Securing Image Metadata using Advanced Encryption Standard

MSc Internship
Cybersecurity

Rohan Bhangale
Student ID: 18147119

School of Computing
National College of Ireland

Supervisor: Ben Fletcher

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Rohan Bhangale
Student ID:	18147119
Programme:	Cybersecurity
Year:	2019
Module:	MSc Internship
Supervisor:	Ben Fletcher
Submission Due Date:	12/12/2019
Project Title:	Securing Image Metadata using Advanced Encryption Standard
Word Count:	4088
Page Count:	18

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

I agree to an electronic copy of my thesis being made publicly available on NORMA the National College of Ireland's Institutional Repository for consultation.

Signature:	
Date:	2nd February 2020

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	☐
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	☐
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	☐

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing Image Metadata using Advanced Encryption Standard

Rohan Bhangale
18147119

Abstract

The fast-growing internet brought an increase in the number of online content sharing platforms, as well as the growing size of the user base. This growth has led to a plethora of challenges for such as privacy and security of the individual online. The work presented in this report focuses on the particular problem of image sharing platforms revolving around image metadata, for which an information leakage may help adversaries to track user's activities or may put the businesses at risk of reputation and financial losses. The aim is to improve the security of image metadata for images shared on social media or other types of media platforms, knowingly or unknowingly by users. In this report, we have proposed a design in which the image metadata is secured by applying Advanced Encryption Standard or AES-128 bits algorithm. The report also discusses the details of the proposed model and the potential challenges of unsecured metadata. The proposed design secures the image metadata through encryption and prevents its misuse, hence protecting the user's privacy.

Keywords - AES, Image Metadata, Privacy, EXIF,JPEG.

1 Introduction

The number of individuals using the internet has seen tremendous growth recently, according to the World Internet Stats of 2019, 58.8% of the human population. [1]. The significant consequence of this increase is the arisen online commerce and content sharing culture which comes with security issues that range from individual to organisation's privacy and safety. Over the past decades, technology vendors from industry and academia were focusing their efforts on exploiting the advances in technology with super-fast computers, data communication and smartphones to make the existing internet environment more efficient. Most of these innovations were driven by human convenience with not much attention to the security aspect in mind. Within the last few years, digital cameras have become more and more popular and sharing the captured images online. Businesses and individuals now use images for engaging with the audience. Users are not aware of the information shared along with the image such as geolocation and device information .Which can pose a privacy issue disclosing private information of an individual or business such as address and manufacturer model of users device, which helps an attacker in information gathering over the victim.

[1]Internet World Stats: `https://www.internetworldstats.com/emarketing.htm`

In the past decade, logs for numerous such events which demonstrated the privacy implications of exposed metadata in terms of user's location. From events such as Hollywood celebrities unknowingly giving up their home addresses which were then exploited by burglars for carrying out thefts. Furthermore, in 2017 four U.S. Army Apache helicopters were pinned down by Iraqi insurgents with the help of metadata holding co-ordinates, the metadata was leaked by web-published images by unaware soldiers[2].Also, the documents published by Whistleblower Edward Snowden shows the classified nationwide surveillance, i.e. XKeyscore program which used metadata to collect information on users[3]. Image Metadata is a double-sided sword, while it is used for protecting copyrights of the image and at the same time exposing information. However, it is important to protect metadata of these both kinds.

Much research from the past focus on securing image metadata by creating identical image files free from metadata [1], privacy settings configuration on content-sharing sites [2], classifying access to group-based models [3], stripping data or implementation of privacy settings which are based on contemporary issues.

The model proposed in this report enables users to share metadata without leaking their personal information online using AES-128 bits algorithm. AES is a symmetric key algorithm which means that a shared key is used for encryption and decryption of the data. The motive of this research is to blend image metadata stripping and embedding the encrypted metadata in the image. The report seeks to address the research question, *Can the use of Advanced Encryption Standard (AES)-128 bits algorithm help in securing information leakage caused by image metadata?*

The structure of the report is as follows, Section 1:Introduction focuses on the motivation and justification behind securing image metadata. In Section 2: Related Work provides the past researches and their findings on the topic of image metadata. In Section 3, the proposed model is outlined with the justifications leveraging from the literature. Section 4, illustrates the architecture underlying the implementation.Further Section 5: implementation shows the implementation of the proposed model with the help of algorithms and tools available. Section 6, Evaluation, discusses the results from the test cases.Section 7, finally discusses the conclusion and possible future works

2 Related Work

2.1 Previous approaches for securing Image Metadata

Metadata summarises information about the data. The author [4] gives a detailed overview of a digital image's lifecycle and concludes with the importance of metadata the digital image creation processing, indexing, and distribution. Furthermore, the EXIF standard for digital camera still images discusses how it supports technological advancement by adding metadata identifiers, recently added as GPS and Printer output [5]. Unsecure metadata is a rapidly increasing threat towards privacy against the exposure of attributes such as geolocation, model/manufacturer and other metadata. Combined with the easy-to-use smartphone devices, location services such as GPS and the proliferation of high-speed internet technologies, gave rise to a culture of spontaneous image sharing with an enabled feature for geotagging. Geotagging marks the location of digital photos,

[2]Geotagging poses security risks: `https://www.army.mil/article/75165/Geotagging_poses_security_risks`

[3]XKeyscore: `https://en.wikipedia.org/wiki/XKeyscore`

which can be compromised and can pose a threat to the privacy of individuals. Creating a significant range of challenges to their associated environments (family, friends, and work organization), posing a threat against CIA triad. Research has been conducted to secure metadata, numerous approaches are being proposed viz. configuring access control lists, defining content-based policies and access levels, removing metadata, separating images using applications, creating privacy zones, and educating users about user awareness [1]. A substantial amount of research has been carried out in the domain of privacy settings and the application of access control based on the role of the audience, which users can easily implement. Access to photos is determined by rules and policies are defined by users. The audience is classified in Policies based on the group, location, and role in addition to providing the audience with access to complete or partial metadata[1]. Besides, two models of access control for uploading images, hierarchical and group-based, were proposed to provide a broad set of privacy protection [1]. Hierarchical is a model of access control based on lattice, structured in a way that restricts the metadata accessible by the audience. Group-based model operates on a group of audience with the help of predefined privacy settings [4]. Another study [2] uses a simulation model, that helps users automate privacy policies for uploaded images. Depending on their content and metadata, photos are classified on the basis of their content and metadata, and then privacy policy is evaluated and projected for the classification. Such techniques allow secure sharing of accurate metadata, but hackers have become more sophisticated and have several ways to gain access to user profile on content-sharing sites, which is still a threat. Friedland et al. . [6] suggested a phrase cybercasing, i.e. determining a stranger's precise location from the individual's shared information. Author also addresses situations from the viewpoint of potential attackers on details that can be explored with unsafe metadata from images. The study further emphasizes the importance in order to avoid and minimize such an assault by knowledge and user education. Work has also been involved in the development of tools for removing and modifying metadata. Henne, Benjamin et al. [7] suggested developing smart privacy zones that would exploit the location tracking capabilities in which users would like to protect their privacy.

Henne et al [8] introduces a Google Chrome browser extension to help users access and control metadata for images. As such, the study conducted by Sarvas et al. [9] facilitates metadata management by creating useful semantic metadata by interacting with the user to confirm the metadata provided by the device at the time of image capture. Nonetheless, some things are not dealt with wisely Lepsoy et al. [1] work focuses on descriptive metadata contained in the EXIF data and flagging for stripping and generating a metadata-free image, as well as on metadata editing tools such as Exiftool, which is helpful but does not serve the end goal of being easily accessible to end-users.The above studies have so far concluded on the need for user awareness of geolocation marking, which is by default setting. We investigated the established approaches to securing metadata in this study and concluded that a technical solution needs to address the problem. Delgado et al. [4] indicate the need to encrypt metadata in their future work. Some encryption standards are discussed in the next section to protect metadata through encryption

2.2 Study of Encryption Algorithm

Most scientists are attracted to cryptography because, due to the widespread use and exchange of information on the Internet, it is important to protect information from hacking and interference [10]. The most important part of the image is the metadata containing information such as image colour, texture and the point of interest of this geolocation of research and the device manufacturer/model used.Wijayanto et al. demonstrate the use of a cryptographic technique to encrypt the metadata of EXIF(eXchangeable Image File Format) in an image file. The Japan Electronic Industries Development Association (JEIDA) created EXIF as a camera image format in accordance with ISO Standard 12234-1. It also talks about the important role of photo protection when posting online. As proposed in future works using various authentication strategies to protect the picture and different types of metadata [11]. Cryptography has a set of goals in terms of confidentiality availability and integrity to ensure information security [10]. Cryptographic algorithms are known as symmetric(Single secret key) and asymmetric(public key/private key) algorithms on the basis of the number of keys used in encryption / decryption [12]. The weakness of the symmetric key algorithm is the key sharing between the sender and the receiver, on the other hand, due to the need for more processing power, asymmetric key algorithms are approximately 1000 times slower than symmetric key algorithms [12] [10].. Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES) and Blowfish are the most widely used symmetric key algorithms. DES has been suggested as the first standard for encryption of NIST (National Standards and Technology Institute). It was developed around 1974 by IBM and adopted as a standard in 1997, it has 56-bit key length and 64-bit block size [13] [14].DES is vulnerable to key attack DES functions [13] were improved with variants such as 3DES and AES. Published in 1998, 3DES gets its name by applying DES thrice to each data block, unlike DES, 3DES is feasible when it comes to a brute-force attack, but 3DES is slower than DES due to the three-time DES ciphering [10]. Conferring to et al [10] Blowfish was established by Bruce Schneier in 1993. Blowfish is a 64-bit block cipher capable of taking 32-bit to 448-bit variable-length key; 128-bit default. To replace DES, it was developed. AES is a round-based, symmetric block algorithm based on cipher / decipher. It is specified for a block size of 128-bit and key lengths of 128, 192 and 256-bit. Depending on the key length, these AES variants are called AES-128, AES-192, and AES-256 [15]. The performance analysis of these cryptographic cyphers was performed on the basis of parameters such as encryption, decryption time, memory usage, battery/power consumption in various environments such as cloud and java simulations [14] [12] [10]. The study shows that AES used less time to execute, Blowfish used less memory [14], and DES took less time to encrypt. Every encryption strategy has its pros and cons. . It was concluded that Blowfish was best against attacks using entropy parameters to test DES, 3DES, AES and Blowfish. However, if the main factor in the application is cryptographic strength, then AES is best suited [14]. Every encryption technique has its pros and cons. To apply a suitable cryptography algorithm to implementation, an understanding of the performance, strength and weakness of the algorithms is required [12].

3 Methodology

Authors [4] and [3] explain about the risk of losing information due to sharing of the images on the internet increases and discuss the format JPEG which is the most widely used image format through which user's privacy may be compromised by the spillage of the details from the metadata especially GPS location. Further, [3] have discussed the misuse of the metadata through social networks such as youtube and facebook. A script was written where youtube videos with geotagging (GPS location) were extracted further to trace the video owner's home location. Facebook to prevent metadata misuse began to trim the data from the images which raise numerous problems. Few of them were related to copyright issue and important information about image properties. [4] suggested an approach using XACML policy which uses access control and encryption to protect the privacy but the drawbacks of these are it is not standardised currently in the industry and has to be specified in different file format. For this practice for striping metadata, facebook was sued by a german photographer[4] and lost the legal battle against the german as facebook was found in breach of the German Copyright Act

Researchers at the University of Nevada [1] have developed an algorithm that allows stripping of metadata partially or fully so as to protect the privacy of the users present on social media. [3] explains the odds of removing the metadata from the images and one such issue is loss of intellectual property and copyrights. They propose two different models for access control on the metadata, cause media services have various requirements and needs so it's hard to include everything under a single model. The author also mentions about EXIF data and how it can be exploited by engineers for commercial purposes and by adversaries to cyber-bully and discusses the use of Exiftool to parse metadata from image, video and audio files. [11] Proposed encryption of the EXIF data using the XTEA 64 bit encryption algorithm with End Of File embedding methodology. The drawback of this system is that the image file lost 25.15% of pixel data which doesn't seem to affect much but still heavy image files may get affected by it.

As we can see from the above that study that securing the image metadata is crucial for protecting the privacy of the user, which motivated us to develop the method through which we extract, encrypt and embed the important tags in image metadata so as to make it secure. For this proposed method, we haven't made use of steganography or complex policies for access control hence, the algorithm is efficient in terms of time, resource and cost. This method helps to conceal the information metadata by using AES-128 bits algorithm with no extra action. Hence, it's simplified and optimised.

AES Algorithm: Advanced Encryption Standard (AES) [16] identify the Rijndael algorithm which is a symmetric block cipher that takes the input of 128 bits data block and using the key of size 128 bits, 196 bits and 256 bits encrypts the block. The symmetric key block means that to perform the operation of encryption and decryption it uses the same key. AES has three flavors “AES-128”, “AES-192” and “AES-256” that are based on its three different key sizes mentioned above.

The model is divided into 3 phases, Key Derivation, Encryption and Decryption. The key generation takes place with the help of key derivation algorithm, which takes the password from the user and the random number generated by the random number generator function. The result is a hash value which is considered as the key of size 128 bits. The key works as a private key for the next encryption and decryption processes. During the AES Encryption phase, AES-128 IN CBC mode is used for encryption. The key generated and a nonce is used for encryption. A nonce is a pseudo-random number which can be used only once. On having these two things, AES generates the ciphertext. While in AES Decryption phase, the ciphertext derived from the previous phase along with the same password is fed to AES-128 decryption in CBC for getting the plaintext.

Dr Prerna Mahajan Abhishek Sachdeva [17] have analysed how secured, efficient is the AES algorithm compare to RSA and DES. AES can be implemented on small devices as well, due to its less resource consumption compared to RSA and DES. AES has been

[4] https://petapixel.com/2016/11/22/german-photographer-sued-facebook-removing-exif-data-won/

vigorously tested for its security and has proven to be one of the most secure algorithms which has much faster encryption and decryption process. Hence, we chose the AES-128 bits algorithm of our proposal.

In this research, we apply python and Linux based tools to extract the metadata information from the image and AES-128 bits algorithm to encrypt and decrypt it. Further, we analyse our approach to check how it affects the images in terms of quality and size in the evaluation section below.

4 Design Specification

4.1 Exif metadata encryption process

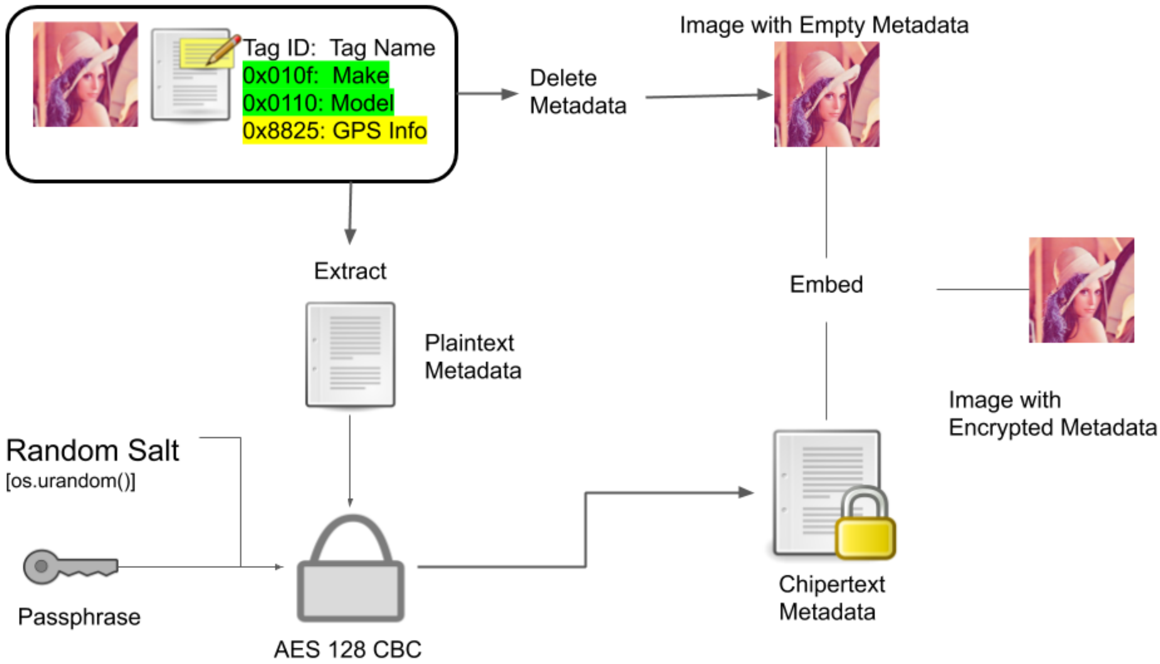

Figure 1: Encryption Process

Step 0: Start
Step 1: Input: Digital Image JPEG IMAGE
Step 2: Check for the image inputted in Step 1 for EXIF metadata tags
Step 3: Extract all the EXIF metadata tags and write it on to the file.
Step 4: Strip the image of its EXIF metadata.
Step 5: Initiate encryption process for the file that has EXIF data using AES-128 bits algorithm.
Step 6: Input passphrase
Step 7: Generate nonce using secure random number generator.
Step 8: Feed passphrase and generated nonce to the AES encryption function Step 9: Store the generated key
Step 10: Encrypt the file with extracted EXIF metadata using AES-128 bits algorithm and output the ciphertext to a file.
Step 11: Select image from which the EXIF data was stripped.

Step 12: Embed the ciphertext into Exif.Image.ImageDescription metadata tag in image selected in step 11.
Step 13: Stop.

4.2 Exif metadata decryption process

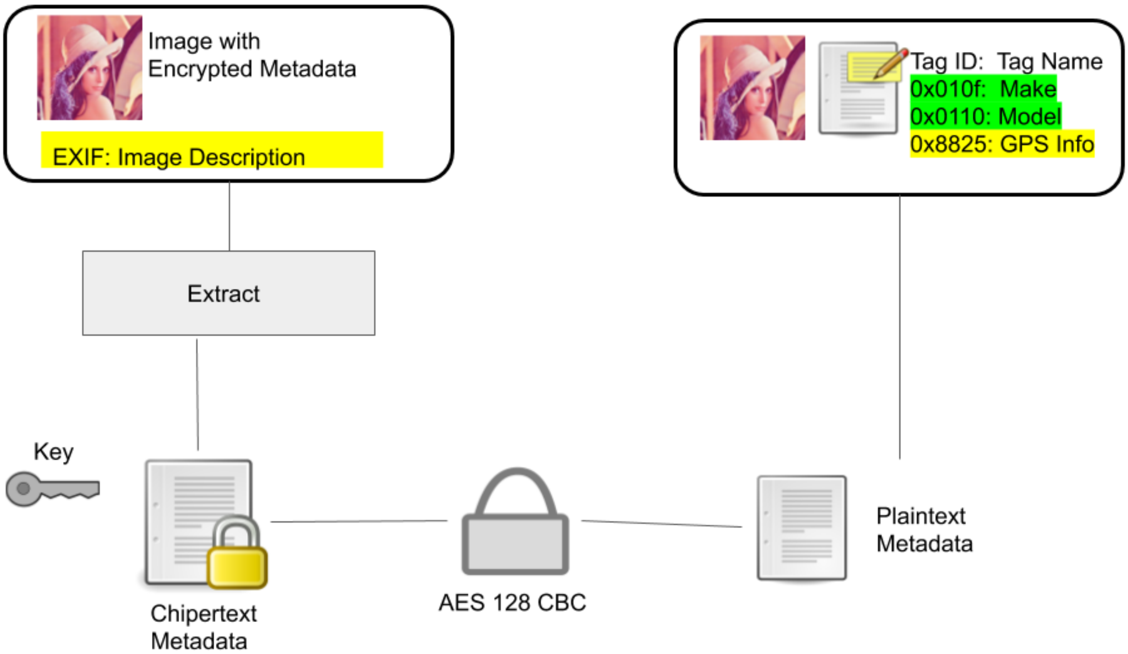

Figure 2: Decryption Process

Start.
Step 1: Input: digital image JPEG IMAGE with encrypted EXIF metadata.
Step 2: Extract the embedded ciphertext from Exif.Image.ImageDescription tag in the image inputted in step 1.
Step 3: Store the extracted ciphertext in a file
Step 4: Initiate decryption process by requesting the AES-128 bits cipher key.
Step 5: Input the ciphertext file and cipher key received from step 4 to AES-128 bits algorithm for decryption.
Step 6: Write the plaintext obtain to a file.
Step 7: Read EXIF using metadata tag id.
Step 8: Stop

5 Implementation

The paper proposes a method, which is demonstrated by implementing AES Encryption and Decryption scripts in Python along with use of Exiftool and EXIV2.

5.1 Extracting and Stripping EXIF data

On the base linux system, the command line application EXIFTOOL will extract metadata and will store it in a separate text file and will then strip the metadata from the image.

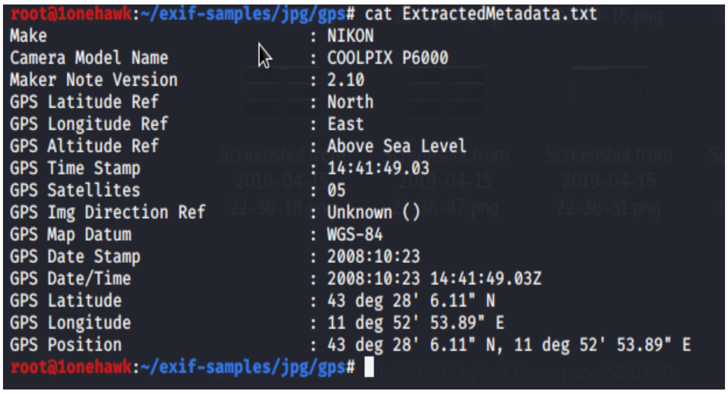

Figure 3: Extracted Metadata

5.2 AES Encryption

The AES Encryption python script will then perform encryption on the obtained extracted metadata file and while generating an encrypted metadata file For encryption the passphrase is provided through user input while nonce is added using a random number generator function for derivation of key which is then stored for the decryption process.

Figure 4: Encryption Process

5.3 Embedding Image EXIV2

The generated encrypted metadata is then embedded in the Image which was stripped of metadata in phase 1

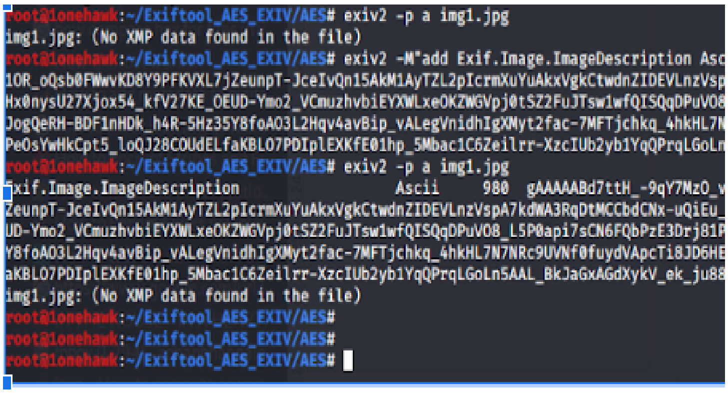

Figure 5: Embedding Process

5.4 Extracting Chipertext and applying AES Decryption

The encrypted text then is extracted using EXIFTOOL and then stored in a separate text file. The file is then decrypted the AES Decryption python script. While decrypting the encrypted metadata the key is provided through user input. The decrypted metadata is then stored in a separate file.

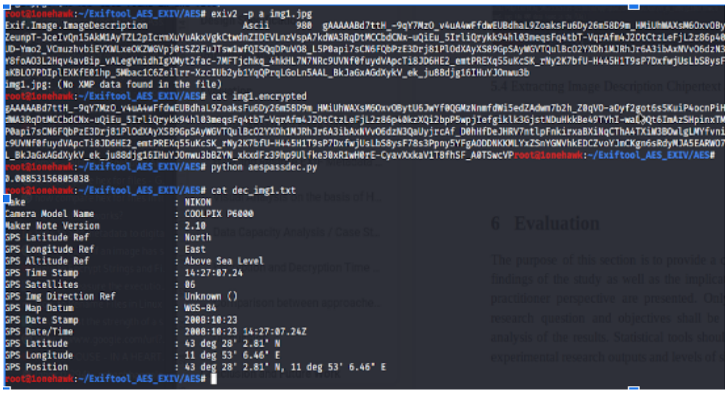

Figure 6: Decryption Process

6 Evaluation

6.1 Visual Analysis

Visual analysis of the process of encryption and decryption on EXIF metadata using AES showed no change in terms of color and pixel of the image, as shown in figure 6.

Figure 7: Visual Analysis

6.2 Hide and Restore EXIF Metadata

The process to improve the security of the EXIF metadata using AES algorithm that can hide and restore EXIF metadata after encryption and decryption method.

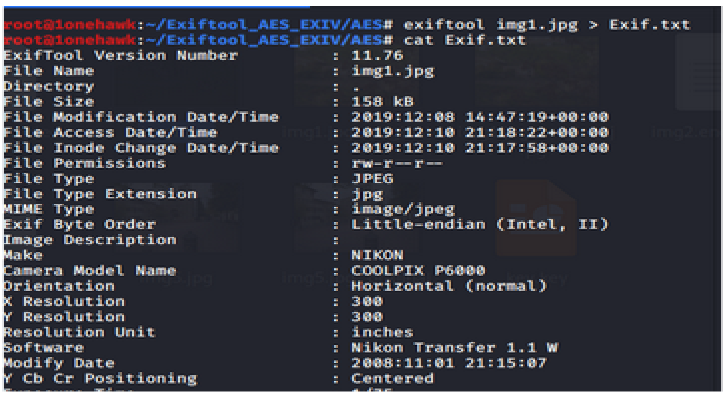

Figure 8: Original Metadata

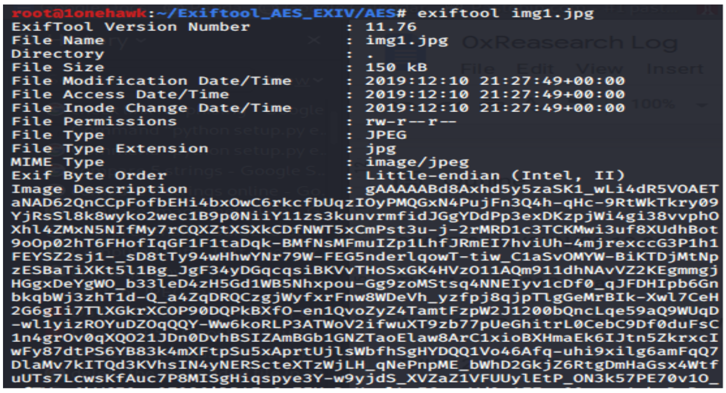

Figure 9: Encrypted Metadata

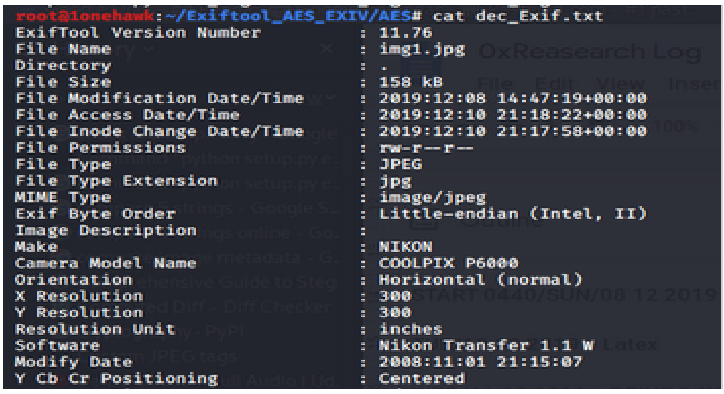

Figure 10: Decrypted Metadata

6.3 Hexadecimal Analysis

Visual analysis on the hexadecimal values of the file was performed. There was no difference observed in the original striped image and the decrypted image. As per the figure, changes occur in the metadata after the encryption is performed

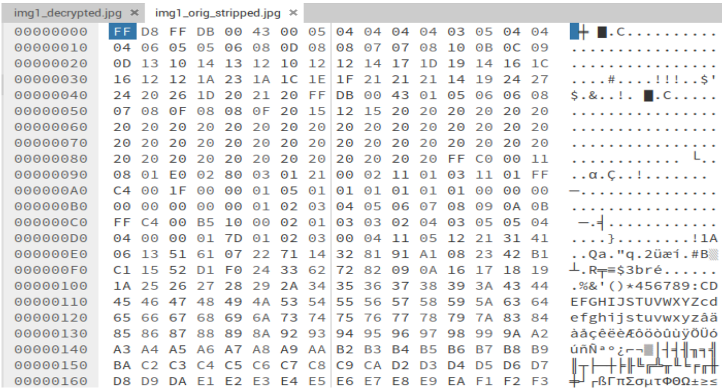

Figure 11: Original Metadata Striped

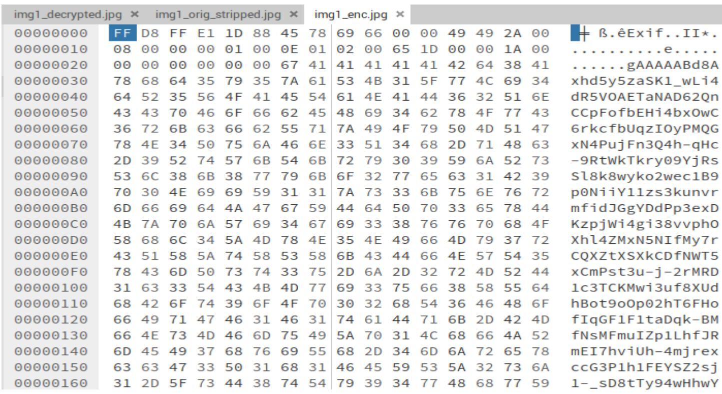

Figure 12: Encrypted Metadata

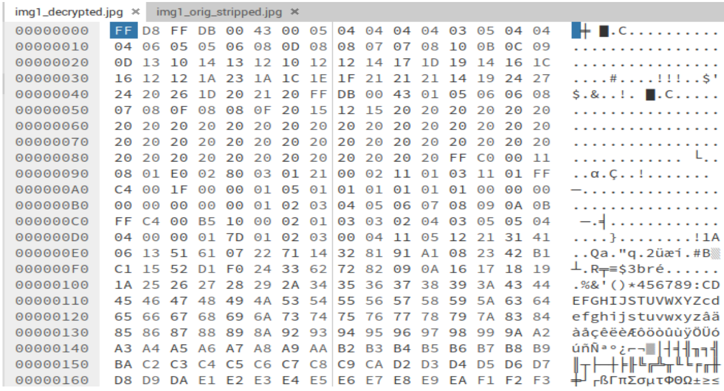

Figure 13: Decrypted Metadata

6.4 Data Capacity Analysis

Reduction in file size is caused due to the changes in the metadata in the header file of the image and the shift of bits of data.

Sample	Original Size	Without Chiphertext (Decrypted)	Loss in file size	Percentage
img1	157.9	143	14.9	-9.436352122
img2	159.137	140.8	18.337	-11.52277597
img3	157.382	139.1	18.282	-11.61632207
img4	150.301	132.9	17.401	-11.57743461
img5	157.723	140	17.723	-11.23678855

Figure 14: Data Capacity Analysis

Formula used for calculating the percentage change in image is as follows

$$(O - D)/O * 100 = P \tag{1}$$

O=Original Image D=Decrypted Image P=Percentage Change

6.5 Histogram Analysis

Each image has red,blue, green and grey color composition in each pixel. The color composition will fill the pixels with these color values. Color change occurring in single pixel of the image will cause the whole histogram to change. Histogram analysis is needed to know if any changes had occurred to the image during the process of encryption and decryption

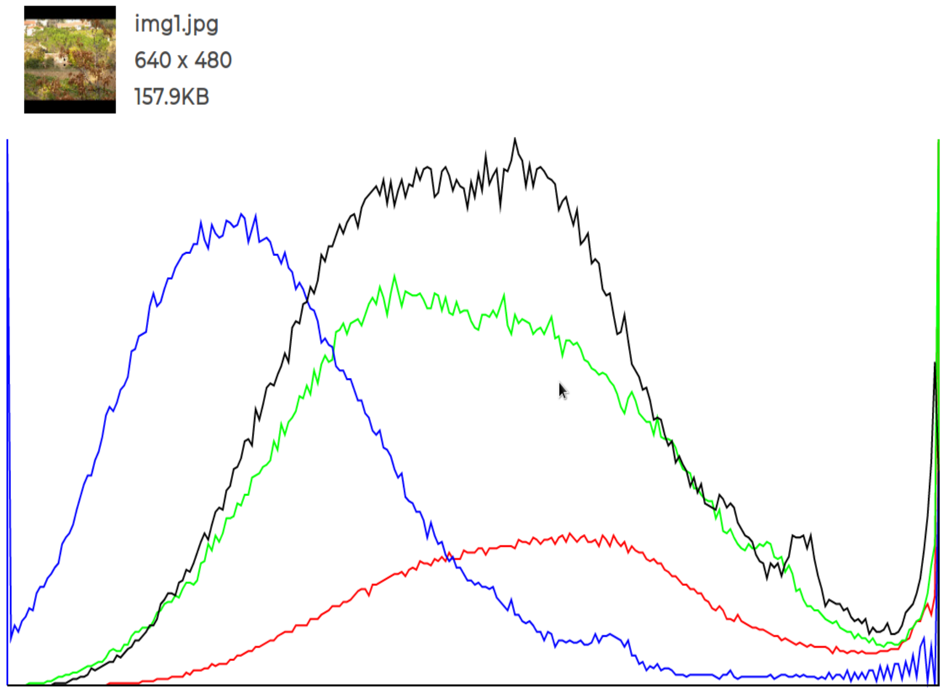

Figure 15: Original Image

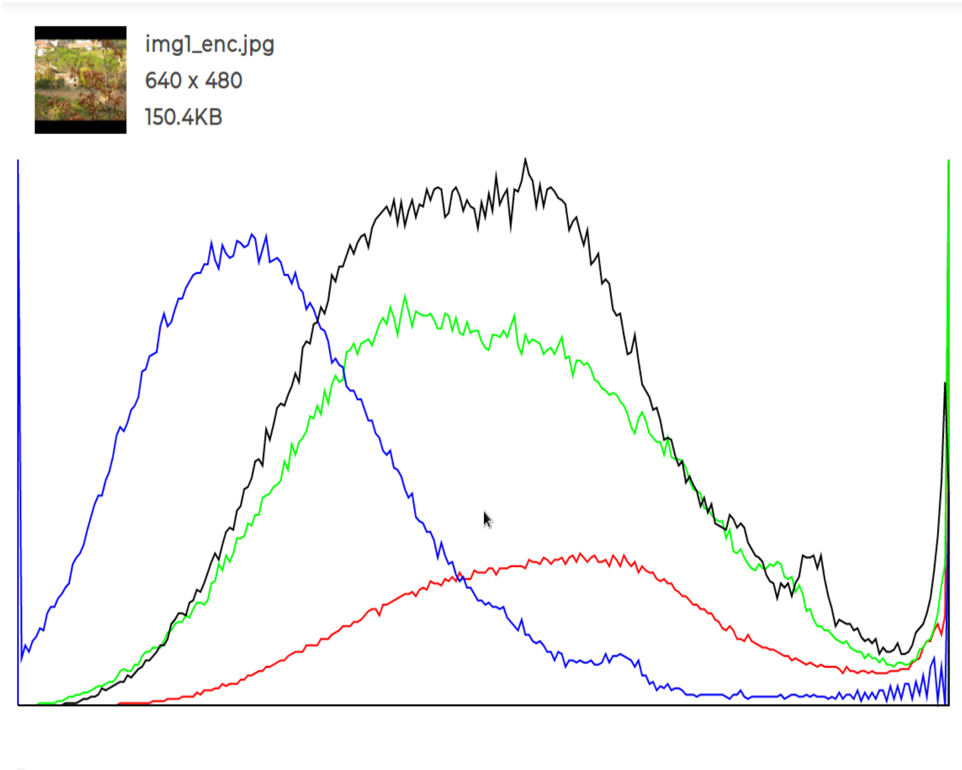

Figure 16: Image with encrypted Metadata

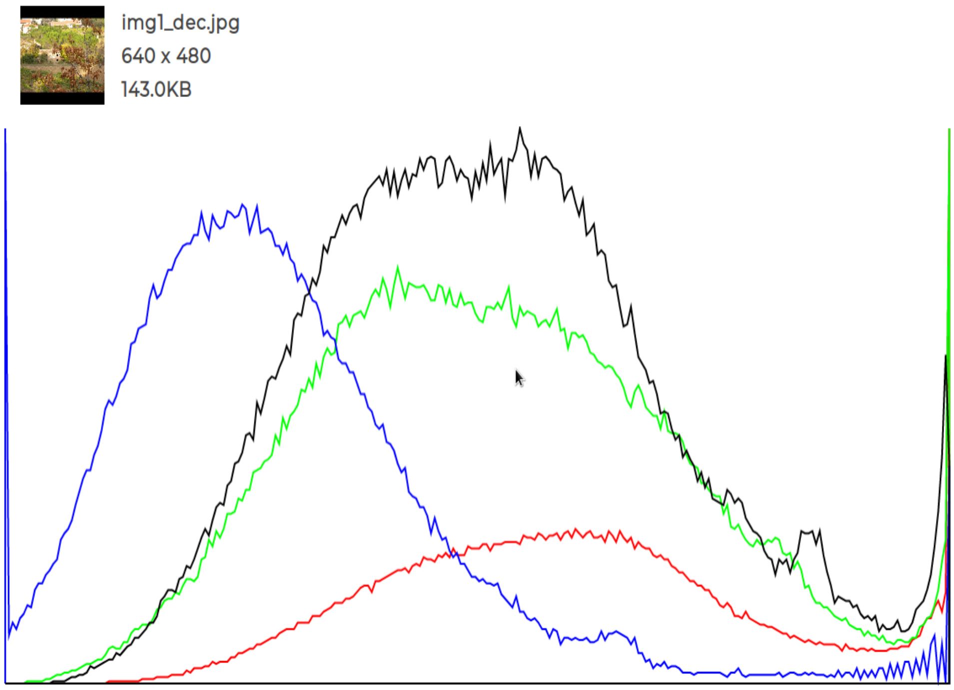

Figure 17: Image with decrypted Metadata

6.6 Comparison between approaches of securing metadata

Paper	Approach	Pros and Cons
Improving Privacy in JPEG Images	Adding Privacy policy inside image and encrypting both	Has access control but has the need to send separate file for handling more access permissions
Encryption EXIF Metadata for Protection Photographic Image of Copyright Piracy	Encrypting metadata using XTEA algorithm and insert it into end of file and deleting original EXIF	Hides the metadata but XTEA is weak as compared to AES
Proposed Paper	Stripping EXIF metadata and encrypting it using AES and inserting it into Image Description tag	AES is strong. Lightweight implementation however issues such as key management and not entirely secure against MiTM Ciphertext attack

Figure 18: Approach Evaluation

6.7 Limitations

In the proposed model, poses the limitation of secure key exchange, also the shared key is stored in a file. If the file comes in the hands of an attacker, it becomes easy for the attacker to decrypt the ciphertext metadata. Encryption will avoid the change of EXIF metadata from getting modified and will keep the integrity intact. Still, however, there exists the possibility of Man in the Middle attack, the attacker can modify the ciphertext in transit of the image file.

6.8 Discussion

Multiple test cases were conducted in order to test whether the aim of the research was achieved. The aim of the research was to secure image metadata from leaking users' GPS information, make and model of the users' device using encryption algorithm AES. The findings from the first test case state that the process of encrypting and decrypting the metadata using AES does not affect the image colour and pixel. The second evaluation provides evidence that the process of encrypting and decrypting image metadata using AES is able to hide and restore the image metadata, and that adds security to the image metadata. Another test case shows that the hex values of the original image after stripping metadata and that of the decrypted image is the same. In the fourth test case, data capacity analysis states that the average of -11.07 is observed in file size reduction from the original image to the decrypted image. Other finding revealed that the histogram for the original image with striped metadata, the image with encrypted metadata and image with decrypted metadata is same and provides the substance that the aim for the research question of securing image metadata is achieved.

7 Conclusion and Future Work

In this report, AES-128 bits algorithm was implemented to build a model for securing EXIF metadata for the JPEG image file format using scripts written in the python programming language, Linux command-line applications such as ExifTool and exiv2. Conducted case studies have proved that the implemented model can extract, strip, encrypt and decrypt EXIF metadata from JPEG image without affecting the pixel image. However, variation in the file size is caused after performing metadata stripping and after embedding encrypted metadata in the image. Furthermore, it was also observed that after performing decryption, the image file size is the same as the original striped metadata image file. These changes alter the file size by an average of -11.07 from the original file size.

From the obtained results, EXIF encryption can be used for securing image metadata from getting read or altered by the bad actor who can be used for exploiting individuals, businesses and endangered animal species.

Future work will be aimed at expanding the proposed approach to all image file formats, implementing file checksum for the encrypted metadata files, creating an automatic photographic metadata remover and a standard to be applied for all photographic metadata.

Acknowledgement

I would like to take this opportunity to thank my supervisor and mentor Ben Fletcher for the insights and guidance which has added more value to this research and the for encouraging me to conduct the research and assisting me to focus on the key aspect of the project. I am thankful and appreciative of his mentorship due to which I was able to complete the journey. I would like to offer gratitude to my professors Irina Tal and Arghir Moldovan for their valuable knowledge and immense support throughout the course.

References

[1] S. Tayeb, A. Week, J. Yee, M. Carrera, K. Edwards, V. Murray-Garcia, M. Marchello, J. Zhan, and M. Pirouz, "Toward metadata removal to preserve privacy of social media users," in *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)*, Jan 2018, pp. 287–293.

[2] A. C. Squicciarini, D. Lin, S. Sundareswaran, and J. Wede, "Privacy policy inference of user-uploaded images on content sharing sites," *IEEE Transactions on Knowledge and Data Engineering*, vol. 27, no. 1, pp. 193–206, Jan 2015.

[3] J. Lepsoy, S. Kim, D. Atnafu, and H. J. Kim, "Metadata protection scheme for jpeg privacy security using hierarchical and group-based models," in *2015 5th International Conference on Information Communication Technology and Accessibility (ICTA)*, Dec 2015, pp. 1–5.

[4] J. Delgado and S. Llorente, "Improving privacy in jpeg images," in *2016 IEEE International Conference on Multimedia Expo Workshops (ICMEW)*, July 2016, pp. 1–6.

[5] J. Tešić, "Metadata practices for consumer photos," *Multimedia, IEEE*, vol. 12, pp. 86 – 92, 08 2005.

[6] G. Friedland and R. Sommer, "Cybercasing the joint: On the privacy implications of geo-tagging," in *HotSec*, 2010.

[7] B. Henne, C. Szongott, and M. Smith, "Snapme if you can: Privacy threats of other peoples' geo-tagged media and what we can do about it," in *Proceedings of the Sixth ACM Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '13. New York, NY, USA: ACM, 2013, pp. 95–106. [Online]. Available: http://doi.acm.org/10.1145/2462096.2462113

[8] B. Henne, M. Koch, and M. Smith, "On the awareness, control and privacy of shared photo metadata," in *Financial Cryptography and Data Security*, N. Christin and R. Safavi-Naini, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 77–88.

[9] R. Sarvas, E. Herrarte, A. Wilhelm, and M. Davis, "Metadata creation system for mobile images," in *Proceedings of the 2Nd International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '04. New York, NY, USA: ACM, 2004, pp. 36–48. [Online]. Available: http://doi.acm.org/10.1145/990064.990072

[10] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *2017 International Conference on Engineering and Technology (ICET)*, Aug 2017, pp. 1–7.

[11] H. Wijayanto, I. Riadi, and Y. Prayudi, "Encryption exif metadata for protection photographic image of copyright piracy," vol. 5, pp. 2320–5156, 05 2016.

[12] P. Kumar, S. Rawat, T. Choudhury, and S. Pradhan, "A performance based comparison of various symmetric cryptographic algorithms in run-time scenario," in *2016 International Conference System Modeling Advancement in Research Trends (SMART)*, Nov 2016, pp. 37–41.

[13] M. Panda, "Performance analysis of encryption algorithms for security," in *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, Oct 2016, pp. 278–284.

[14] P. Patil, P. Narayankar, D. Narayan, and M. S M, "A comprehensive evaluation of cryptographic algorithms: Des, 3des, aes, rsa and blowfish," *Procedia Computer Science*, vol. 78, pp. 617–624, 12 2016.

[15] M. Biglari, E. Qasemi, and B. Pourmohseni, "Maestro: A high performance aes encryption/decryption system," in *The 17th CSI International Symposium on Computer Architecture Digital Systems (CADS 2013)*, Oct 2013, pp. 145–148.

[16] A. E. Standard, "Federal information processing standards publication 197," pp. 46–3, 2001.

[17] P. Mahajan and A. Sachdeva, "A study of encryption algorithms aes, des and rsa for security," 2013.