INVISIBLE BOUNDARIES: BALANCING IMAGE METADATA PRIVACY WITH FORENSIC IMPERATIVES

*Abdullah Golam (1), Umar Albalawi (2)**

(1) College of Computer and Information Science, King Saud University, Riyadh;
(2) College of Computing and Information Technology, University of Tabuk, Tabuk Saudi Arabia

* Corresponding Author, e-mail: ualbalwi@ut.edu.sa

Abstract: Metadata provides a wealth of information that is invaluable for digital forensic investigations, but it also poses significant privacy risks. The varying degrees of metadata retention across social media platforms have significant implications for digital forensic investigations. Metadata plays a crucial role in constructing timelines, verifying data authenticity, and providing evidence of interactions. In this research, we investigate the handling of EXIF metadata by various social media platforms and assess the implications for user privacy and digital forensic investigations. Our findings underscore the critical need for specialized software to manage and remove metadata from images uploaded to social media, preserving user privacy while retaining necessary data for legal and forensic purposes. To address these concerns, we implement a framework for encrypting and decrypting metadata, ensuring that sensitive information can be protected before images are uploaded to social media platforms. This research aims to encapsulate the findings and emphasize the need for balanced solutions that respect user privacy while supporting forensic investigations.

Key words: encrypted metadata, digital forensic, privacy vs usability, privacy policy, policy agreement,

1. INTRODUCTION

The world is developing rapidly. It is also moving at the same speed as the digital world. In the digital world, digital crimes are spreading. Therefore, countries are trying to develop a digital investigation department, which includes many investigators and forensic elements [1]. As the number of users of digital tools in the world is constantly increasing, countries are trying to put in place many monitoring and protection systems and programs to enhance privacy. The research community tries to provide approaches that ensure a balance between privacy and reducing penetration rates and digital crimes [2]. On the other hand, the rates of related digital crimes have increased in many areas. Therefore, the importance of digital investigation has increased. Countries and institutions are trying to design systems to manage digital investigations, including

building the capabilities of investigators and forensic medicine in processing metadata, image files, etc. [3].

Metadata is data that provides information about other data. Information that is generated as you use the technology [4]. Metadata can be used with many items, such as criminal cases, to make a multimedia database of data available to investigators that is easy to use. Image metadata plays a crucial role in criminal investigations. This embedded data, often known as EXIF (Exchangeable Image File Format) data [5], contains various details about the image, including data and time, geolocation, camera information, technical details, and a thumbnail. Thus, these metadata help in confirming or disputing by establishing the exact time an image was taken and can track movements or place individuals at crime scenes. In addition, unique identifiers in metadata can link photos to specific devices, which can be linked to suspects.

2. RESEARCH PROBLEM AND CONTRIBUTIONS

2.1. Metadata: privacy concerns

Metadata may not disclose the content of all communications, but it can provide a highly detailed portrait of our lives. In fact, analyzing patterns in a vast collection of metadata and correlating them with real-world events is often much easier than conducting a semantic analysis of all someone's emails and phone calls [6]. Mining metadata can not only expose sensitive information about the past, but it can also even allow an observer to predict future actions, location, recipient or sender of an email, and Internet purchases. In addition, privacy may affect the unconscious dissemination of important metadata from users, especially in light of the spread of social media, and users' desire to upload many images. These images are associated with metadata that is important to users. Therefore, users and others should be supported with specialized software to ensure the removal of metadata contained in images and files uploaded via social media applications, with the need to keep an original copy to preserve this data [7].

2.2. Importance of metadata in a digital forensic investigation

Digital forensics is one of the emerging elements in light of digital crimes and digital investigations. It relies on metadata as one of the sources of evidence, data collection, and report writing. Also, digital forensics considers digital sources, including metadata, images, and devices such as mobile phones, computers, and various applications, to be sources that contain useful data that can be used in digital investigations, can be verified, and can be stored for long periods of time for reference. This requires the ability of forensic medicine to extract this data from its sources while maintaining its privacy [8].

Digital investigations relate to a variety of metadata. Therefore, investigators and forensic elements are in urgent need of programs and mechanisms that support them in dealing with metadata, as follows:

- The temporal and spatial details are associated with the metadata and how to verify the validity of the data.
- How to verify that metadata has not been interfered with.
- How to verify that the data has not been deleted.

In addition, metadata also provides the investigator with many advantages, including file tracking and management and file creation details. Thus, metadata may be useful in resolving legal disputes and achieving justice. Nevertheless, metadata can support in providing communication or cooperation evidence between groups of people because some people are not concerned about which type of information is gathered within their document [9]. As a result, the digital forensics investigator can access this hidden document information [10].

2.3. Novel contributions of this paper

As discussed above, metadata provides a wealth of data and evidence for investigators and forensic personnel. It helps in constructing the chronological sequence of events and is directed towards understanding the relationships between those events and the people in them. The metadata also provides the possibility for investigators to write various reports. On the other hand, metadata also provides forensic information with more accurate details and can be shared between investigations and forensic authorities. The proposed system preserves the privacy of users on the Internet, so image metadata is encrypted and can be referred to in cases of digital investigation if there is a need to show evidence that condemns or exonerates the user. In this paper, a novel mechanism is proposed for image metadata that achieves criminal justice and preserves the privacy of metadata. The unique contributions of this research are as follows:

1. An investigation of the image metadate in social media platforms.
2. A symmetric encryption protocol to encrypt metadata.

3. RELATED WORKS

The process of uploading images on social media is related to users' unawareness of the metadata about images and devices used in photography is indicated in [11]. Social media companies may attempt to illegally access and use this data. The research proposes a mechanism that performs and allows removing all metadata associated with images before uploading them. This mechanism also supports users to make a copy of the images without metadata about the users and their devices, so the images can be uploaded without concern. The way how the courts view metadata and the need for the investigator to be familiar with metadata files and how to deal with them when presented as arguments and evidence to the court is emphasized in [12]. The authors in [13] classify digital forensics as one of the scientific and legal branches associated with the collection, creation, and analysis of databases. They mainly focus on the significance of metadata in database forensics. A framework has been proposed to perform a forensic investigation of the database by producing its metadata documents and files independently of the DBMS framework utilized. They likewise aim to produce digital evidence against lawbreakers for introducing it in the court of law as to who, when, why, what, how, and where did the deceitful exchange happen.

Mobile phones are a source of digital forensics in many disputes and issues. And digital forensics needs some tools that give a clear view of the files, data, and programs included in cell phones as data sources. The framework that investigates the possible image and file system types is proposed in [14]. The outcomes show that the tool can

open the image and show the files that are gathered based on the predetermined file framework types that have been recorded. Based on the importance of digital forensics in digital crimes, which began to increase continuously, the duties and responsibilities of forensic medicine are related to participation in digital investigations.

A novel method for safeguarding personal privacy in online content is introduced in [15]. The approach focuses on preferential selective encryption, which allows users to encrypt specific elements of their media posts. It highlights the growing need for enhanced privacy measures in the digital age and demonstrates how this selective encryption method can be effectively implemented to achieve this goal.

The research [16] presents a comprehensive framework designed to conduct computer forensics investigations that are both efficient and compliant with legal privacy standards. The framework aims to balance the need for thorough digital investigations with the necessity of preserving the privacy rights of the individuals involved. The authors [17] explore the challenges of protecting privacy in an era where photos taken by others can inadvertently reveal your location and activities. The authors propose a large-scale, location-aware privacy protection system designed to address the complexities of multi-party image sharing. The critical issue of protecting privacy in the context of image provenance is addressed in [18].

The study [19] introduces LocGuard, a tool designed to protect users' location privacy when sharing images online. The system focuses on preventing the unintentional disclosure of location data embedded in images, which can lead to privacy breaches. LocGuard works by analyzing and removing or obfuscating sensitive location information before images are shared, ensuring that users can enjoy the benefits of image sharing without compromising their privacy.

A novel application designed to improve digital forensics investigations is presented in [20]. This app focuses on extracting and analyzing text embedded within images, providing investigators with critical insights that may otherwise go unnoticed. By leveraging advanced image processing and text recognition techniques, the app helps uncover hidden or obscured information, enhancing the ability to gather evidence from digital images. A work by Bharati all [21] focuses on Image Provenance Analysis where the task is to study relationships across manipulated versions of images that have some correspondence in terms of content. The most important aim is to establish the sequence of transformations that have operated on an image by identifying its edit history. The authors present a deep learning model which can learn embedding transformation aware-representations, representations that encode both its content and how it has been edited. A thorough search was conducted in digital forensics investigation jurispudence. It explores the legal framework surrounding digital forensic investigations, focusing on challenges related to ensuring evidence is authentic, accurate, complete, and compelling enough to be admissible in court. it addresses both the legal and technical factors necessary to resolve these challenges and proposes ways to harmonize them for effective forensic application.

In terms of of next genration digital forensic investigation a model has been prposed in [23]. The model establishes a structured framework that supports investigators throughout the forensic process. It aims to collect a greater volume of evidence during incident response compared to traditional investigation methods. In addition, it shortens

analysis time and enhances privacy protection for suspects by using selective content imaging, focusing only on relevant data.

4. INVESTIGATING THE METADATA IN SOCIAL MEDIA PLATFORMS: THE NEED FOR BOTH USIBILITY AND PRIVACY

Image metadata on social media platforms typically includes sensitive information such as GPS location [24, 25]. As a part of this research, we aim to evaluate how various social media platforms handle and preserve EXIF metadata. By using Algorithm 1, EXIF tags are extracted as listed in Table 1. We capture a series of photos using multiple mobile devices with various operating systems, including Apple iOS and Android. Each photo is examined to extract and document its EXIF metadata. Then, these photos are uploaded to several social media applications: Facebook, Snapchat, Instagram, X, and TikTok. After the upload process, the photos are downloaded from the social media platforms to assess any changes to the metadata, as shown in figure 1.

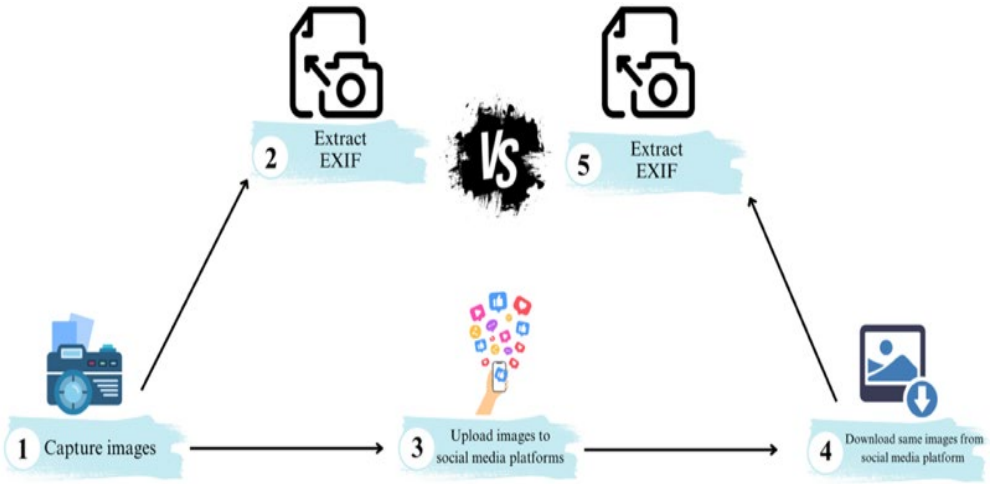


Figure 1. Proposed framework to investigate the metadata in social media platforms

The objective of this experiment is to analyze how different social media platforms handle the EXIF metadata of photos uploaded from various mobile devices. After downloading the uploaded photos, we extract the EXIF metadata and compare it with the original data to evaluate the modifications made by the platforms. Appendix A shows the original photo metadata before uploading it. The result of the comparison is shown in Figure 2. Facebook and TikTok remove all EXIF labels and their corresponding data. Instagram, Snapchat, and X retain 90%, 50%, and 40% of the EXIF labels and their corresponding data, respectively. X and Snapchat remove sensitive labels such as GPS and detailed camera settings.

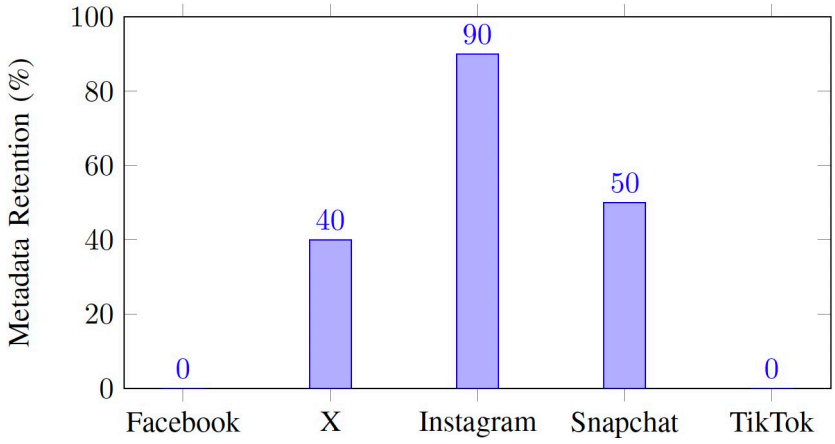


Figure 2. Metadata retention comparison among selected social media platforms

5. THE PROPOSED FRAMEWORK: ACHIEVING CRIMINAL JUSTICE AND PRESERVING THE PRIVACY OF METADATA

The proposed system, as illustrated in figure 3, preserves the privacy of users on the Internet so that the data that belongs to metadata is hidden and can be referred to in cases of digital investigation if there is a need to show evidence that condemns or exonerates the user. The proposed method ensures secure access to metadata, which allows only the owner of the assets to access the data it contains.

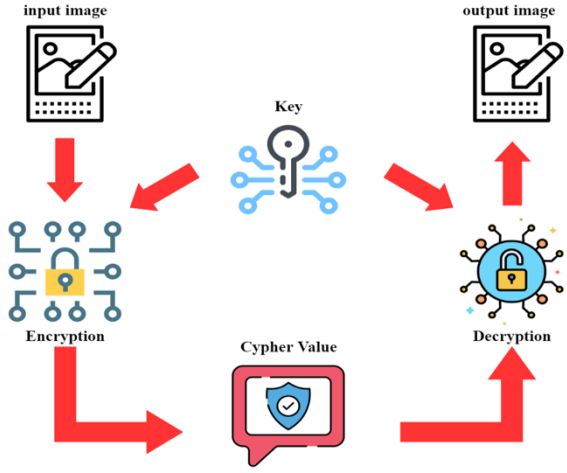


Figure 3. Proposed framework

Table 1. EXIF tag names

Tag ID	Tag Name	Tag ID	Tag Name
1	GPS Latitude Ref	2	GPS Latitude
3	GPS Longitude Ref	4	GPS Longitude
5	GPS Altitude Ref	6	GPS Altitude
7	GPS Time Stamp	12	GPS SpeedRef
13	GPS Speed	16	GPS Img Direction Ref
17	GPS Img Direction	23	GPS Dest Bearing Ref
24	GPS Dest Bearing	29	GPS Date Stamp
31	GPS Differential	256	Image Width
257	Image Length	258	Bits Per Sample
262	Color Space	264	Document Name
270	ImageDescription	274	Orientation
282	X Resolution	283	Y Resolution
296	Resolution Unit	305	Software
306	Date and Time	316	Host Computer
34665	EXIF Offset	34850	ExposureProgram
34853	GPSInfo	34855	ISOSpeedRatings
34864	SensitivityType	34866	Extended ISO
36864	EXIF Version	36867	DateTimeOriginal
36868	DateTimeDigitized	36880	TimeZoneOffset
36881	TimeZone	36882	TimeZoneDst
37121	ComponentsConfiguration	37377	ShutterSpeedValue
37378	ApertureValue	37379	BrightnessValue
37380	ExposureBiasValue	37381	MaxApertureValue
37383	MeteringMode	37384	LightSource
37385	Flash	37386	FocalLength
37396	SubjectArea	37500	MakerNote
37510	UserComment	37520	SubSecTime
37521	SubSecTimeOriginal	37522	SubSecTimeDigitized
37724	ImageUniqueID	37888	Temperature
40960	FlashpixVersion	40961	Color Space
40962	Pixel X Dimension	40963	Pixel Y Dimension
40965	InteroperabilityOffset	41495	Sensing Method
41729	SceneType	41986	ExposureMode
41987	WhiteBalance	41988	DigitalZoomRatio
41989	FocalLengthIn35mmFilm	41990	SceneCaptureType
42034	LensSpecification	42035	LensMake
42036	LensModel	42080	Gapless Playback
271	Make	272	Model
531	YCbCrPositioning	33434	ExposureTime
33437	FNumber	544	Unknown Tag 544
545	Unknown Tag 545	546	Unknown Tag 546
547	Unknown Tag 547	548	Unknown Tag 548
549	Unknown Tag 549		

The proposed architecture contains three steps: metadata label extraction and classification, key generation, and encryption. These metadata, typically generated by cameras and other recording devices, contains technical details about an image and how it is captured, including capture time, GPS location, and camera model.

The first step is to extract metadata labels and their values. The proposed algorithm, as illustrated in algorithm 1, is designed to retrieve and display the Exchangeable Image File Format (EXIF) data embedded in an image file. EXIF data includes metadata such as the camera settings, the date and time the photo was taken, and other details about the image file.

ALGORITHM 1: EXIF EXTRACTION

```
1  Open image at image_path
2  Check exif data
3  If exif data exist then
4      For each tag_id, value in exif data do
5          Tag name= get tag name from tag_id
6          Print tag_id : value
7  Else
8      Print "no exif data found"
```

The second step is to generate a key. The proposed method is essential for securely generating cryptographic keys from passwords, which can then be used for encryption and decryption. By using a salt and a high number of iterations, the security of the key derivation process is significantly enhanced, making it resistant to attacks, as shown in Table 2. The encryption algorithm utilizes a password-based key derivation function (PBKDF2) to generate a secure key from a user-provided password and a randomly generated salt [23]. This key is then used to encrypt the metadata using the Fernet symmetric encryption scheme. The decryption algorithm reverses this process, allowing authorized users to decrypt and access the metadata when necessary. These algorithms provide a robust mechanism for protecting metadata while maintaining its availability for legitimate forensic and investigative purposes.

Table 2. Set algorithm and parameters

Parameter	***Specification***
Encryption Algorithm	*Fernet symmetric scheme*
Algorithm	*SHA256*
Length	*32 bytes*
Key-derivation	*PBKDF2*
Iterations	*100000*
Backend	*Default cryptographic*
Encode	*URL-safe based64*

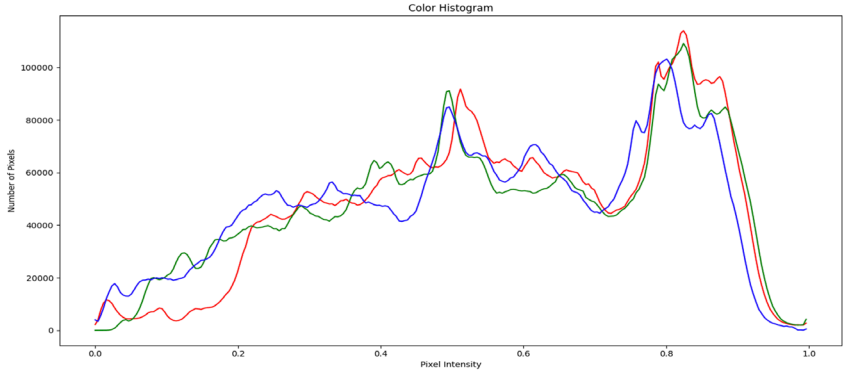
The experiment results, as shown in detail in Table 3, demonstrate the changes between the original image and the image with the encrypted metadata in terms of size, entropy, and noise level. The image entropy is a representation of an image where each

pixel value reflects the amount of local randomness or disorder (entropy) within neighborhood around that pixel. Entropy in this context is a statistical measure used in information theory to quantify the unpredictability of information content [24].

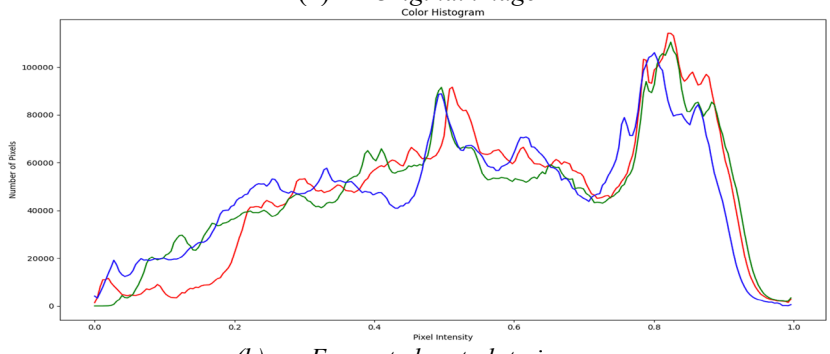
Table 3. Comparison between original image and encrypted-metadata image

Characteristics	***Original Image***	***Encrypted-Metadata Image***
resolution	*4032x3024 pixels*	*4032x3024 pixels*
Size	*3.8 MB*	*1.06 MB*
Entropy	*5.37*	*5.37*
Noise level	*0.0323*	*0.31*

Figure 4 represents the distribution of pixel intensities in the red, green, and blue channels of the images. The noise level is an estimate of the amount of noise present in an image. Noise can be introduced during image capture, transmission, or processing, and it often manifests as random variations in pixel intensity. In the script, the noise level is calculated using the Sobel filter, which measures the mean gradient magnitude of the image [25]. Higher noise levels indicate more variations in pixel intensity, which can suggest higher noise. Both images have low and similar noise levels.



(a) *Original image*



(b) Encrypted-metadata image

Figure 4. The distribution of pixel intensities

6. CONCLUSION

The retention of metadata by social media platforms raises substantial privacy concerns. Users often unknowingly upload images with embedded metadata that can reveal their location, device information, and other personal details. The retention of metadata by social media platforms raises substantial privacy concerns. Users often unknowingly upload images with embedded metadata that can reveal their location, device information, and other personal details. Our study reveals the diverse approaches taken by social media platforms in handling metadata and highlights the need for tools and regulations that protect user privacy while preserving essential forensic data. By addressing these challenges, we can enhance both user privacy and the effectiveness of digital forensic investigations, contributing to a safer and more transparent digital environment. The proposed system underscores the necessity for users to have access to tools that can remove metadata before uploading images to social media, ensuring their privacy is protected. Our research contributes to the field of digital forensics by highlighting the importance of metadata in investigations and the challenges posed by its removal. We advocate for the development of forensic tools that can extract and preserve metadata from images before they are uploaded to social media platforms. Such tools would ensure that investigators have access to crucial metadata while still protecting user privacy. Additionally, our findings support the need for legal frameworks that address the handling of metadata by social media platforms. Clear regulations can ensure that metadata is managed in a way that balances privacy with the needs of digital forensic investigations.

REFERENCES

[1] Khalaf, R. S., Varol, A. Digital forensics: focusing on image forensics. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*, Barcelos, Portugal, June 2019, pp.1-5. DOI: 10.1109/ISDFS.2019.8757557.

[2] Gupta, A. Privacy preserving efficient digital forensic investigation framework. *2013 Sixth International Conference on Contemporary Computing (IC3)*, Noida, India, August 2013, pp. 387-392. DOI: 10.1109/IC3.2013.6612225.

[3] Zhou, G., Lv, D. An overview of digital watermarking in image forensics. *2011 Fourth International Joint Conference on Computational Sciences and Optimization*, Kunming and Lijiang City, China, April 2011, pp. 332-335. DOI: 10.1109/CSO.2011.85.

[4] Chen, S., Jin, T., Xia, Y., Li, X. Metadata and image features co-aware semi-supervised vertical federated. *IEEE Transaction on Vehicular Technology,* vol.73, no.2, 2024, pp. 2520-2532. DOI: 10.1109/TVT.2023.3313593

[5] Fan, J, Chen, T., Kot, A. C. EXIF-white balance recognition from image forensic analysis. *Multidimensional System and Signal Processing,* vol.28, 2017, pp. 795-815. DOI: 10.1007/s11045-015-0377-9.

[6] Orescanin, D., Hlupic, T, Vrdoljak, B. Managing personal identifiable information in data lakes. *IEEE Access,* vol.12, 2024, pp. 32164-32180. DOI: 10.1109/ACCESS.2024.3365042

[7] Jia, R., Zhang, J., Lin, Y. Machine learning security defense algorithms based on metadata correlation features. *Computers, Materials & Continua,* vol.78, no.2, 2024, pp. 1385-1401. DOI: 10.32604/cmc.2024.044149

[8] Tuharea, I. R., Luthfi, A., Ramadani, E. Enhancing digital forensic investigation: a focus on compact electronic devices and social media metadata. *Journal of Information Systems and Informatics,* vol.5, no.4, 2023, pp. 2391-2418. DOI: 10.51519/journalisi.v5i4.594

[9] Oh, J., Lee, S., Hwang, H. Forensic detection of timestamp manipulation for digital forensic investigation. *IEEE Access,* vol.12, 2024, pp. 72544-72565. DOI: 10.1109/ACCESS.2024.3395644

[10] Oh, J., Lee, S., Hwang, H. Forensic recovery of file system metadata for digital forensic investigation. *IEEE Access,* vol.10, 2022, pp. 111591-111606. DOI: 10.1109/ACCESS.2022.3213030

[11] Tayeb, S., week, A., Yee, J., Carrera, M., Edwards, K., Garcia, V. M., Zhan, J., Pirouz, M. Toward metadata removal to preserve privacy of social media users. *2018 IEEE 8th Annual Computation and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, January 2018, pp. 287-293. DOI: 10.1109/CCWC.2018.8301741

[12] Alanazi, F., Jones, A. The value of metadata in digital forensics. *2015 European Intelligence and Security Informatics Conference*, Manchester, UK, September 2015, pp. 182-182. DOI: 10.1109/EISIC.2015.26

[13] Khanuja, H., Suratkar, S. S. Role of metadata in forensic analysis of database attacks. *2014 IEEE International Advance Computing Conference (IACC)*, Gurgaon, India, February 2014, pp. 457-462. DOI: 10.1109/IAdCC.2014.6779367

[14] Senturk, S., Apaydin, T., Yasar, H. Image and file system support framework for a digital mobile forensics software. *2020 Turkish National Software Engineering Symposium (UYMS)*, Istanbul, Turkey, October 2020, pp. 1-3. DOI: 10.1109/UYMS50627.2020.9247055

[15] Shetty, N. P., Muniyal, B., Priyanshu, A., Kumar, D., Maben L. M., Agrawal, Y. Protecting your online persona: a preferential selective encryption approach for enhanced privacy in tweets, images, memes, and metadata. *IEEE Access,* vol. 12, 2024, pp. 86403-86424. DOI: 10.1109/ACCESS.2024.3415663

[16] Halboob, W., Almuhtadi, J. Computer forensics framework for efficient and lawful privacy-preserved investigation. *Computer Systems Science & Engineering*, vol. 45, no. 2, 2023, pp. 2071-2092. DOI: 10.32604/csse.2023.024110

[17] Morris, J., Newman, S., Palaniappan, K., Fan, J., Lin, D. "Do you know you are tracked by photos that you didn't take": large-scale location-aware multi-party image privacy protection. *Computers, IEEE transactions on Dependable and Secure Computing,* vol. 20, no. 1, 2021, pp. 301-312. DOI: 10.1109/TDSC.2021.3132230

[18] Fotos, N., Delgado, J. Ensuring privacy in provenance information for image. *2023 24th International Conference on Digital Signal Processing (DSP)*, Rhodes, Greece, June 2023, pp. 1-5. DOI: 10.1109/DSP58604.2023.10167902

[19] Ma, W., Wang, D., Chen, C., Wen, S., Fei, G., Xiang, Y. LocGuard: a location privacy defender for image sharing. *IEEE Transactions on dependable and Secure Computing,* 2024, DOI: 10.1109/TDSC.2024.3376929

[20] Bandal, S., Rath, S. Unveiling digital secrets: an image text vision app for enhanced digital forensics investigations. *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, San Antonio, TX, USA, April 2024 Unveiling, pp. 1-6. DOI: 10.1109/ISDFS60797.2024.10527293

[21] Bharati, A., Moreira, D., Flynn, P., Rocha, A., Bowyer, K., Scheirer, W. Learning transformation-aware embeddings for image forensics. *arXiv preprint arXiv:2001,* 2020. DOI: 10.48550/arXiv.2001.04547

[22] Yeboah-Ofori, A., Brown, A. D. Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences,* vol. 6, 2020, pp. 1-8, DOI: 10.24966/flis-733x/100045

[23] Thakar, A. A., Kumar, K., Patel, B. Next generation digital forensic investigation model (NGDFIM) enhanced, time reducing and comprehensive framework. *Journal of Physics*, vol. 1767, no. 1, 2021, DOI: 10.1088/1742-6596/1767/1/012054

[24] Hidayati, S. C., Thalib, M. R. F., Munif, A. The Influence of User Profile and Post Metadata on the Popularity of Image-Based Social Media: A Data Perspective. *2024 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, Osaka, Japan, February 2024, pp. 806-811. DOI: 10.1109/ICAIIC60209.2024.10463510

[25] Zaeem, R. N., Anya, S., Issa, A., Nimergood, J., Rogers, I., Shah, V., Barber, K. S. PrivacyCheck's machine learning to digest privacy policies: competitor analysis and usage patterns. *2020 IEEE/WIC/ACM International Joint Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, Melbourne, Australia, December 2020, pp. 291-298. DOI: 10.1109/WIIAT50758.2020.00042

Information about the authors:

Abdullah Golam – received his master's degree in information security from University of Tabuk, in 2020. He is currently a Ph.D. Student in Computer Science, King Saud University, Riyadh, KSA.

Umar Albalawi – received his Ph.D. degree in Computer Science and Engineering from the University of North Texas in 2016, and master's degree in computer science from Texas A&M University, in 2013. He is currently an Associate Professor in the Department of Information Technology, Faculty of Computing and Information Technology, University of Tabuk, Saudi Arabia. His research interests focus on Security and Privacy in Internet of Things (IoT), Network Security, and Cryptography. He served on the Editorial Boards of Several peer-reviewed international journals and magazine.

Manuscript received on 30 August 2024