Can I Post That?: An Empirical Study of Fingerprint Information Leakage in Social Media

***Abstract*—In the ubiquitous social media and online communication era, the inadvertent exposure of sensitive biometric information, specifically fingerprint data, has become an emerging concern. This paper presents an empirical investigation into the potential leakage of fingerprint information through photographs shared on social media and captured using advanced camera technology. Our study demonstrates the feasibility of identifying fingerprint data from unconstrained photographs using readily available technologies, requiring minimal technical expertise. We conducted experiments with photographs taken from varying distances in diverse environments. We posted these images on 11 popular social media platforms to assess the potential for detecting and extracting sensitive fingerprint information. The outcomes find that irrespective of the detectability variations induced by platform-specific image resolution, the extraction of fingerprint information remains feasible from images captured from a distance of 12 feet. In addition, we examined user photo-sharing behavior and the associated perception gap through a survey involving 43 participants. The findings reveal a substantial perception gap. Despite the frequent sharing of personal photographs in public and private digital platforms, awareness of the potential risk associated with biometric data leakage remains alarmingly low, with fewer than 5% of respondents aware of the potential for inadvertent fingerprint data exposure.**

***Index Terms*—fingerprint, biometric information, social media, leakage, privacy, risk awareness**

I. Introduction

Fingerprints have long served as the predominant form of physical biometric identification, with their use in law enforcement spanning over a century [1], [2]. The reliance on fingerprint analysis for identifying suspects and resolving criminal cases is primarily attributed to the robust physical evidence provided by fingerprint matches. The unique and persistent characteristics of fingerprints, such as the distinctive ridge and valley patterns present on the human fingertip, have facilitated their widespread adoption. The advent of the modern computer age in the 1960s saw the deployment of Automated Fingerprint Identification Systems (AFIS) across global agencies [3]. After this development, fingerprint-based recognition technology experienced significant success within security agencies. This success can be attributed to the affordability of scanning devices, the escalation in computational power, and the universal acceptability of this form of biometric identification [4], [5].

However, until the late 2000s, this authentication mechanism was not extensively applied at the user level [6]. Several manufacturers have recently integrated fingerprint sensors into everyday gadgets for authentication purposes, such as smartphones, personal computers, encrypted USBs, smart vehicles, etc. For example, fingerprint authentication became widely accessible on phones in 2013 when Apple introduced TouchID in the iPhone 5. Adapting fingerprint scanning sensors in those gadgets provides advantages over traditional security systems. It is passwordless. This provides users an added layer of comfort and convenience since they no longer have to remember and type in long and complicated passwords to access their data. In addition, several countries use fingerprint technology for mass identification purposes, such as Electronic Voting Machines (EVM) to identify voters at the polling station (i.e., India, Brazil, Canada, etc.), resulting in the storage of fingerprint data. However, privacy concerns have been raised about attackers gaining access to user data and spoofing law enforcement equipment if fingerprint data is compromised. Therefore, protecting fingerprint information is important since it cannot be changed or modified and is nearly permanent.

On the other hand, engaging in various forms of social media is a regular activity in modern life. In the United States, more than 72% of adults use social media, according to the Pew Research Center [7]. People share personal matters on social media, including photos and information. It is almost ubiquitous across all age groups, especially young adults. In addition, the advancement of camera technology and the availability of the internet amplify sharing of photos with the larger community. People easily take and share 4k photos nowadays with their smartphones. Several manufacturers have already combined 8k cameras into their smartphones. Therefore, it is undeniable that people will be able to take high-resolution pictures with their handsets in the coming future and post it online. In addition, with the advancement of digital cameras, anybody may capture a high-resolution photo of a target individual. In both circumstances, a high-resolution finger photo of a person may be obtained, which might provide partial or complete fingerprint information. Figure 1 shows a few publicly accessible photos where individuals are willingly showing their fingers.

The fingerprint extraction from photos first got attention in 2014 when a German hacker group successfully recreated the fingerprint of the German defense minister [8]. However, no details have been provided. In 2019, during the Geekpwn Cybersecurity competition, the X-Lab security research team from Tencent broke the fingerprint authentication from three different phones, but no details about the research were provided [9]. However, according to a Forbes article, the team took a picture of a fingerprint on glass and recreated a fake fingerprint [10]. In addition, plenty of practical experiments have shown how to fake a fingerprint and deceive the small fingerprint sensors employed in smartphones using PVA glue, gelatine, and conductive ink [11]–[14]. However, most previous

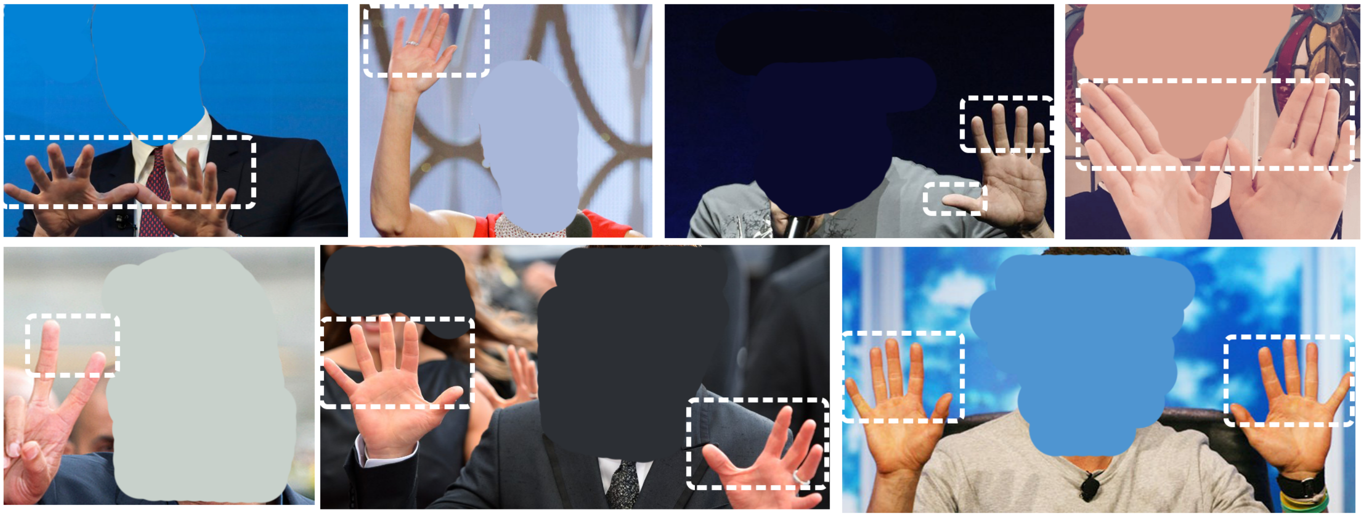

Fig. 1. Many finger photos have been exposed online (intentionally degrading the image quality and size).

research either does not provide details or is performed in a controlled environment.

This paper illustrates the potential for leakage of fingerprint information from photographs captured in uncontrolled environments. We photographed target objects from varying distances and reconstructed the fingerprint to understand the privacy risk. Additionally, we conducted an empirical study on 11 major social media platforms and examined their privacy practices regarding fingerprint information leaking. The study illustrates that fingerprint data can be extracted utilizing commercially available technologies, requiring only a minimal level of technical proficiency.

Contributions: The contributions of this study are as follows:

1) This research conducts an empirical investigation into the leakage of fingerprint information, revealing that fingerprints can be identified from images captured from distances of up to 12 feet.
2) We provide an in-depth analysis of photographs captured at varying distances using multiple cameras, along with a comparison of matching scores between the original fingerprints and those extracted from the images.
3) We conducted a survey on photo-sharing habits and perception gaps regarding finger photo extraction. The results present that over 74% of participants said their photo-sharing practices and exercise more caution in the future.

Organization. The rest of the paper is organized as follows: section II provides background information. Section III discuss the experimental procedure. Section IV discuss the findings and analysis. Section V presents s user perception survey. And finally, in Section VI, we conclude and discuss future works.

II. Background

A. *Fingerprint Matching and Identification*

Fingerprint identification is a process grounded in pattern recognition, where the unique arches, loops, and whorls present in the ridge patterns of fingerprints are compared to previously recorded data. Plenty of commercial providers in the market provide scanners and matching software. Consequently, various methodologies can be employed for matching fingerprint images, including transform-based, correlation-based, and minutiae-based approaches. Certain algorithms focus on extracting local features, while others employ a pattern-based method encompassing the entire fingerprint image, integrating local and global features. Notably, the fingerprint scanners recently incorporated into smartphones are significantly more compact and smaller in size compared to traditional scanners. [15], [16].

B. *Fingerprint Features*

Fingerprints are the complex patterns seen on the pads of the fingers and thumbs. Though prints from palms, toes, and feet are similarly distinct, they are adopted less often for identification. A fingerprint is comprised of ridges and valleys. The lines across the fingerprints are called the ridges, and the valleys are the spaces between the ridges. If we look at the fingerprint in the 2D window, the black lines indicate the ridges, while the white region between the ridges represents the valleys. During fingerprint matching, the ridges between two images are compared [17], [18].

Fingerprint matching employs a multitude of features for accurate identification. A diverse array of factors contribute to the matching process, with the most common approach being the utilization of minutiae and/or pattern-matching techniques. Two primary types of minutiae are recognized: ridge endings and bifurcations. The termination of a ridge characterizes a ridge ending, while a bifurcation, referred to as a Y-junction

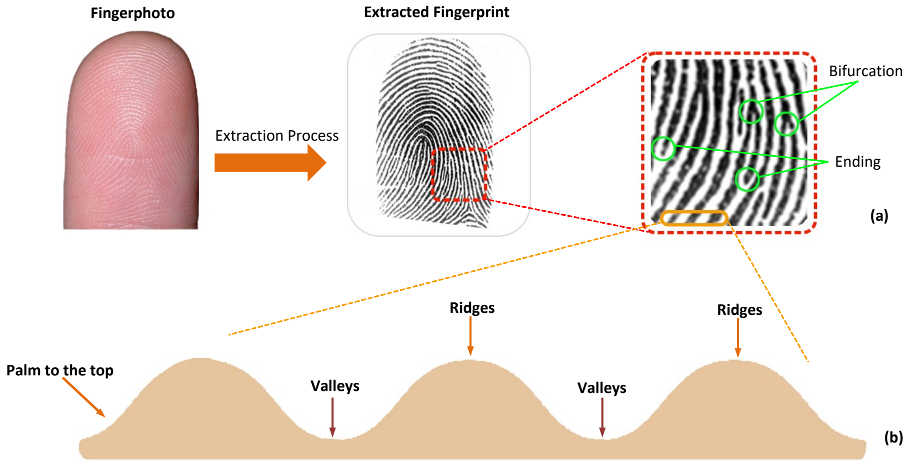

Fig. 2. Multiple features of fingerprint, figure (a) shows ending and bifurcation, (b) shows the ridges and valleys. [The fingerphoto is presented with consent.]

due to its similarity to the letter 'Y', is defined by the division of a single ridge into two distinct ridges. Figure 2 shows the multiple features of fingerprints. Minutiae is featured as the position (x,y) and direction in the matching technique.

Another type of feature pattern, the different global and local patterns, are used in matching. This approach compares ridges flow at all locations between a pair of fingerprint images. The ridge flow constitutes a global pattern of the fingerprint. The Arch, Loop, and Whorl are the basic pattern; however, different classification schemes use more classes [19], [20]. Arch is a specific fingerprint pattern characterized by friction ridges that enter from one side and exit on the opposite side, forming a distinctive rise or wave in the center. Statistically, Arches constitute approximately 5 percent of all observed fingerprint pattern types [21]. Conversely, a Loop is a fingerprint pattern where one or more ridges enter from one side, touch or cross an imaginary line drawn from the delta to the core, and terminate on the same side from which they originated. Loops represent a significant majority of pattern types and account for an estimated 60 percent of all fingerprint patterns [21]. Finally, Whorls form circular or spiral patterns, like tiny whirlpools, representing about 35 percent of pattern types [21]. Some subcategories of patterns exist, consisting of the above three combinations, such as Double Loop, Ulnar loops, Accidental whorl, etc. Figure 3 shows the different fingerprint patterns.

III. Experiment

A. Experiment Setup

We set up a photographic setting to capture participants' images. We marked a distance meter in the outdoor and indoor environment. The outdoor setup operated in daylight (without an external light source). However, the indoor setup has a built-in lighting setup. The distance meter extended to 15 feet, with markings from zero to fifteen. A tripod, equipped with either an iPhone, Google Pixel, or DSLR camera, was positioned at the zero marker. The tripod's location remained constant throughout the experiment, with participants moving to stand at each distance marker in turn. After capturing the photo, participants proceed to the next label, which ranges from 0 to 15. While taking photographs, participants perform the "Hi" gesture with their hands (left or right). Figure 4 illustrates the experimental setup.

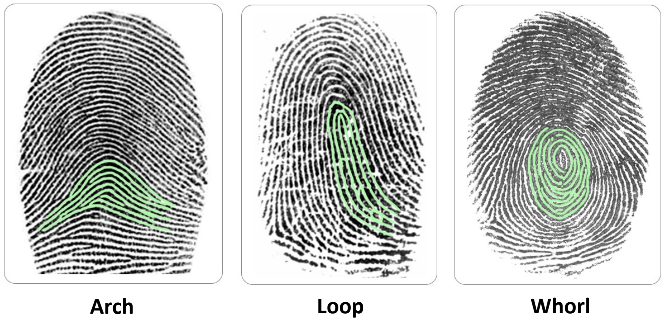

Fig. 3. Fingerprint patterns: Arch, Loop, and Whorl

We used three different types of devices to capture participants' photos. There are iPhone 10 Plus and iPhone 13 Pro for iOS; Google Pixel 4 and Google Pixel 6 Pro for Android; and Nikon D700 (DSLR) with Sigma 50mm f/1.4 lens. Multiple photographs were taken at each position, but after manual filtering, only one image per participant for each device was selected for further analysis.

B. Data Collection

This study collected samples in multiple steps to detect the fingerprint from the photograph. First, we collected the original scanner-produced fingerprint from the devices to get the reference fingerprint for comparison. We collected one original fingerprint per participant. The images used in our experiment were of 300x300 dimensions and stored in a database for subsequent comparison. Additionally, we attempted the traditional method of fingerprint collection, which involves imprinting fingerprints using ink on hard

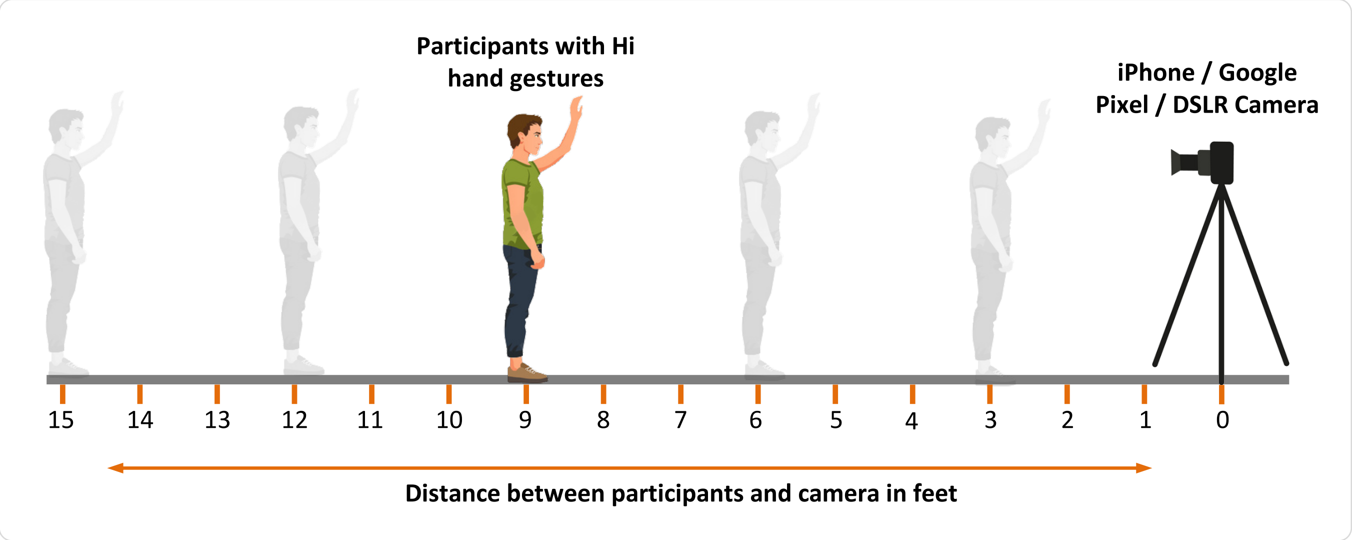
Participants with Hi hand gestures
iPhone / Google Pixel / DSLR Camera
15
14
13
12
11
10
9
8
7
6
5
4
3
2
1
0
Distance between participants and camera in feet

Fig. 4. Experimental setup for capturing participants' photos. We marked a distance meter from one to fifteen. The camera with a tripod is installed at the 0^{th} position on the distance meter. Each time participants stand in front of the camera and increase the distance from one to fifteen.

white paper and scanning the resultant image. However, our experiments revealed that this method did not reliably allow for the automatic identification of fingerprint ridges. The ridge patterns varied even within the same fingerprint, and the results were inconsistent, primarily due to variations in ink thickness. Consequently, we opted to use only scanner-produced fingerprints for comparison and reference. Second, we collected photographs from participants at the distance meter setup. We captured five images for each participant at individual distance levels, one for DSLR, two for iPhones, and two for Google Pixels.

C. Online Images

We uploaded or shared all captured photographs to the targeted 11 online platforms for online sample sources. The online platforms are - Facebook[1], Instagram[2], Messenger[3], WhatsApp[4], Tumblr[5], Pinterest[6], LinkedIn[7], Viber[8], Flickr[9], Twitter[10], and Snapchat[11] without maintaining any order. Some platforms, including Facebook and Instagram, automatically reduce the size and resolution of uploaded images. Despite this, users often aim to upload the highest quality versions of their photos, optimizing them according to the platform's specifications. In this study, we classified our images based on these requirements and optimization processes into full and partial images. Full images refer to those that are not automatically modified in terms of resolution and size by online platforms. Conversely, when online platforms alter the image resolution and size, we categorize these as partial images.

D. Fingerprint Extraction and Matching Score

We have implemented a semi-automated process for the extraction and comparison of fingerprints. The intent was to utilize publicly accessible and free technology that is commercially available. Therefore, we used ImageMagick[12] to extract photos to fingerprint and related editing, enhancements, and photo quality assessment. In addition, we used the SourceAFIS[13] algorithm for recognizing and comparing extracted and original fingerprints. ImageMagick is an open-source, ready-to-run binary distribution software supporting a comprehensive range of operating systems. Primarily, ImageMagick incorporates several command-line interface utilities designed for image manipulation. In contrast to software such as Adobe Photoshop and GIMP, ImageMagick does not possess an extensive graphical user interface for image editing. However, it offers a rudimentary native X Window GUI for Unix-like operating systems, titled IMDisplay, which is utilized for rendering and manipulating images. Moreover, ImageMagick contains API libraries compatible with various programming languages. During photo editing and enhancement, we employed a series of commands. The first stage of extracting the fingerprint required the photo to be cropped to focus on the desired portion, which we identified as the Region of Interest (ROI). Subsequently, we implemented a predefined set of ImageMagick commands to eliminate noise and discard unnecessary portions of the image, thereby revealing the authentic ridges of the finger. However, applying these predefined commands does not always

[1] Facebook - https://www.facebook.com
[2] Instagram - https://www.instagram.com
[3] Messenger - https://www.messenger.com
[4] WhatsApp - https://www.whatsapp.com
[5] Tumblr - https://www.tumblr.com/
[6] Pinterest - https://www.pinterest.com
[7] LinkedIn - https://www.linkedin.com/
[8] Viber - https://www.viber.com/en/
[9] Flickr - https://www.flickr.com
[10] Twitter - https://twitter.com/?lang=en
[11] Snapchat - https://www.snapchat.com
[12] ImageMagick - https://imagemagick.org/index.php
[13] SourceAFIS - https://sourceafis.machinezoo.com

produce optimal outcomes across all images. Variables such as lighting conditions, image resolution, and size required adjustments to our command sets. We manually applied enhancement commands to eliminate unnecessary noise and outliers, modifying them according to specific image conditions.

We compared the fingerprints extracted from photos and those stored in the original fingerprint database to calculate a matching score. A fingerprint is considered a match if its score exceeds an established threshold. In this study, we used the threshold value is 40. In contrast, the fingerprint is classified as non-matching if the matching score falls below this threshold. Java implementations of SourceAFIS were used to calculate this match score. The SourceAFIS API, which is designed for maximum simplicity and usability, provides our application with sufficient precision and speed. Figure 5 shows procedures to get the matching score.

E. Participants and Research Ethics

This study involved collecting finger photos and fingerprints from six participants, with an age restriction set at above 18 years. Ethical principles, particularly informed consent, and privacy, were meticulously respected throughout this process. Participants informed consent was obtained before data collection, ensuring their awareness and acceptance of the study's purpose and implications. Crucially, we maintained strict confidentiality by not storing any personally identifiable information.

IV. Findings

We collected actual fingerprints and captured 450 photographs of six participants during our investigation. Subsequently, these images were uploaded and disseminated across 11 distinct online platforms. We then downloaded all these shared images from their respective sources from different accounts. As a result, we have obtained a set of actual fingerprints for reference and a collection of web-sourced images. It has allowed us to conduct a comparative analysis between the extracted fingerprints and the original fingerprints to identify similarities. We use SourceAFIS to determine the matching score after completing the extraction procedure. The matching scores from the experiments are shown in Table I. The experiments discovered that photographs shot with DSLR cameras provide higher overall matching scores. For instance, a DSLR shot taken 12 feet distant has a matching score of 41.37, larger than the threshold value. In contrast, the iPhone 13 Pro delivers matching results exceeding the threshold at most 9 feet. The iPhone 10 Plus and Google Pixel 6 Pro deliver this level of matching at a maximum distance of 8 feet, while the Google Pixel 4 gives this level of matching at a maximum distance of 6 feet. Therefore, if an attacker takes a photograph of a targeted individual from a distance of 12 feet using a primary lens (Sigma 50mm f/1.4 lens) or from a distance of 9 feet using an iPhone 13 Pro, or from a distance of 8 feet using an iPhone 10 Plus / Google Pixel 6 Pro or from a distance of 6 feet using a Google Pixel 4, the attacker will be able to extract the targeted individual's fingerprint. In addition, we found that the combination of multiple photos gives higher results. Therefore, we anticipate that sophisticated lenses capable of taking several high-resolution photographs will provide better outcomes. However, as evidenced by the results, the performance of user-level devices is improving. The photograph taken by Google Pixel 4 gives matching scores of 70.32, whereas Google Pixel 6 Pro provides 77.3 at the same distance and performance increases by 10%. Overall, photographs taken by Google Pixel 6 Pro and iPhone 13 Pro provide higher matching scores than Google Pixel 4 and iPhone 8 Plus, respectively.

Our investigation focused on the potential for fingerprint information leakage across 11 online platforms, aiming to determine whether these platforms implement any protective measures to mitigate such risks. We identified a subset of these platforms utilizing partially effective practices that could restrict fingerprint information leakage. For instance, Facebook suggests specific image dimensions (720px, 960px, or 2048px in width) and recommends file sizes to remain under 100KB. Facebook implements compression if an uploaded image exceeds these parameters, resulting in an image with fewer identifiable fingerprint features. However, it should be noted that Facebook's image compression is not specifically aimed at preventing fingerprint information leakage. Facebook's practice of compressing images is primarily motivated by its platform's vast volume of daily photographs. Consequently, compressing these files is a practical strategy for managing their vast digital infrastructure.

The platforms such as Facebook, Instagram, Pinterest, LinkedIn, and Twitter employ image compression techniques. However, our research indicates that this method is not fully effective in preventing information leakage. For example, we posted partial photographs instead of complete images to bypass size constraints. After downloading and executing the extraction procedure, we could still obtain fingerprint information (matching score). On the other hand, some platforms do not impose size limitations, allowing us to upload full photographs. Therefore, the images shared across these platforms were contingent on their image size restrictions, involving both full and partial images. Table II shows where we uploaded the full images and the partial images. We have selected the same distance photos for testing of comparison to eliminate the bias. For example, we tested photographs that were taken from three and five feet distances. Because according to TableI, regardless of the camera used (DSLR, or iPhone, or Google Pixel), we see that all images taken within six feet distance provide a matching score higher than the threshold value. Therefore, we formulated a parameter termed 'detection possibility', which is defined as the number of photographs that, after being processed by the online platform, retained a matching score exceeding the predefined threshold value, identical to their pre-processing state. TableII shows the results for target platforms. While we uploaded partial photographs to Facebook and Instagram, Facebook, Instagram, and Tumblr give above 70% detection possibilities. Pinterest, LinkedIn, and Twitter provide 80% possibility. In comparison, all messing-related applications and

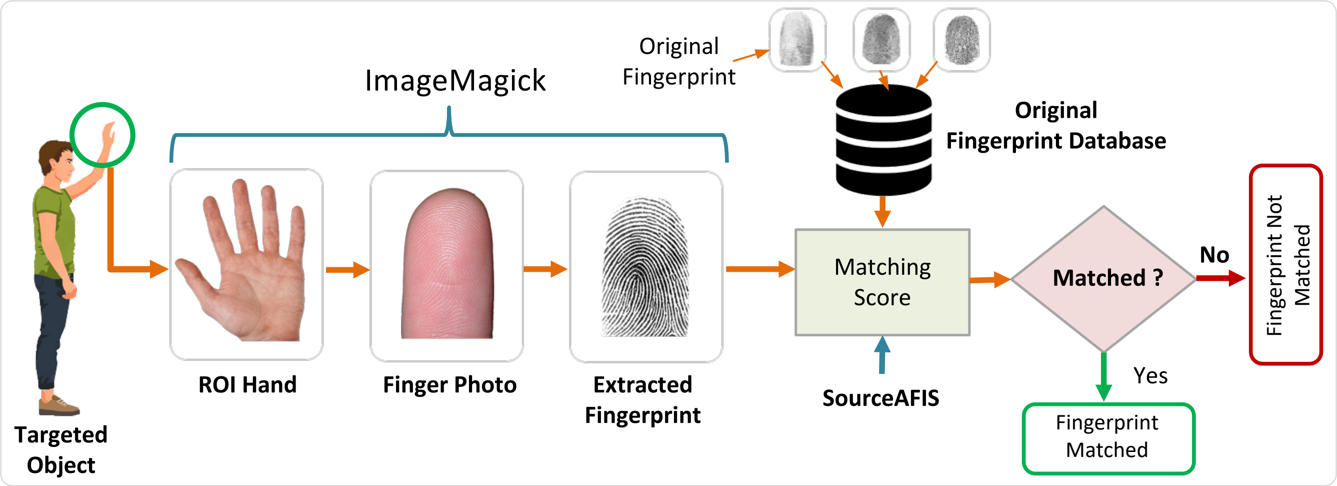

Fig. 5. Fingerprint extraction process from photos using ImageMagick and SourceAFIS.

TABLE I
MATCHING SCORES (IN PERCENTAGE) OF EXTRACTED FINGERPRINT AND ORIGINAL FINGERPRINT

Distance	Detection Possibility				
(feet)	DSLR	iPhone 13 Pro	iPhone 10 Plus	Google Pixel 6 Pro	Google Pixel 4
1	73.38	72.13	69.18	77.3	70.32
2	72.09	65.27	61.33	75.29	65.87
3	70.16	64.4	59.4	70.4	64.39
4	68.39	61.83	58.8	69.8	63.9
5	66.11	61.17	56.22	60	51.48
6	64.22	60.2	49.28	58.3	43.27
7	61.66	55	44.73	56.2	38.33
8	53.27	52.4	40.26	48.11	32.57
9	58.59	43.29	36.51	39.72	23.51
10	50.81	30.21	29.58	25.42	6.8
11	42.19	26.58	15.77	11.25	0.36
12	41.37	15.2	11.8	3.46	not comparable
13	35.74	9.7	11.56	not comparable	not comparable
14	29.48	not comparable	4.2	not comparable	not comparable
15	19.46	not comparable	not comparable	not comparable	not comparable

🟩 - Represents the matching score greater than the threshold value.
🟥 - Represents the matching score less than the threshold value.
🟧 - Represents no matching score found.

Flickr give above 90%.

V. USER PERCEPTION SURVEY

A. Methodology

To understand users' behavioral practices and perception gaps, we conducted a survey. This choice immediately validates users' photo-sharing behavior and privacy concerns regarding fingerprint information leakage. This was an online survey, and we made efforts to reach diverse participants at the university through email and phone.

1) Study Design: We collected participants' answers anonymously. The collected answers were later stored in our local computer for further data analysis. The survey questionnaires consist of three parts:

Part A: Demographic questions about age, gender, education, and race.

Part B: Mainly asked about the behavioral practice of how frequently users share or send photos (personal or group photos) on social media. Or which type of social media users share their photos, etc.

TABLE II
FINGERPRINT DETECTION FROM ONLINE PLATFORM

Platform	Full Image	Partial Image	Detection Possibility (%)		
			≥ 70	≥ 80	≥ 90
Facebook		✓	✓		
Instagram		✓	✓		
Messenger	✓				✓
WhatsApp	✓				✓
Tumblr	✓		✓		
Pinterest		✓		✓	
LinkedIn		✓		✓	
Viber	✓				✓
Flickr	✓				✓
Twitter		✓		✓	
Snapchat	✓				✓

Part C: Questions on privacy concerns regarding photos to fingerprint information leakage. We wanted to know how many users were aware of the finger photo to fingerprints. After collecting initial perception, we added a short note regarding the recent development of finger photos for fingerprint extraction. We asked a few more questions after the note.

2) Demographics: We recruited 43 participants for the user perception survey; 65.12% were male and 34.88% female. The participants were from a range of different age group categories, with an average age of 27.58 years, and SD is 7.3. Among the participants, 6.98% were African American 37.21% were Asian or Pacific Islander, and 30.23% were white. Additionally, 20.93% of participants had earned a college degree, 60.47% had a bachelor's degree, and 18.6% earned a Master's or Ph.D.

B. Results

1) Photo Sharing Behavior: We asked all participants about their photo-sharing behavior. The result is summarized in Figure 6. According to the survey, individuals prefer to exchange images using messaging apps rather than publishing them on social media. The question was how frequently users upload photos or share in messaging. 39.53% of participants responded that they upload 5-10 photos every year, more than 20% of participants said they post 11-30 photos, and just 9.3 percent said they upload more than 30 photos per year.

In comparison, more than 76 percent of participants use messaging services to send more than 30 images every year. Additionally, 2.33 percent of respondents do not post images online, while every respondent sends at least one photo through messaging. We enquired about the platforms that participants frequently use. There were 37 Facebook and Messenger users, 32 LinkedIn users, 29 Instagram users, and 23 Instagram users among the 43 participants. However, when we asked which three platforms they preferred, Facebook, WhatsApp, and Messenger came out on top.

TABLE III
DEMOGRAPHIC DETAILS OF SURVEY PARTICIPANTS

	Participants (n=43)
Gender (%)	
Male	28 (65.12)
Female	15 (34.88)
Age (years)	
Min	19
Max	46
Avg	27.58
SD	7.3
Education level (%)	
College degree	20.93
Bachelor	60.47
Master or Ph.D	18.6
Race/Ethnicity (%)	
African American/Black	3 (6.98)
Asian/Pacific Islander	16 (37.21)
White	13 (30.23)
Other	11 (25.58)

2) Fingerphoto to Fingerprint: We started by asking participants about extracting fingerprint information from photographs. We ask if they believe someone could steal their fingerprint information from publicly available photos or shared photos in closed groups. Over 34% of the participants were neutral; 21% strongly disagreed, and over 18% disagreed. Additionally, except for neutral respondents, more than 15% think that internet platforms have mechanisms to prevent fingerprint extraction. We present a brief overview of the use of finger photographs for fingerprint extraction and the current advancements in that area. Participants seemed convinced and got an awareness of the fingerprint information leakage. For instance, more than 74% of participants said that after reading the notes, their photo-sharing behavior would change, and they would be more careful in the future.

VI. CONCLUSION AND FUTURE WORK

The fingerprint information leakage is critical since it is difficult (but not impossible) to change or revoke the information after it has been compromised. However, However, this study presents that fingerprints may be recognized from images taken up to 12 feet away. This technique can be completed using off-the-shelf technologies. In addition, accuracy may be improved by combining multiple photographs. Shared photos from many sources for a given individual may be used to identify the user. Some anonymous photographs are unable to conceal the fingerprint. Image masking technology may be a solution for automated platforms to reduce the chance of fingerprint information leakage. In addition, users must share their photographs with caution [22].

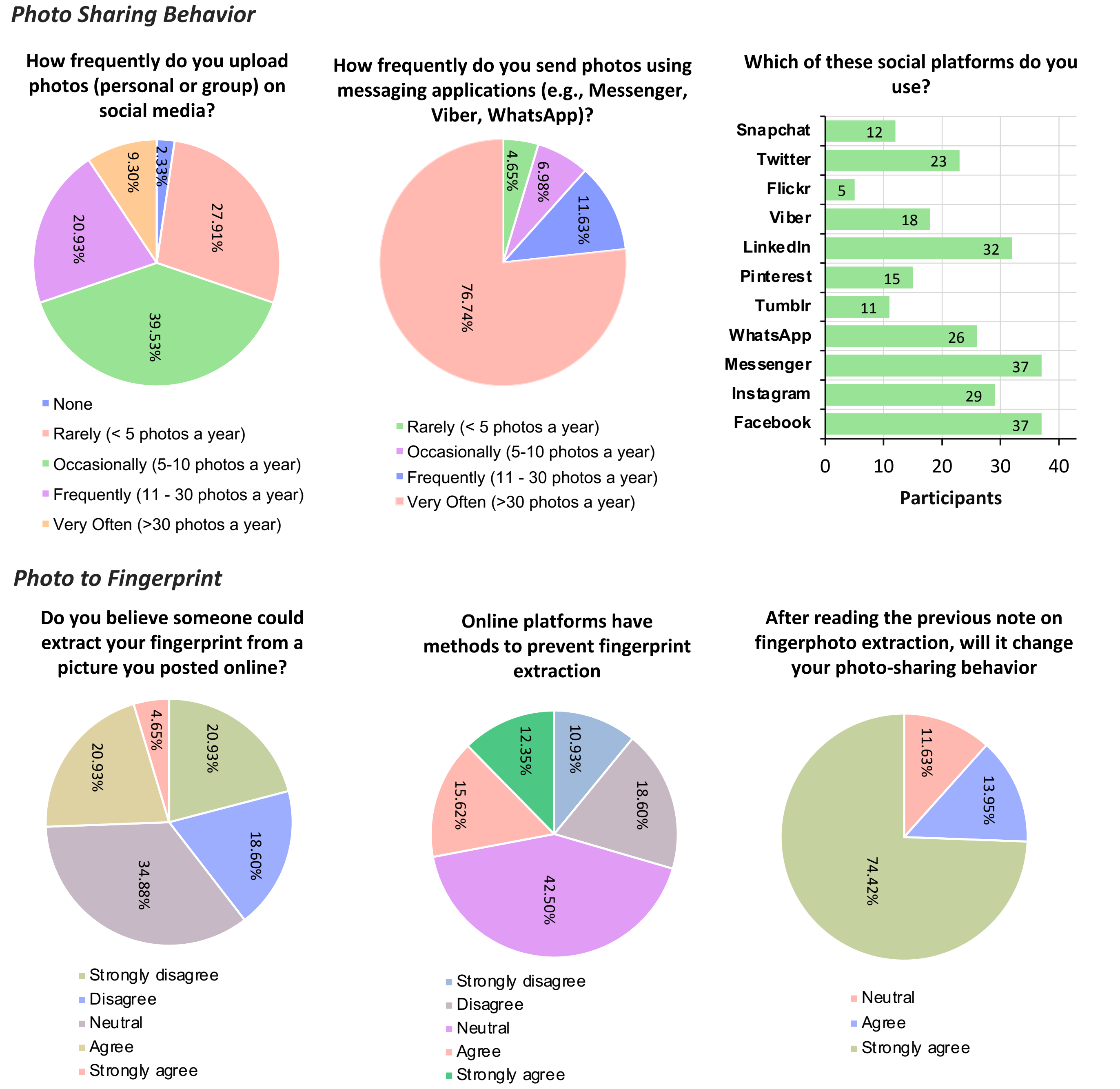

Fig. 6. The survey result shows how participants' perceptions change regarding finger photo extraction.

References

[1] A. K. Jain, K. Nandakumar, and A. Ross, "50 years of biometric research: Accomplishments, challenges, and opportunities," *Pattern recognition letters*, vol. 79, pp. 80–105, 2016.

[2] M. Hawthorne, *Fingerprints: Analysis and Understanding*. CRC Press, 2017.

[3] B. Jefferson, *Digitize and punish: Racial Criminalization in the Digital Age*. U of Minnesota Press, 2020.

[4] K. N. Win, K. Li, J. Chen, P. F. Viger, and K. Li, "Fingerprint classification and identification algorithms for criminal investigation: A survey," *Future Generation Computer Systems*, vol. 110, pp. 758–771, 2020.

[5] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[6] D. A. Horsley, Y. Lu, H.-Y. Tang, X. Jiang, B. E. Boser, J. M. Tsai, E. J. Ng, and M. J. Daneman, "Ultrasonic fingerprint sensor based on a pmut array bonded to cmos circuitry," in *2016 IEEE International Ultrasonics Symposium (IUS)*, pp. 1–4, IEEE, 2016.

[7] "Pew research center: Social media fact sheet," *https://www.pewinternet.org/fact-sheet/social-media/*, June 12, 2019.

[8] P. Monckton, "Hacker Clones Fingerprint From Politician's Photograph." https://www.forbes.com/sites/paulmonckton/2014/12/30/hacker-

clones-fingerprint-from-photograph/?sh=257ca8dc6896, 2014. Last Accessed: March 12 2022.

[9] A. TECHNEWS, “Hackers Use a Photograph of a Fingerprint to Bypass Phone Security.” https://cacm.acm.org/news/240730-hackers-use-a-photograph-of-a-fingerprint-to-bypass-phone-security/fulltext, 2019. Last Accessed: March 12 2022.

[10] D. Winder, “Hackers Claim ‘Any’ Smartphone Fingerprint Lock Can Be Broken In 20 Minutes.” https://www.forbes.com/sites/daveywinder/2019/11/02/smartphone-security-alert-as-hackers-claim-any-fingerprint-lock-broken-in-20-minutes/?sh=41e85dae6853, 2019. Last Accessed: March 13 2022.

[11] K. Cao and A. K. Jain, “Hacking Mobile Phones using 2D Printed Fingerprints,” *Michigan State University, Tech. Rep. MSU-CSE-16-2*, 2016.

[12] JLaservideo, “How To Copy a Fingerprint Like a Spy - iPhone Touch ID Hack.” https://www.youtube.com/watch?v=bp-MrrAmprA, 2016. Last Accessed: March 17 2022.

[13] A. Sankaran, A. Malhotra, A. Mittal, M. Vatsa, and R. Singh, “On Smartphone Camera based Fingerphoto Authentication,” in *2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–7, IEEE, 2015.

[14] A. Taneja, A. Tayal, A. Malhorta, A. Sankaran, M. Vatsa, and R. Singh, “Fingerphoto spoofing in mobile devices: a preliminary study,” in *2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pp. 1–7, IEEE, 2016.

[15] I. Cherapau, I. Muslukhov, N. Asanka, and K. Beznosov, “On the impact of touch {ID} on {iPhone} passcodes,” in *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*, pp. 257–276, 2015.

[16] Y. Javed, M. Shehab, and E. Bello-Ogunu, “Investigating user comprehension and risk perception of apple’s touch id technology,” in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, pp. 1–6, 2017.

[17] Xudong Jiang and Wei-Yun Yau, “Fingerprint minutiae matching based on the local and global structures,” in *Proceedings 15th International Conference on Pattern Recognition. ICPR-2000*, vol. 2, pp. 1038–1041 vol.2, 2000.

[18] H. Choi, K. Choi, and J. Kim, “Fingerprint matching incorporating ridge features with minutiae,” *IEEE Transactions on Information Forensics and Security*, vol. 6, pp. 338–345, June 2011.

[19] M. Tico and P. Kuosmanen, “Fingerprint matching using an orientation-based minutia descriptor,” *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, pp. 1009–1014, Aug 2003.

[20] W. Lee, S. Cho, H. Choi, and J. Kim, “Partial fingerprint matching using minutiae and ridge shape features for small fingerprint scanners,” *Expert Systems with Applications*, vol. 87, pp. 183–198, 2017.

[21] A. de Jongh, A. R. Lubach, S. L. Lie Kwie, and I. Alberink, “Measuring the Rarity of Fingerprint Patterns in the Dutch Population Using an Extended Classification Set,” *Journal of forensic sciences*, vol. 64, no. 1, pp. 108–119, 2019.

[22] M. Nebeling and K. Madier, “360proto: Making interactive virtual reality & augmented reality prototypes from paper,” in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–13, 2019.