*MUST Journal of Research and Development (MJRD) Volume 6 Issue 2, June 2025*
*e ISSN 2683-6467 & p ISSN 2683-6475*

# The Potential Risks of Using Social Media: How Sharing Pictures with a Particular Pose Could Expose Biometric Data

Lazaro Inon Kumbo*, Victor Simon Nkwera, Rodrick Frank Mero, Robert Michael Sikumbili and Martin Ludovick Mushi

Department of Computing and Communication Technology, National Institute of Transport, P. O Box 705, Dar es Salaam, Tanzania

DOI: https://doi.org/10.62277/mjrd2025v6i20016

## ARTICLE INFORMATION

### Article History

*Received:* 10th September 2024
*Revised:* 05th April 2025
*Accepted:* 14th May 2025
*Published:* 30th June 2025

### Keywords

Biometric data exposure
Fingerprint extraction
Social media privacy
Image processing techniques
Digital forensics

## ABSTRACT

The rapid expansion of social media has transformed communication, enabling seamless information sharing across global networks. While these platforms enhance connectivity, they also pose significant privacy risks, particularly through the unintended exposure of sensitive biometric data. Every day, billions of images are shared online, often revealing more information than users intend, including identifiable fingerprint details. This study examines how publicly available images can be exploited to extract biometric data using digital image processing and forensic analysis. By applying techniques such as contrast enhancement, noise reduction, and ridge pattern extraction, we assess the feasibility of retrieving fingerprint details from shared images. Findings highlight the potential risks of unauthorised biometric data collection, raising concerns about identity theft, unauthorised access, and financial fraud. The study emphasises the need for greater user awareness and advocates for stronger security measures, including automated detection tools, stricter privacy settings, and enhanced encryption, to mitigate the risks associated with biometric data exposure on social media.

*Corresponding author's e-mail address: lazaro.kumbo@nit.ac.tz (Kumbo, L)

## 1.0 Introduction

The rapid expansion of social media platforms has fundamentally transformed how individuals communicate, interact, and share information (Dwivedi *et al.,* 2021). These platforms enable users to share personal photos and experiences globally, fostering unprecedented connectivity and engagement (Kapoor *et al.,* 2017). However, this digital revolution introduces significant risks, particularly the unintentional exposure of biometric data embedded in high-resolution shared photos, such as fingerprints (Ma & Fan, 2022). Biometrics play a crucial role in authentication processes due to their reliability and ability to uniquely identify individuals. Among biometric traits, fingerprints are particularly valued for their accuracy in security and authentication systems (Ghazinour & Ponchak, 2017; Kutschera, 2022). However, the protection of biometric data is essential to maintain the integrity and safety of these practices. Safeguarding such sensitive information ensures the authentication process remains secure and resistant to potential misuse or breaches. To ensure reliability, biometric data must be securely stored using encryption techniques, with access restricted to authorised personnel and systems. Improper handling of biometric data, such as failing to implement adequate encryption and permitting unauthorised access or sharing, can lead to significant security risks, including identity theft, unauthorised system breaches, and fraudulent activities (Kutschera, 2022).

Photo-sharing online has become a common practice with the rise of social media platforms, where users post personal photos for social interaction and self-expression (Archer & Wildman, 2021). However, many individuals are unaware that seemingly harmless photos can contain sensitive information, such as biometric data, that may be inadvertently exposed. Laas-Mikko *et al.* (2022) observed that the growing sharing of photos raised concerns about privacy and data security in the digital age. High-resolution photographs shared online can unintentionally reveal detailed biometric information, including fingerprints, which malicious actors can extract and exploit for unauthorised purposes (Quach *et al.,* 2022). This exposure poses severe threats such as identity theft, unauthorised access to secure systems, and financial fraud. Despite the growing prevalence of this issue, public awareness remains limited, and existing privacy measures often fail to address these specific risks effectively, leaving individuals vulnerable to exploitation.

A significant research gap exists in the limited examination of the technical feasibility and implications of extracting biometric data, specifically fingerprints, from publicly accessible social media photos. While existing studies broadly address privacy concerns, they often lack a focused analysis of the mechanisms through which photo processing and forensic technologies enable biometric data identification. This study bridges these gaps using photo processing techniques to evaluate the technical feasibility of extracting and enhancing fingerprint details from publicly shared photos. Additionally, it examines the potential misuse of this biometric data, highlighting the security risks and ethical challenges posed by these emerging threats, thereby underscoring the critical need for enhanced awareness and preventive measures.

The study proposes actionable solutions to mitigate these risks, including raising public awareness about the dangers of sharing high-resolution photos online, developing advanced security protocols to safeguard biometric data, and implementing stringent privacy regulations to limit unauthorised access. By addressing these vulnerabilities, the research aims to contribute to the broader discourse on digital privacy and security while providing practical measures to enhance biometric data protection in an increasingly connected world.

## 2.0 Materials and Methods

This study employed an exploratory research methodology to investigate biometric risks associated with publicly shared photos on social media. Given the difficulty of defining a clear target population, this methodology enabled an in-depth examination of specific cases, such as fingerprint orientation, without aiming to generalise findings to a broader population. Content analysis was chosen as the primary analytical method, allowing for a rich understanding of the subject matter. To supplement the analysis, interviews were conducted to gain additional insights into the security risks posed by shared biometric data. The study aimed to answer the research question: how can publicly shared photos on social media inadvertently expose biometric data, specifically fingerprints, and what are the associated security risks?

### *2.1 Target Population*

The study focused on publicly shared photos featuring visible fingerprints on social media platforms. It analysed these photos to explore the potential risks associated with online photo sharing regarding biometric data exposure.

### *2.2 Sampling Frame*

The sampling frame comprised publicly accessible photos from Instagram and Facebook in Tanzania. These platforms were selected for their widespread usage in Tanzania and their emphasis on photo-based content, aligning with the study's objectives. Other platforms, such as TikTok and Twitter, were excluded because TikTok primarily focuses on short-form video content. Twitter emphasises text-based posts, making them less suitable for analysing static fingerprint photos.

### *2.3 Sampling Technique*

A purposive sampling technique was employed to select photos that directly aligned with the study's focus. This approach minimised selection bias and ensured the inclusion of only photos most relevant to the study's objectives, such as those featuring visible and front-facing fingerprints.

### *2.4 Sample Size*

The dataset comprised 10,615 photos, of which 10,562 were deemed irrelevant because they did not meet the inclusion criteria. The remaining 53 photos were identified as relevant for analysis. These photos met specific criteria, such as the visibility of front-facing fingerprints, and were considered sufficient for addressing the study's objectives.

#### *2.4.1 Data Acquisition*

Data were collected using the Facebook Graph API and Instagram Basic Display API. These tools allowed for systematically gathering a large volume of publicly shared photos, ensuring efficiency and scalability in the data collection process.

#### *2.4.2 Photo Categorisation*

The photos were categorised into two groups based on relevance. The relevant category included photos featuring visible, front-facing fingerprints, which were further divided into three subcategories: one fingertip (thumb), two fingertips (index and middle), and a waving hand (all five fingertips). On the other hand, the irrelevant category encompassed photos that did not meet these criteria, such as those lacking fingerprints or those with poor photo quality, which made them unsuitable for analysis.

Table 1

*Classification of Photos by Relevance Based on Hand Positioning for Analysis*

| Category | Number of Photos |
|---|---|
| Relevant | 53 |
| Irrelevant | 10562 |
| Total: | 10615 |

##### *2.4.2.1 Inclusion Criteria*

Photos were included in the analysis if they met two key criteria: a) they featured front-facing fingertips visible for potential biometric analysis, and b) they were publicly accessible, having been posted on Instagram or Facebook within Tanzania. These conditions ensured that the selected photos were suitable for studying the exposure of biometric data in publicly shared social media content.

##### *2.4.2.2 Exclusion Criteria*

Photos were excluded from the analysis if they did not meet specific criteria: a) they either did not feature fingertips or had poor photo quality, and b) they were sourced from other platforms such as TikTok and Twitter. These platforms were excluded because their primary focus on video and text content made them less suitable for static photo analysis, which required clear and relevant visual data for biometric assessment.

### *2.5 Justification for Sample Size and Technique*

The purposive sampling technique ensured the inclusion of only photos most relevant to the study's objectives, thereby enhancing data quality and reducing selection bias. While only 53 photos were deemed relevant, this sample size was sufficient to explore the targeted phenomenon comprehensively. The exclusion of irrelevant photos ensured that the analysis focused solely on cases that provided valuable insights into biometric risks.

### *2.6 Data Analysis*

The study used a content analysis approach to examine the photos collected for biometric exposure. This method allowed for a detailed evaluation of variables such as fingertip visibility, hand positioning, and photo quality.

### *2.6.1 Steps in the Content Analysis Approach*

In this analysis, key variables such as fingertip visibility, hand angle, and photo clarity were defined for examination. Photos were selected based on the inclusion criteria, which required the presence of at least one visible fingerprint in a front-facing orientation. To assess the level of biometric exposure, the photos were further categorised into three risk levels: low, moderate, and high, based on the number of exposed fingerprints and the photo's clarity. This classification allowed for a comprehensive evaluation of the potential biometric risks associated with the shared photos.

### *2.7 Sampling Techniques*

Using purposive sampling ensured that the study prioritised depth and relevance over breadth. This approach aligns with the exploratory nature of the research, focusing on qualitative insights into biometric risks rather than statistical generalisation. Despite the small number of relevant photos, the sample size was sufficient to meet the study's objectives and provide meaningful insights into the targeted phenomenon.

## 3.0 Results

This section provides a discussion on the risks of posting photos based on specific camera poses during capture. The analysis focuses on how different poses can unintentionally expose sensitive information, such as fingerprints, in greater detail. The study highlights the importance of mindful photo sharing on social media by examining these risks based on the Fingertip Orientations in Camera Poses.

### *3.1 Fingertip Orientations in Camera Poses*

According to this study, fingertip orientations in camera poses are divided into three categories: the pose showing two fingertips (middle and index), one fingertip (thumb), and a waving hand (five fingertips). The prevalent pose shows two fingertips prominently while the remaining three are closed, creating a distinct visual focus on the fingertips. Another frequently seen pose is where the individual closes all four fingertips while extending the thumb outward, often used in gestures or expressions. Lastly, the waving hand gesture was also considered, where all five fingertips were prominently shown. The summary of the data collected and analysed for this study is indicated in Table 1.

Table 1
*Fingertips Orientation for Picture Poses*

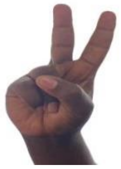
| Fingertip Orientation | Frequency | Percentage |
|---|---|---|
| The pose shows two fingertips (Middle and index) | 29 | 54.7 |
| One fingertip (thumb) | 21 | 39.6 |
| Waving had | 03 | 05.7 |
| **Total** | **53** | **100** |

### *3.1.1 Pose with Two Fingertips Prominently Displayed*

In a comprehensive analysis of photos shared on social media platforms, Instagram and Facebook, 53 pictures were examined to understand the common poses displayed by individuals. Among these, a notable 29 photos, which represent 54.7% of the total, prominently feature a pose characterised by the display of the index and middle fingers. In stark contrast, only three photos depict a gesture with closed fingers. This hand gesture is closely associated with Chama cha Demokrasia na Maendeleo (CHADEMA), a leading political party in Tanzania. Within the party's community, this pose is a sign of camaraderie and a customary greeting among its members. The prevalence of this gesture in the analysed photos highlights its cultural significance and the shared identity among supporters of CHADEMA. It reflects individual expression and a broader social and political ethos that is significant within

Tanzanian politics. The consistent use of this gesture in various contexts underlines its importance in creating a sense of belonging and solidarity among the party's followers.

Figure 1
*The Pose with Two Fingertips Prominently Displayed*



These gestures are also commonly used in various scenarios for picture poses. For instance, people often use this gesture to signify peace or victory in casual and formal photographs. It is a famous pose during celebrations, protests, rallies, and even everyday social media posts to convey a sense of positivity and solidarity. The widespread use of this gesture in different contexts highlights its versatility and symbolic power in visual communication.

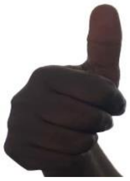
The distinct pose of displaying the middle and index fingers facilitates an in-depth examination of these digits, rendering them susceptible to comprehensive biometric data extraction. High-resolution photos can be meticulously analysed using sophisticated photo-processing techniques to reveal intricate fingerprint patterns with remarkable clarity and precision. It benefits specific applications, including applications in biometric security systems and accessibility for sign language recognition. Analysing unique fingertip poses can enhance identity verification in biometric security, providing an additional layer of authentication in secure logins or mobile banking apps. Meanwhile, inaccessibility and recognising different fingertip orientations are vital for interpreting hand signs in sign language. Applications that identify hand gestures based on fingertip positioning can translate sign language into text, supporting communication for those who are deaf or hard of hearing and enhancing inclusivity in virtual meetings.

The extraction of biometric information from fingertip poses, while beneficial, also presents significant privacy risks. This process can inadvertently expose individuals to heightened vulnerabilities, as malicious actors may exploit extracted biometric data. Such misuse could lead to severe consequences, including identity theft, unauthorised access to sensitive systems, financial fraud, and other forms of cybercrime. The potential ramifications of these privacy breaches emphasise the urgent need to protect biometric data by implementing rigorous security protocols and robust privacy safeguards, underscoring the critical importance of responsible data handling in an increasingly digital world.

#### *3.1.2 Pose with Thumb Extended Outward*

When analysing pictures posted on Instagram and Facebook, we found that 21 out of 53, or 39.6%, of the photos depict a pose with the thumb extended outward and the remaining four fingers closed. This specific gesture is commonly associated with Chama cha Mapinduzi (CCM), the political party in Tanzania, and is frequently used as a form of salutation among its members. This gesture is widely recognised and used globally to signify that something is okay or proceeding well. The prevalence of this gesture in the analysed photos highlights its cultural significance and everyday usage in both political and general social contexts.

Figure 2
*The Pose with Thumb Extended Outward*



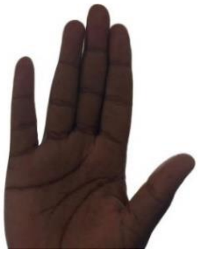
These gestures are also commonly used in various scenarios for picture poses. For instance, people often use this gesture in selfies, group photos, and casual snapshots to convey a positive or relaxed mood. It is also popular in celebratory contexts, such as sporting events, parties, and social gatherings, where individuals want to express approval or success. The widespread use of this gesture in different contexts underscores its versatility and symbolic power in visual communication. The prominent pose display with the thumb finger exposes this finger to detailed scrutiny and potential biometric data extraction.

Advanced photo processing techniques can enhance these high-resolution photos to extract fingerprint patterns with significant clarity and detail. This inadvertently exposes individuals to privacy risks, as biometric information could be used maliciously for identity theft, unauthorised access, or other forms of cybercrime.

### *3.1.3 Waving Hand*

When analysing pictures posted on Instagram and Facebook, we found that 3 out of 53, or 5.7%, of photos captured individuals waving and revealing their hands' fingertips. This pose contrasts with others where only specific fingertips, like the index and middle fingers, are prominently displayed. The waving gesture, showing an open hand, is commonly used in various settings to greet others, signal goodbye, or attract attention. In Tanzania, this gesture is frequently observed in public gatherings, political rallies, community events, and social interactions to convey friendliness, openness, and acknowledgement. The prevalence of this gesture in different contexts underscores its significance as a universal symbol of communication and connection.

Figure 3
*Waving Hand*



The display of all fingertips in a waving action exposes a broader surface area of the hand, potentially revealing more detailed biometric information such as fingerprint patterns. Unlike posts where only specific fingertips, like the index and middle fingers, are prominently displayed, waving exposes all fingers, making it easier for advanced photo processing techniques to extract biometric data.

Qualitative analysis used structured interview questions to better understand users' perceptions of biometric data exposure through social media image posting. This approach allowed for an in-depth exploration of participants' insights and experiences. The interview questions were designed to uncover various aspects of user awareness, behaviour, and suggestions for improving security measures. Below is a detailed discussion of each question and its relevance to the study. The discussion started with regular users, followed by technical users like information security specialists.

***QN 1:***

How aware are you of the risks of sharing images on social media, specifically concerning biometric data like fingerprints?

A respondent noted:

> *I am somewhat aware of the risks, but I did not realise that sharing images could lead to biometric data exposure. I knew there were privacy concerns, but the idea that fingerprints could be extracted from photos is new to me.*

This response highlights a gap in awareness regarding the specific risks of biometric data exposure through social media images. Similar findings are reported in other studies. For example, research by Kutschera (2022) indicates that while users are generally aware of privacy issues related to social media, they often underestimate the risks associated with biometric data exposure. Ma & Fan (2022) further confirm that many users do not fully grasp how high-resolution images can inadvertently reveal sensitive biometric information such as fingerprints. This gap in awareness underscores the need for increased education and transparency about the potential risks of sharing high-resolution images online.

***QN 2:***

Have you ever considered the potential security implications of your gestures or poses in your social media photos, such as prominently displaying your fingers? A respondent noted:

A respondent noted*, "Honestly, I have not given much thought to the security implications of the gestures I use in my photos. I usually focus on how the pose looks and whether it suits the occasion."*

***QN 3:***

What precautions, if any, do you currently take when posting photos online to protect your privacy?

A respondent noted:

> *In case I want to post a photo containing my partner or my kids, and I do not want the face to be shown, I usually use blur or crop out identifiable details, such as faces or location markers. Additionally, I limit my audience by adjusting privacy settings on my social media accounts.*

***QN 4:***

Have you ever received warnings or educational content about biometric security risks on social media? If so, what was your reaction?

A respondent noted:

> *No, I do not recall seeing any warnings about biometric risks. Most security alerts I see on social media focus on phishing scams and account hacking but nothing about fingerprint or facial recognition risks. If I had seen such content, I would have taken more precautions when posting photos.*

***QN 5:***

How do your peers perceive the risks of sharing biometric data online?

A respondent noted*, "Most of my friends are not aware of these risks. They frequently post high-resolution selfies and hand gestures without realising biometric data could be extracted. Some think privacy risks only apply to passwords or location sharing, not photos."*

***QN 6:***

Would you change how you post images if you knew that biometric data could be extracted? Why or why not?

A respondent noted:

> *Yes, I would be more careful. If I knew that my fingerprints or other biometric data could be misused, I would avoid posting images that show my hands clearly. I would also educate my friends about these risks so they could be more cautious.*

The responses from QN2 to QN6 reflect a common oversight among social media users, who often prioritise aesthetic considerations over security concerns. Social media users often prioritise aesthetics over security, overlooking the risks of sharing biometric data (Ziegele & Quiring, 2011; Pomeroy *et al*., 2020). Many remain unaware that gestures and poses in photos can reveal sensitive information, a finding supported by Holub *et al.* (2023). While some users take precautions by blurring or cropping identifiable details and adjusting privacy settings (Laas-Mikko *et al.,* 2022), others assume privacy risks are limited to passwords or location sharing, leading to careless posting of high-resolution images (Quach *et al.,* 2022; Kapoor *et al.,* 2017). The absence of educational content on biometric security (Ma & Fan, 2022) further contributes to this oversight, as most security alerts focus on phishing or account hacking (Dwivedi *et al.,* 2021). Raising awareness through proactive educational efforts and platform-integrated security measures could encourage users to adopt safer practices when sharing images online.

Another group of respondents involved in this study were information security specialists whose insights provided a more technical and in-depth perspective on the risks and mitigation strategies associated with biometric data exposure on social media. Unlike general social media users, these specialists possess advanced knowledge of cybersecurity threats, data privacy concerns, and digital forensics, allowing them to assess user behaviour and platform security measures critically. The questions included the following:

***QN 7:***

How confident are you that social media platforms adequately protect users from unintended biometric data exposure?

A respondent noted:

> *I am not very confident. Social media platforms focus more on protecting passwords and accounts from hacking, but they do not seem to address biometric security. There are no clear warnings or automatic alerts when someone uploads a photo that could expose their fingerprints or other sensitive details.*

***QN 8:***

What features or tools should social media platforms provide to help users better protect their biometric data?

A respondent noted:

> *Social media platforms should develop automatic detection tools that notify users when their photos contain biometric data. They should also provide an option to blur or*

*mask sensitive parts of images before posting. Additionally, privacy awareness campaigns should be integrated into the platforms to educate users about these risks.*

***QN 9:***

Do you believe government regulations should require social media platforms to implement biometric security measures?

A respondent noted, *"Regulations should be implemented to ensure platforms take responsibility for biometric security. Since biometric data is unique and cannot be changed like a password, it is crucial to have legal frameworks that mandate stronger protection measures."*

***QN 10:***

Do you think social media users are unaware that biometric data can be collected through sharing photos?

A respondent noted: *"Many users are unaware that their biometric data is being collected, not only by hackers but sometimes by the platforms themselves. Strict policies must be in place to prevent misuse and ensure user control over their biometric identifiers."*

***QN 11:***

If given the opportunity, what suggestions would you give policymakers regarding protecting biometric data on social media?

A respondent noted:

> *I recommend that policymakers require social media platforms to implement built-in biometric protection tools. There should also be laws regulating how companies collect and use biometric data. Public awareness campaigns should be funded to educate users about the risks and best practices for protecting their biometric information online.*

The responses from QN7 to QN11 highlight a significant gap in biometric security on social media platforms observed by information security specialists, as respondents expressed low confidence in current protections, noting the absence of clear warnings or alerts about biometric data exposure. This aligns with prior research indicating that social media primarily focuses on password security while overlooking biometric vulnerabilities (Kutschera, 2022). Respondents emphasised the need for automatic detection tools to notify users when biometric data is present in uploaded images, along with options to blur or mask sensitive details, measures supported by previous studies advocating enhanced security protocols (Dwivedi *et al.,* 2021). Additionally, the lack of public awareness about biometric data collection, sometimes even by social media platforms, underscores the need for stricter policies and regulatory frameworks (Laas-Mikko *et al.,* 2022). Given the irreversible nature of biometric data, respondents strongly supported government intervention to mandate protective measures, reinforcing the urgency of implementing legal safeguards to prevent unauthorised data use and mitigate security risks (Ghazinour & Ponchak, 2017; Quach *et al.,* 2022).

***QN 12:***

What role should influencers and content creators play in raising awareness about biometric security risks?

A respondent noted, *"Influencers and content creators have a large audience, so they should use their platforms to educate people about biometric security risks. If they share best practices and promote privacy-conscious behaviour, more users will become aware and take precautions."*

The response highlights the significant influence that content creators and influencers have in shaping public awareness and behaviour, particularly regarding biometric security risks. As individuals with large followings, influencers can leverage their platforms to educate their audience on the risks of sharing biometric data through social media photos, promoting privacy-conscious behaviour, and encouraging precautions (Archer & Wildman, 2021). By sharing best practices for securing biometric data and advocating for more stringent privacy measures, influencers can help bridge the knowledge gap and foster a more security-conscious online community. This aligns with recommendations from Kutschera (2022) and Ma & Fan (2022), who stress the need for awareness campaigns to empower users to protect their data better.

### *3.2 Level of Risks Based on the Number of Fingerprints Exposed*

The study classified the number extent of effect as low, moderate, and high per number of fingertips front facing exposed.

Table 2

*Level of Risks as Per the Number of Fingertips Front-Facing*

| Risks | Number of Fingertips |
|---|---|
| Low | 01 |
| Moderate | 02 |
| High | 05 |

Exposing all five fingertips of one hand significantly heightens the risk of attackers harvesting multiple data points, thereby increasing the likelihood of successful biometric cloning and unauthorised access. Many security systems permit the registration of multiple fingerprints, meaning that revealing all five fingers simultaneously provides would-be assailants with abundant material to exploit. This scenario presents a high risk for identity theft or misuse. In contrast, exposing two fingertips, such as the index and middle fingers, presents a moderate risk to biometric security. Although fewer fingers are displayed compared to the complete hand, the clarity and prominence of these two fingers in most poses render them particularly vulnerable to biometric data extraction. Advanced photo processing techniques can capture detailed fingerprint patterns from high-resolution photos of these two fingers, which could be misappropriated for unauthorised access or identity theft. The risk remains moderate because these two are often the primary ones utilised in various fingerprint authentication systems despite the reduced number of exposed fingers.

Exposing just one fingertip, like the thumb, carries a relatively low to moderate risk to biometric security. While only a single finger is visible, the thumb is frequently displayed prominently in poses, making it susceptible to meticulous examination in high-resolution photos. Despite the ability of advanced photo-processing techniques to extract fingerprint patterns from a solitary exposed fingertip, the overall risk is somewhat diminished compared to the exposure of multiple fingers. Moreover, since many security systems require multiple fingerprints for verification, exposing just one fingertip may not suffice for comprehensive biometric exploitation, further reducing the overall risk.

### *3.2 Fingerprint Extraction Process*

The practice of capturing fingertip orientations in photographs and posting them on social media carries significant implications. Advanced photo processing techniques can extract detailed biometric information that may be exploited illegally (Agarwal *et al.,* 2024). For example, high-resolution photos shared on platforms like Instagram and Facebook can inadvertently expose intricate fingerprint patterns, including those visible on extended thumbs. This capability underscores the potential risks of unintentional biometric data exposure through seemingly innocuous gestures. The following steps illustrate how advanced photo processing can extract and utilise such detailed biometric information:

#### *3.2.1 Identifying Photos with Visible Fingerprints*

In our analysis, the initial step involves meticulously scanning a collected photo dataset to pinpoint those prominently displaying fingerprints. Whether manual or automated, this screening process isolates relevant photos whose fingertips are visible and identifiable (Kellman *et al.,* 2014).

#### *3.2.2 Applying Photo Enhancement Techniques*

The next crucial phase entails applying advanced photo enhancement techniques upon identifying suitable photos. These methods are pivotal in refining the clarity and visibility of the fingerprint patterns embedded within the photos. Adjustments to contrast, brightness, and sharpness are meticulously made to accentuate the fingerprints' unique ridges and minutiae points (Agarwal *et al.,* 2024).

#### *3.2.3 Using Forensic Software to Extract and Analyse Fingerprint Patterns*

Forensic software tools are pivotal in extracting and analysing fingerprint patterns from enhanced photos. These specialised tools meticulously scrutinise and identify the intricate details of the fingerprint ridges and minutiae. By leveraging these technologies, we can compile and analyse extracted data to uncover potential matches or recurring patterns within the dataset (Agarwal *et al.*, 2024; Kellman *et al.,* 2014).

### *3.3 Cultural and Social Significance*

The prevalence of this gesture in our dataset underscores its cultural and social significance. Beyond political contexts, people commonly use this pose in various social settings, such as selfies, group photos, and casual snapshots (Holub *et al.,* 2023). It serves as a visual cue to communicate a positive or relaxed mood, making it popular in celebratory scenarios like sporting events, parties, and social gatherings (Maclean *et al.,* 2022). The gesture's versatility in different contexts highlights its symbolic power and its role in visual communication on social media platforms.

### *3.4 Implications for Biometric Data Exposure*

The widespread use of gestures and poses that reveal fingerprints in high-resolution photos shared on social media carries significant implications for biometric data security. Advanced photo processing techniques can extract detailed biometric information, such as fingerprint patterns, from these photos, posing substantial risks to user privacy and security (Dunsin *et al.*, 2024; Holub *et al.*, 2023).

#### *3.4.1 Identity Theft and Unauthorised Access*

One of the most concerning implications is the potential for identity theft. Biometric data, like fingerprints, are unique identifiers used in various security systems, from unlocking smartphones to accessing secure facilities (Alsmirat *et al.,* 2018). If criminals can extract and replicate fingerprint photos from social media posts, they could bypass biometric authentication systems, leading to unauthorised access to personal devices, financial accounts, and sensitive information (Cinar & Kara, 2023). This capability dramatically increases the ease with which identity theft can occur, as traditional forms of identification can be circumvented with forged biometric data.

#### *3.4.2 Financial Fraud*

The misuse of biometric data for fraudulent financial transactions is another significant threat. Financial institutions increasingly rely on biometric authentication for secure transactions. However, if criminals can extract fingerprints from social media photos, they could potentially authenticate fraudulent transactions, resulting in substantial financial losses for individuals and institutions (Ho *et al.,* 2023). The extraction and exploitation of biometric data thus extend beyond personal privacy violations, threatening the integrity of financial systems.

#### *3.4.3 Legal and Regulatory Challenges*

The legal and regulatory landscape concerning biometric data exposure through social media is complex and often insufficient to address the rapid advancements in digital forensics and photo processing technologies. Current regulatory frameworks may not adequately protect user data or ensure accountability for misusing biometric information extracted from publicly shared photos (Baechler, 2020). Effective regulatory measures must navigate the intersections of privacy laws, digital rights, and technological innovation to provide robust protections against biometric data exploitation (Kutschera, 2022; Laas-Mikko *et al.,* 2022).

#### *3.4.4 Need for User Awareness and Education*

Enhancing user awareness and education is crucial to mitigating the risks associated with biometric data exposure. Many users are unaware of the potential dangers of sharing high-resolution photos that could reveal biometric data. Educating users about these risks and encouraging them to use privacy settings effectively can empower them to make informed decisions about their online activities (Maclean *et al.,* 2022). Social media platforms also play a pivotal role in implementing robust privacy settings and transparency measures to protect user data.

#### *3.4.5 Role of Social Media Platforms*

Social media platforms must adopt advanced security protocols to prevent unauthorised biometric data extraction from posted photos. This includes developing tools to detect and blur sensitive biometric information automatically before publicly sharing photos. By taking proactive measures, platforms can help mitigate the risks associated with biometric data exposure and protect their users from potential security breaches (Ma & Fan, 2022).

### *3.5 Image Resolution and Forensic Tools Limitations*

The image resolution plays a crucial role in determining the accuracy of biometric data extraction. Higher-resolution images increase the risk of unintended fingerprint exposure, while lower-resolution images may reduce forensic reliability. However, the study does not provide a detailed examination of how resolution impacts fingerprint extraction accuracy, which could be an area for future research. Additionally, the practical examination of images using forensic tools was not part of this study, as it is not in the scope. Forensic tools may have inherent limitations, including variations in lighting, image compression artefacts, and inconsistencies in biometric feature recognition. These factors may affect the precision and reliability of extracted fingerprints, leading to potential false positives or incomplete data. A critical evaluation of these forensic tools is necessary to establish the robustness of biometric analysis in the real world.

## 4.0 Conclusion and Recommendation

### *4.1 Conclusion*

This study highlights the significant risks of biometric data exposure, specifically fingerprint patterns, through sharing photos on social media. The findings indicate that various camera poses, such as displaying two fingertips, a single thumb, or a full hand, increase the risk of unintentionally exposing sensitive biometric information. The poses featuring two fingers (middle and index) were found to be the most common and prone to biometric data extraction, followed by the thumb pose. The waving hand pose, though less frequent, also poses privacy risks. These risks are further amplified by high-resolution images, which can be processed to reveal intricate details of fingerprint patterns. The study's qualitative analysis shows that many social media users remain unaware of these risks, often prioritising aesthetics over security. The lack of educational content and security measures related to biometric data exposure exacerbates this oversight.

For those with a higher understanding of security, such as information security specialists, the concern about social media platforms' inadequate protection of biometric data was evident. They called for more robust privacy features, such as automatic detection of biometric data in images, enhanced privacy settings, and government regulations to ensure that platforms take responsibility for protecting biometric information.

### *4.2 Recommendations*

The study recommends the following measures to mitigate the risks associated with biometric data exposure through social media images:

1. User Education and Awareness: Social media platforms should provide clear educational content highlighting the risks of exposing biometric data through image posting, particularly focusing on how certain poses and gestures can unintentionally reveal sensitive information like fingerprints. Platforms can implement proactive notifications or pop-ups alerting users when their photos might expose biometric data, encouraging them to modify their images before posting.
2. Enhanced Privacy Features: Social media platforms should integrate advanced tools to automatically detect biometric data in images and prompt users to blur or mask sensitive parts of the photos before posting. Users should have more control over their photos' privacy settings, including options to selectively hide certain parts of their images (e.g., fingertips or faces).
3. Stronger Regulations: Governments should enforce regulations that require social media platforms to implement stronger biometric security measures to protect users from inadvertent data exposure. Legal frameworks should mandate transparency in how platforms handle biometric data and ensure that users have control over their biometric information.
4. Awareness Campaigns: Both social media platforms and governments should fund and

support campaigns to raise awareness about the risks of biometric data exposure on social media. Such campaigns can focus on the importance of photo privacy and the potential consequences of exposing personal biometric information.

5. Security Measures in Social Media Platforms: Security specialists emphasised the need for social media platforms to protect biometric data, similar to how they protect login credentials and accounts. Platforms should adopt stronger policies regarding the collection and use of biometric data.

## 5.0 Acknowledgement

The authors are grateful to their employers, the National Institute of Transport (NIT), and anonymous journal reviewers for their valuable suggestions on improving the quality of the article. Usual disclaimers apply. We, the authors, are so grateful to our employer, the National Institute of Transport (NIT), for the time and resources we acquired for the study.

## 6.0 Funding Statement

The study was self-financed by researchers.

## 7.0 References

Agarwal, A., Gupta, S. &Vashishath, M. (2024). Analysis of conventional and modern contrastEnhancement mechanisms. *Multimedia Tools and Applications.*https://doi.org/10.1007/s11042-024-18773-0

Alsmirat, M. A., Al-Alem, F., Al-Ayyoub, M., Jararweh, Y., B. (2018). Impact of digital Fingerprint photo quality on fingerprint recognition accuracy. *Multimedia Tools and Applications, 78* (3), 3649–3688. https://doi.org/10.1007/s11042-017-5537-5

Archana, R. &Jeevaraj, P. S. E. (2024). Deep learning models for digital photo processing: a Review. *Artificial Intelligence Review*, 57(1). https://doi.org/10.1007/s10462-023-10631-z

Archer, A. and Wildman, N. (2021). Internet Access as an Essential Social Good. In: Aarts, E., Fleuren, H., Sitskoorn, M. andWilthagen, T. (eds) *The New Common(pp. 29–33).*Springer, Cham. https://doi.org/10.1007/978-3-030-65355-2_4

Barth, S., De Jong, M. D., Junger, M., Hartel, P. H., & Roppelt, J. C. (2019). Putting the privacy Paradox to the test: Online privacy and security behaviours among users with technical knowledge, privacy awareness, and financial resources. *Telematics and Informatics*, *41*, 55-69. https://doi.org/10.1016/j.tele.2019.03.003

Baechler, S. (2020). Document Fraud: Will your identity be secure in the twenty-first century? *European Journal on Criminal Policy and Research, 26* (3), 379-398. https://doi.org/10.1007/s10610-020-09441-8

Cinar, A. C. and Kara, T. B. (2023). The current state and future of mobile security in light of the Recent mobile security threat reports. *Multimedia Tools and Applications, 82*(13), 20269-20281. https://doi.org/10.1007/s11042-023-14400-6

Dunsin, D., Ghanem, M. C., Ouazzane, K. and Vassilev, V. (2024). A comprehensive analysis of the Role of artificial intelligence and machine learning in modern digital forensics and incident response. Forensic Science International. *Digital Investigation, 48*, 301675.https://doi.org/10.1016/j.fsidi.2023.301675

Dwivedi, Y. K., Ismagilova, E., Rana, N. P. &Raman, R. (2021). Social Media Adoption, Usage and Impact in Business-To-Business (B2B) Context: A State-Of-The-Art Literature Review. *Information Systems Frontiers*, 25(3), 971–993. https://doi.org/10.1007/s10796-021-10106-y

Ghazinour, K. &Ponchak, J. (2017). Hidden privacy risks in sharing pictures on social media. *Procedia Computer Science, 113*, 267–272.https://doi.org/10.1016/j.procs.2017.08.367

Girod-Frais, A. and Bécue, A. (2021). Past, Present, and Future of the Forensic Use of Fingermark s. In: De Alcaraz-Fossoul, J. (eds) *Technologies for Fingermark Age Estimations: A Step Forwa* *rd (pp. 1-33).* Springer, Cham. https://doi.org/ 10.1007/978-3 030 69337 4_1

Ho, F. N., Ho-Dac, N. &Huang, J. S. (2023). The effects of privacy and data breaches on Consumers' online Self-Disclosure, protection behavior, and message valence. *SAGE Open, 13* (3). https://doi.org/10.1177/2158244023 1181395

Holub, P., Müller, H., Bíl, T., Pireddu, L., Plass, M., Prasser, F., Schlünder, I., Zatloukal, K., Nenutil, R. and Brázdil, T. (2023). Privacy risks of whole-slide photo sharing in digital pathology. *Nature Communications, 14* (1).https://doi.org /10.1038/s41467-023-37991-y

Kellman, P. J., Mnookin, J. L., Erlikhman, G., Garrigan, P., Ghose, T., Mettler, E., Charlton, D. &Dror, I. E. (2014). Forensic Comparison and Matching of Fingerprints: Using Quantitative Photo Measures for Estimating Error Rates through Understanding and Predicting Difficulty. *PloS One, 9*(5), e94617. https://doi.org/10.1371/journal.pone.009461 7

Kutschera, S. (2022). Incidental data: observation of privacy-compromising data on social media platforms. *International Cybersecurity Law Review, 4* (1), 91-114. https://doi.org/10.136 5/s43439-022-00071-w

Laas-Mikko, K., Kalvet, T., Derevski, R. and Tiits, M. (2022). Promises, Social, and Ethical Challenges with Biometrics in Remote Identity Onboarding. *In Advances in computer vision and pattern recognition* (pp. 437–462). https://doi.org/10.1007/978-3-030-87664-7_20

Ma, X. &Fan, X. (2022). A review of the studies on social media photos from the perspective of Information interaction. *Data and Information Management, 6* (1), 100004. https://doi.org/1 0.1016/j.dim.2022.100004

Maclean, J., Al-Saggaf, Y. &Hogg, R. (2022). Instagram photo sharing and its relationships with Social connectedness, loneliness, and Well-Being. *Social media + Society, 8*(2), 205630512211076. https://doi.org/10.1177/ 20563051221107650

Mundt, M., Ross, K. &Burnett, C. M. (2018). Scaling social movements through social media: The case of Black Lives Matter. *Social media + Society, 4* (4), 205630511880791. https://doi. org/10.1177/2056305118807911

Pomeroy, C., Bond, R. M., Mucha, P. J. and Cranmer, S. J. (2020). Dynamics of social network Emergence explains network evolutio n. *Scientific Reports, 10* (1). https://doi.org/10 .1038/s41598-020-78224-2

Singh, M., Singh, R., & Ross, A. (2019). A comprehensive overview of biometric fusion. *Information Fusion*, *52*, 187 205. https: //doi.org/10.1016/j.inffus.2018.12.003

Quach, S., Thaichon, P., Martin, K. D., Weaven, S. &Palmatier, R. W. (2022). Digital Technologies : tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*(6), 1299-1 323.https://doi.org/10.1007/s11747-022-00845-y

Ziegele, M. and Quiring, O. (2011). Privacy in social network sites. *In Springer eBooks* (pp. 175–89). https://doi.org/10.1007/978-3-642-21521-6_13