Digital fingerprint

captain Maciej Fabiszak[1]
ORCID 0009-0009-6647-4827

Forensic Laboratory of the Voivodeship Police Headquarters in Szczecin, maciej.fabiszak@sc.policja.gov.pl

Abstract

Based on the example of activities performed in the Forensic Laboratory of the Police Headquarters in Szczecin in the case of the Central Police Investigation Bureau, the article presents the issue related to the possibility of obtaining investigation material for fingerprint examination in the form of graphic files and video files secured from smartphones with images of fingers and hands. Due to the high quality of a photograph and a single frame from a video, it was possible to positively identify the person, which made it possible to largely substantiate the person's involvement in the criminal act. The widespread access to smartphones that enable taking and sharing high-quality graphic files, as well as a huge number of photographs and videos shared on the Internet, with increasing frequency, in combination with simple tools for processing video frames and unsophisticated procedures for rescaling traces in AFIS, make a new form of obtaining material for fingerprint identification in the form of a digital fingerprint, and may become more significant.

Keywords: digital fingerprint, fingerprint identification, AFIS

Introduction

There is no doubt that on the one hand the technological progress that has been observed over the last three decades, brings new opportunities and solutions for forensics in the fight against crime, but on the other hand, it poses new challenges to forensics related to innovative forms and methods of criminal activity. Indeed, the biggest changes have occurred due to the development of computer, digital and mobile technologies. The development of the information society, based on almost unlimited access to the Internet and mobile devices, means that the reality in which modern forensics operates is not only materialized objects, but cyberspace with digital, intangible data that is an information carrier.

The report "*10 years of the mobile revolution*" prepared by Kantar Public for Digital Care shows that over the last 10 years in Poland the percentage of people owning smartphones has increased from 5.4% to 76%. Smartphones have taken over the function of personal computers. In 2022, 83% of Poles used the Internet, and 69.3% of respondents declared daily use of the Internet[1].

In a reality marked by the digital revolution, modern fingerprinting operates very efficiently, creating solutions based on modern achievements of science and technology. Undoubtedly, the greatest achievement is the Automatic Fingerprint Identification System (AFIS) with digital images of fingerprints, which are collected and processed in order to detect the perpetrator of a crime or determine the identity of a person.

The starting point in collecting study material for fingerprint examinations are traditional investigative examinations. During procedural activities, fingerprints and items for laboratory tests are revealed and secured. The most frequently used method of recording fingerprint traces discovered at the scene of the incident is to transfer them to fingerprint foil. Macro photography recorded on a digital medium is also used more often. However, fingerprint traces revealed on objects during laboratory tests are recorded photographically and secured in the form of graphic files on digital media and in the form of paper printouts. In the traditional approach described above,

1 Poles and their smartphones – a study conducted in 2022 by Kantar Public for Digital Care.

a fingerprint is a material, substantive trace that was created as a result of the contact of a finger or hand with the surface, as a result of the transfer of a trace-forming substance (usually sweat and fat) from the skin ridges to the touched surface. Such a trace reproduces the arrangement of fingerprints on the surface of the object on the fingers and hands, which is physically revealed and secured. As already mentioned, one of the methods of securing the revealed fingerprint trace is taking a digital photograph. In this case, the image of the original fingerprint is saved as a graphic file. However, it is possible that the image of a finger or hand with fingerprints in the form of a graphic file or video file will be the original trace, and not a way of recording and securing it. These may be photographs and video files saved on computers, smartphones or shared on the Internet, containing images of fingers and hands with fingerprints. Due to the degree of organization of matter, these will be intangible, digital traces, made of bits, not atoms, revealed in the memory of a digital medium or in cyberspace, containing image information in digital form, in the form of a moving or still image, showing fingers and/or hands with fingerprints.

Please note that forensic research on digital data media, relating to the analysis of visual records and objects recorded in the visual image, is focused, among others, on: identifying objects and places, determining their dimensions, determining the course of the recorded event, taking into account the relationships between objects, and extracting single images from recordings. The aforementioned studies do not include external features of the human body structure[2].

This publication presents the issue of using information from graphic files and video files secured from smartphones for fingerprint investigations.

Literature review

In 2014, the Police Forensic Laboratory in Madrid (Spain) received ten photographs showing hands containing stolen items from archaeological excavations. The photographs came from an online store where there was a sales offer for these items. After graphic processing, seven fingers that were positively searched in AFIS and identified with the suspect were qualified for testing (San Miguel et al., 2021).

In 2015, the Police Department in Sarasota, Florida (USA) arrested Danni Horner for trading child pornography on the Internet. Photos showing the genitals of a one-year-old child touched by an adult's hand were discovered on the perpetrator's secured mobile phone. The perpetrator's face was not visible in the secured photographs. The high quality of the photograph made it possible to extract a finger from the photograph with a visible fingerprint pattern. This allowed for positive fingerprint identification and the perpetrator's accusation not only of trading child pornography, but also of crimes related to contact with a minor[3].

In Phoenix (USA), a mother and her daughter were detained on suspicion of ordering the murder of a man. One of the contractors was identified in AFIS based on a photograph from the mother's phone, which was taken in the suspect's car and showed an image of a finger with a gun. The weapon was not used to commit the crime, but identifying the person allowed establishing the circumstances of the incident and arresting the second perpetrator. Both men pleaded guilty to the alleged crimes (Loll, 2022).

In 2021, the Police Crime Laboratory in Alicante (Spain) received a video showing the sexual abuse of a five-year-old child, in which the fingers of the perpetrator's hand were visible. The owner of the phone denied his involvement in the video. A two-second fragment of the film with the image of the perpetrator's fingers was extracted into single frames, one frame with the clearest image of the fingerprints on the fingers was selected and comparative tests were carried out with the fingerprints of the phone owner. The two fingers visible in the recording belonged to the owner of the phone (Boronat-Far V. et al., 2022).

Description of the case carried out at the Forensic Laboratory of the Provincial Police Headquarters in Szczecin. During the activities, police officers found firearms without the required permit in the stopped vehicle. During the proceedings, the apartment and garage of the person who was the driver of the vehicle were searched. As a result of the search of the garage, dried plants and tablets were seized which were placed in foil packaging (photograph 1). As a result of the ordered laboratory tests as part of the opinion on physicochemical tests, it was established, among others, that the secured tablets are ecstasy tablets containing MDMA (3,4-methylenedioxymethamphetamine) – a legally controlled psychoactive substance, the possession of which is prohibited.

2 Methodology for examining digital data media, ed. I of 4 November 2019, Central Forensic Laboratory of the Police in Warsaw.

3 https://eu.heraldtribune.com/story/news/2015/06/21/in-sarasota-child-porn-case-a-fingerprinting-first/29320365007/ (dostęp 24.02.2023).

During fingerprint examination on the original packaging of the secured substances, one fingerprint trace was revealed, which was not consistent with the fingerprints of the vehicle's driver. The person refused to testify and did not explain the circumstances related to the possession of dried plants and ecstasy tablets found in the garage. On the day the person was detained, an iPhone SE A 1723 smartphone (first generation) was seized. A photograph and a two-second video were revealed on the phone, showing a foil package containing tablets of the same appearance (shape, colour) as those seized during the search of the garage. In addition to the foil packaging, fingers with fingerprints were visible in the photograph and video. The person conducting the proceedings secured the photograph file and the video file and sent it for fingerprint examination to determine the origin and assess the suitability for finger identification and to conduct possible comparative tests.

Photograph 1. A bag with ecstasy pills, secured during the inspection of the garage

Investigation material

Photograph

The submitted photograph was a graphic file in JPG format. EXIF data for the photograph is shown in the photograph 2 and photograph 3.

It was found that the photograph showed a finger (the pad with two parts) and a fragment of the lateral part of the finger pad (photograph 4). Clear and legible fingerprints were visible on the finger and part of the fingertip, the number of specific features and arrangement of which were sufficient for identification. The finger of the hand was identified with the index finger of the right hand of the detained person (the driver of the vehicle). In the case of the fragment of the lateral part of the fingertip, it was not possible to issue a categorical positive or negative opinion due to the fact that standard fingerprints on the fingerprint card did not fully reveal the lateral parts of the fingertips.

Property	Value
Copyright	
Image	
Image ID	
Dimensions	4032 x 3024
Width	4032 pixels
Height	3024 pixels
Horizontal resolution	72 dpi
Vertical resolution	72 dpi
Bit depth	24
Compression	
Resolution unit	2
Color representation	sRGB
Compressed bits/pixel	

Photograph 2. EXIF data of the uploaded photograph

Property	Value
Camera	
Camera maker	Apple
Camera model	IPhone SE (1st generat...
F-stop	f/2.2
Exposure time	25 sec
ISO speed	ISO-200
Exposure bias	0 step
Focal length	4 mm
Max aperture	
Metering mode	Spot
Subject distance	
Flash modę	No flash
Flash energy	
Focal length	29

Photograph 3. EXIF data of the uploaded photograph

Photograph 4. Graphic file in JPG format with an image of a finger, a fragment of the side of the fingertip and a bag with tablets, secured from an IPhone SE A 1723 smartphone

Video

The submitted video was a video file in MOV format (Apple, Inc). EXIF data for the video file is shown in the photograph 5 and photograph 6. The two-second film showed, similarly to the photo, a finger (the fingertip with two sections) and a fragment of the side part of the fingertip of the hand along with a foil package containing the tablets. The film was analysed in order to obtain better visibility of an unidentified fragment of the lateral part of the fingertip. It was found that at the end of the video there was a movement of the hand and it was observed that a greater area of the unidentified fingertip was visible. Using the PotPlayer (64-bit) software, single frames were extracted from the movie. 65 graphic files in BMP (Bitmap) format were obtained. The analysis of individual files did not bring the expected results because the hand movement was so rapid that the visible image of the unidentified fingertip of the hand was not clear. Another frame extraction was performed using the same software, doubling the number of frames. This made it possible to obtain 141 graphic files in the BMP format, one of which showed a larger area of the unidentified fingertip and was clear enough that it allowed for identification and demonstration of compliance with the middle finger of the right hand of the detained person (the driver of the vehicle) (photograph 7).

Property	Value
Video	
Length	00:00:02
Frame width	1440
Frame height	1080
Data rate	8185kbps
Total bitrate	8877kb/s
Frame rate	
Audio	
Bitrate	691kbps
Channels	1 (mono)
Audio sample rate	44,00kHz
Multimedia	
Participating performers	
Year	
Genre	

Photograph 5. EXIF data of the uploaded photograph

Property	Value
Initial tone	
Beats per minute	
Protected	No
File	
Name	IMG_2279.MOV
File type	Plik MOV
Folder path	
Size	3,19 MB
File type	
Folder path	
Size	A
Creation date	
Offline status	
Shared with	
Owner	
Computer	

Photograph 6. EXIF data of the uploaded photograph

Photograph 7. A single graphic file in BMP format extracted from the film with an image of the finger and a fragment of the lateral part of the fingertip which enabled identification

In addition, a search was performed in the AFIS database. The entire photograph (JPG file) and a single frame from the movie (BMP file) were entered into AFIS. The fingertip of the hand was qualified for search. The most important issue, apart from reversing the horizontal direction of the image, was scaling the image and adjusting the appropriate size. Due to the fact that there was no scale in the photographs, a size correction tool available in AFIS was used, based on applying a ruler and counting ridges (fingerprints). In both cases, i.e. JPEG (photograph) and BMP (single frame from a movie) the scaling was correct. As a result of the search, a HIT was obtained in the first positions on the candidate list.

Positive fingerprint identification of the fingers from the photographs at the time of the proceedings, in the light of the lack of cooperation of the detained person with the procedural authorities and the failure to demonstrate compliance with the revealed fingerprint on the foil packaging, made it highly probable that the person was directly associated with the secured substances and strengthened the evidence collected so far. Subsequent genetic

tests, which found that the sample from the foil packaging was consistent with the profile of the detained person, confirmed the findings based on fingerprint tests.

Summary

The described case and the cited cases from the USA and Spain demonstrated new possibilities in using information contained in visual records and obtaining valuable material for fingerprint tests. Modern smartphones enable taking and sharing high image quality photographs and videos with fine details. Such material may be very useful in identifying the perpetrator based on fingerprint tests, especially in the case of crimes related to paedophilia and child pornography. In videos and photographs, perpetrators deliberately hide their faces, but when recording moments of contact with the victim, they can record the image of their hands or fingers with fingerprints. Graphic and video content with images of items originating from a crime or criminal acts uploaded on the Internet via social networking sites or auctions may also be subject to analysis in order to obtain material for fingerprint identification.

Preparing material for fingerprint identification from visual records based on graphic programs is not a complex process, and simple and effective tools for rescaling photographs in AFIS allow for effective searches in the database.

The continuous development of mobile technology and the increase in the number of video materials available online will mean that a new form of obtaining material for fingerprint identification, previously less common, will appear more frequently and become more significant. Establishing the identity of a person on the basis of such material may demonstrate a direct connection between the person and the event or object, confirm his or her participation in a criminal act or provide information helpful in determining the circumstances of the act and indicate new directions in the proceedings.

Conclusions

Graphic files and video files secured from smartphones, mobile devices, computers or uploaded on the Internet can be analysed in order to obtain research material for fingerprint examination and constitute material for direct identification of a person.

Such investigation material can be defined as a digital fingerprint, i.e. an intangible trace revealed in the memory of a digital medium or in cyberspace, containing image information in digital form, in the form of a moving or still image, showing fingers and hands with fingerprints.

Acknowledgments

1. My sincere thanks go to cpt Dariusz Jęcek from the Central Police Investigation Bureau in Koszalin for his commitment, initiative and innovative approach to the evidence in the case and for help in the preparation of the article.
2. Moreover, I would like to thank lt Hubert Wacławik from the Document and Audiovisual Techniques Research Team of the LK KWP in Szczecin for substantive and technical support in the part regarding digital data media.

Bibliography

Boronat-Far V., González-Novo I., Pedreño-Sala A., Sanjuán G. Fingerprint Identification from Sexual Abuse Videos Obtained from a Mobile Device. *Journal of Forensic Identification, 72* (3).

1. Loll A. (2022). Two Case Studies of Automated Fingerprint Identifications Using Cellular Phone Photographs. *Journal of ForensicIdentification, 72*(4).
2. Mediavilla E.R., Mosquera S.M., Pińas J.C., San Miguel J.C.J. (2021). Anidentification case study from fingerprint photographs. *Forensic Science International, 324.*

Methodologies

1. Metodyka badania cyfrowych nośników danych, ed. I of 4 November 2019, Central Forensic Laboratory of the Police in Warsaw.

Websites

1. https://eu.heraldtribune.com/story/news/2015/06/21/in-sarasota-child-porn-case-a-fingerprinting-first/29320365007/ (dostęp: 24.02.2023).