light appearing black to an IR sensor. The supplier has provided information about the suitability of the pigment for VDP (Llewellyn Data Processing 2022b).

The standard camera of the smartphone can read and process the visible fluorescence. Such a fluorescence process is referred to as ”up-conversion,” where the phosphor particles convert infrared light into visible light with higher energy and shorter wavelengths (Llewellyn Data Processing 2022b). IR inks which get stimulated when subjected to IR light and emit IR in lower energy with longer wavelengths is called „down-conversion ink“

The “down conversion” process is inherently more efficient than “up-conversion” since it radiates lower energy radiation than what it originally absorbs.
The use of if the ink requires the following properties:

- Ink pigments are stimulated using a near-infrared light in the spectral range of the NIR light emitted from the flood illuminator and the dot projector.
- Ink pigments reemit NIR light in the spectral range detectable by the sensor on smartphones.
- The pigments must be suitable for printing.

The variable data printing can be done via a digital printing press potentially using liquid toner-based ink systems featuring IR ink pigments.

Since the concept relies on individualized security features utilizing biometric data, a digital printing press capable of printing individualized data, also referred to as Variable Data Printing or VDP for short, is required.

The HP Indigo is a digital printing press capable of variable data printing where each print can be used to personalize products. This is done through the utilization of HP’s liquid electrophotography technology, where a heated blanket is used to transfer the ink to the substrate. Digital printing process resembles some of the basis of electrophotography. The process relies on the following stages:

a. The electrophotographic imaging plate is charged in an even manner spanning the whole of the plate
b. The area of the plate where the to be printed image is then discharged using an array of lasers

c. The ink of a single color is then applied to the plate from an inking unit referred to as Binary Ink Developer (BID)
d. The image is transferred to the heated blanket from the plate with the help of an electric field
e. The resin particles in the ink melt due to the higher temperature of the blanket. This forms an even and tacky film of ink
f. The ink is then transferred to the substrate, where it solidifies due to the colder temperature in relation to the heated blanket. This transfer of ink is either done in a one-shot process where all the different color separations are first collected on the blanket then transferred in one go to the substrate. Or in a multi-shot process where each ink separation is transferred separately, one after the other, to the substrate

The individualization and the application of variable data printing rely on specialized software that manages and integrates the variable data into the base documents (Medeiros 2022). Several VDP software could be used to handle the data in the steps prior to printing. HP has its own programmed software that is essentially able to handle and prepare data in the context of security printing. The software is referred to as SmartStream Designer and SmartStream Composer. The software is mainly used in the advertising field due to its ability to customize any printing job with various sorts of data such as designs and images. In addition to that, it has the capability to integrate with other specialized software (HP 2018: 2). Security specialists such as Jura, AGFA, and Haiyaa offer various software that is specialized in creating security features that rely on personalization and variable data (HP Press Center 2021). Using such software allows the inclusion of secure data in a covert manner where the secure data is not standing out from the rest of the fixed data and features contained in the document, thus further improving the level of security and design of the final print. Such software also has the capability to seamlessly integrate personalized secure (variable) data into the original design of the print (JURA 2022).

Conclusion

The results of this study combine the use of near-infrared devices on smartphones, which are mainly used for facial recognition and augmented reality applications, with digital photography and variable data printing to create a technology that offers several advantages over other current verification methods. It will enable law enforcement personnel to verify documents with no additional equipment beyond a smartphone.

Furthermore, the concept of relying on smartphone components and using invisible inks could be an innovative approach to combining smartphones and security printing in a unique way. The concept could then be used in further use cases that go beyond the verification of identity documents. Relevant authorities, such as the

police, should strive to make identity verification methods more efficient, accurate and digital in order to reduce crime and harm caused by identity theft and forgery.

References

AMS 2022. "PMSILPlus - Flood Illuminator | Ams." 2022. https://ams.com/en/pmsilplus#tab/description.

Apple 2017. "The Future Is Here: IPhone X - Apple." 2017. https://www.apple.com/newsroom/2017/09/the-future-is-here-iphone-x/.

——. 2021. "IPhone X - Technical Specifications." 2021. https://support.apple.com/kb/sp770?locale=en_US.

——. 2022a. "About Face ID Advanced Technology - Apple Support." 2022. https://support.apple.com/en-us/HT208108.

——. 2022b. "Augmented Reality Resources - Apple Developer." 2022. https://developer.apple.com/augmented-reality/resources/.

——. 2022c. "IPhone and IPad Models That Support Face ID - Apple Support." 2022. https://support.apple.com/en-us/HT209183.

——. 2022d. "Use Memoji in Messages on IPhone - Apple Support." 2022. https://support.apple.com/guide/iphone/use-memoji-iph37b0bfe7b/ios.

ardo111 2017. "PHOTO: Face ID Infrared Dot Matrix | Page 3 | MacRumors Forums." 2017. https://forums.macrumors.com/threads/photo-face-id-infrared-dot-matrix.2084242/page-3?post=25466257#post-25466257.

Bae, S et al 2021 "Machine-Learned Light-Field Camera That Reads Facial Expression from High-Contrast and Illumination Invariant 3D Facial Images." Advanced Intelligent Systems, 2100182. https://doi.org/10.1002/aisy.202100182.

Bundesamt für Sicherheit in der Informationstechnik. 2010 "Technische Richtlinie Zur Produktionsdatenerfassung,-Qualitätsprüfung Und-Übermittlung Für Pässe Qualitätsanforderungen Bei Der Erfassung Und Übertragung Der Fingerabdrücke Als Biometrische Merkmale Für Elektronische Pässe BSI TR-03104 Annex 2 (QS-Finger) Version 2.1.5." https://www.bsi.bund.de.

Caldwell, S 2017 "TrueDepth vs. Back Camera: Which IPhone X Portrait Mode Is Better? | IMore." 2017. https://www.imore.com/truedepth-vs-portrait-which-iphone-x-portrait-mode-better.

Cambou, P 2017 “The Reality of the IPhone X’s 3D-Sensing Dot Projector - i-Micronews.” https://www.i-micronews.com/the-reality-of-the-iphone-x-s-3d-sensing-dot-projector/.

Campbell, M 2017 “Inner Workings of Apple’s ‘Face ID’ Camera for ‘IPhone 8’ Detailed in Report | AppleInsider.” 2017. https://appleinsider.com/articles/17/09/09/inner-workings-of-apples-face-id-camera-detailed-in-report.

Clover, J 2017 “Apple’s New Face ID Biometric System Works in the Dark and When Your Face Is Obscured by Hats and Beards - MacRumors.” 2017. https://www.macrumors.com/2017/09/13/how-iphone-x-face-id-works/.

CONSULTING-SYSTEMPlus 2021 “Apple IPhone Evolution Apple ’ s Camera Design Choices from the IPhone 6S Plus to the 12.” Vol. 2.

Edmundoptics 2022 “Imaging Electronics 101: Understanding Camera Sensors for Machine Vision Applications.” 2022. https://www.edmundoptics.eu/knowledge-center/application-notes/imaging/understanding-camera-sensors-for-machine-vision-applications/.

Esteves, H 2012 “Introduction to Fraudulent Methods Used in Travel, Identity and Visa Documents.”

Evaporated Metal Films (EMF) 2022 “IR Reflecting FILTER.” 2022. https://www.emf-corp.com/product-category/optical-coatings/hot-mirror/.

Future Think Tank 2020 “TOF IS EXPECTED TO BECOME A MAINSTREAM SOLUTION FOR 3D SENSING - REPORT INTENSIVE READING - FUTURE THINK TANK.” https://www.vzkoo.com/read/50bffeddc483145d14728d3750d3d614.html.

GdP 2020 “Ab 2021 Bekommt Jeder Polizist Ein Eigenes Smartphone! - Gewerkschaft Der Polizei.” https://www.gdp.de/gdp/gdpnrw.nsf/id/DE_Ab-2021-bekommt-jeder-Polizist-ein-eigenes-Smartphone-?open&ccm=200013.

Grey T 2022 “HDR Photography: A Beginner’s Guide - Nature TTL.” 2022. https://www.naturettl.com/a-beginners-guide-to-hdr-photography/.

Hoya 2022 Hoyafilter, https://hoyafilter.com/product/r72_infrared/.

HP 2018 “Impact through Design HP SMARTSTREAM DESIGNER.” 2018. https://www8.hp.com/h20195/v2/GetPDF.aspx/4AA7-4013ENW.pdf.

HP Press Center 2021. “HP Launches Secure Printing for HP Indigo Digital Presses.” 2021. https://press.hp.com/us/en/press-releases/2021/hp-launches-secure-printing-for-hp-indigo-digital-presses-.html.

Ink World Magazine 2018 “Nosco Launches Covert Security Solution Utilizing HP Indigo Invisible Inks - Covering the Printing Inks, Coatings and Allied Industries - Ink World.” 2018. https://www.inkworldmagazine.com/contents/view_breaking-news/2018-11-02/nosco-launches-covert-security-solution-utilizing-hp-indigo-invisible-inks/.

Jampour, M, Mahdi Y, Maryam A and Adel S 2010 “A New Fast Technique for Fingerprint Identification with Fractal and Chaos Game Theory.” Fractals 18 (3): 293–300. https://doi.org/10.1142/S0218348X10005020.

JURA 2022 “Security Design Software & Modules - Jura.” 2022. https://jura.hu/security-design-software-modules/.

Khodadoust, J, and Khodadoust AM 2017 “Fingerprint Indexing Based on Minutiae Pairs and Convex Core Point.” Pattern Recognition 67 (July): 110–26. https://doi.org/10.1016/J.PATCOG.2017.01.022.

LDP LLC 2021 “IR Up-Conversion.” 2021. https://maxmax.com/phosphorsdyesandinks/infrared-phosphors-dyes-and-inks/infrared-up-conversion-powder.

Llewellyn Data Processing 2022a. “IR Absorbing Ink.” 2022. https://maxmax.com/phosphorsdyesandinks/infrared-phosphors-dyes-and-inks/infrared-down-conversion-powder/ir-ink-down-conversion.

——2022b “IR Up-Conversion.” 2022. https://maxmax.com/phosphorsdyesandinks/infrared-phosphors-dyes-and-inks/infrared-up-conversion-powder.

Maltoni, D, Dario M, Anil K J, and Salil P 2016. Handbook of Fingerprint Recognition.

Maynard, N 2021 “Mobile Payment Authentication Market Report.” April 12, 2021. https://www.juniperresearch.com/researchstore/fintech-payments/mobile-payment-authentication-market-research.

Medeiros, R 2022 “6.7 Variable Data Printing – Graphic Design and Print Production Fundamentals.” 2022. https://opentextbc.ca/graphicdesign/chapter/6-7-variable-data-printing/.

Moldovan, A 2012 “Implementing a Data Management Structure to a Computer Assisted Restoration Platform,” 132. https://www.researchgate.net/publication/265425647_Implementing_a_data_management_structure_to_a_computer_assisted_restoration_platform.

Newport 2012 “Infrared Short Pass Filters.” www.newport.com/contact.

Pascu,l2020.“BiometricFacialRecognitionHardwarePresentin90%ofSmartphones by 2024 | Biometric Update.” January 7, 2020. https://www.biometricupdate.com/202001/biometric-facial-recognition-hardware-present-in-90-of-smartphones-by-2024.

Radiant-Vision-Systems 2019. “Near-Infrared (NIR) Light Sources for 3D Facial Recognition.” 2019. https://www.azooptics.com/Article.aspx?ArticleID=1666.

Rhino 2022.“Smartphone Variable ND Filter | Rhino Camera Gear.” 2022. https://rhinocameragear.com/products/smartphone-variable-nd-filter.

Mukul, S and Theuwissen A 2013 A Biologically Inspired CMOS Image Sensor. Studies in Computational Intelligence. Vol. 461. https://doi.org/10.1007/978-3-642-34901-0.

Sawers, P 2018. “Huawei Mate 20 Pro Review: The Notch Giveth, and the Notch Taketh Away | VentureBeat.” November 9, 2018. https://venturebeat.com/2018/11/09/huawei-mate-20-pro-review-the-notch-giveth-and-the-notch-taketh-away/.

Sohail, O 2018 “Huawei Mate 20 Alleged Render Shows off a Borderless Design With Front Camera to Get a 3D Facial Recognition System.” 2018. https://wccftech.com/huawei-mate-20-borderless-design-3d-facial-recognition/.

Standard Colors 2021 “IRT Colors for Security Printing.” 2021. http://standardcolors.com/index.php/infrared-transparent-colors/irt-colors-for-security-printing.

TEL. 2022 “What Is a CMOS Image Sensor? | The Principle of Semiconductor | Nanotec Museum.” 2022. https://www.tel.com/museum/exhibition/principle/cmos.html.

Warner, RD, and Adams RM 2016. “Introduction to Security Printing.”

Zafar, R 2019. “Pixel 4 and Pixel 4 XL Will Feature A Radar Chip To Detect Motion.” 2019. https://wccftech.com/pixel-4-xl-radar-chip-confirmed/.