

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).	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies).	<input type="checkbox"/>
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.	<input type="checkbox"/>

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.

¹Internet 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 soldiers². Also, the documents published by Whistleblower Edward Snowden shows the classified nationwide surveillance, i.e. XKeyscore program which used metadata to collect information on users³. 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,

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

³XKeyscore: <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 stripping metadata, facebook was sued by a german photographer⁴ 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

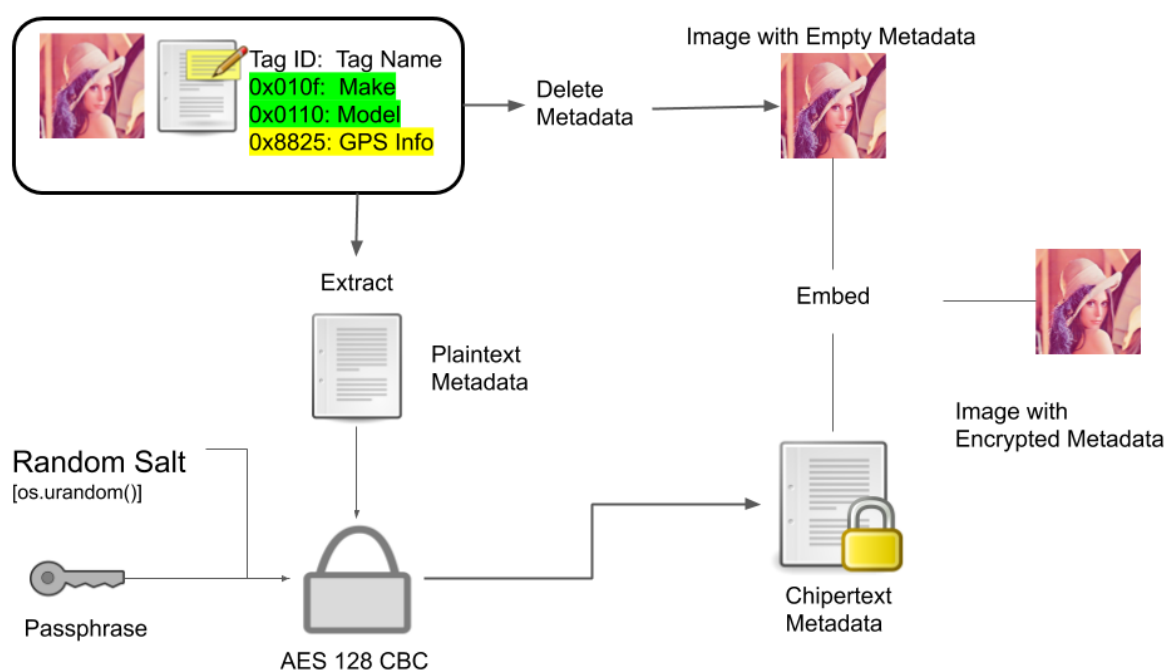


Figure 1: Encryption Process

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

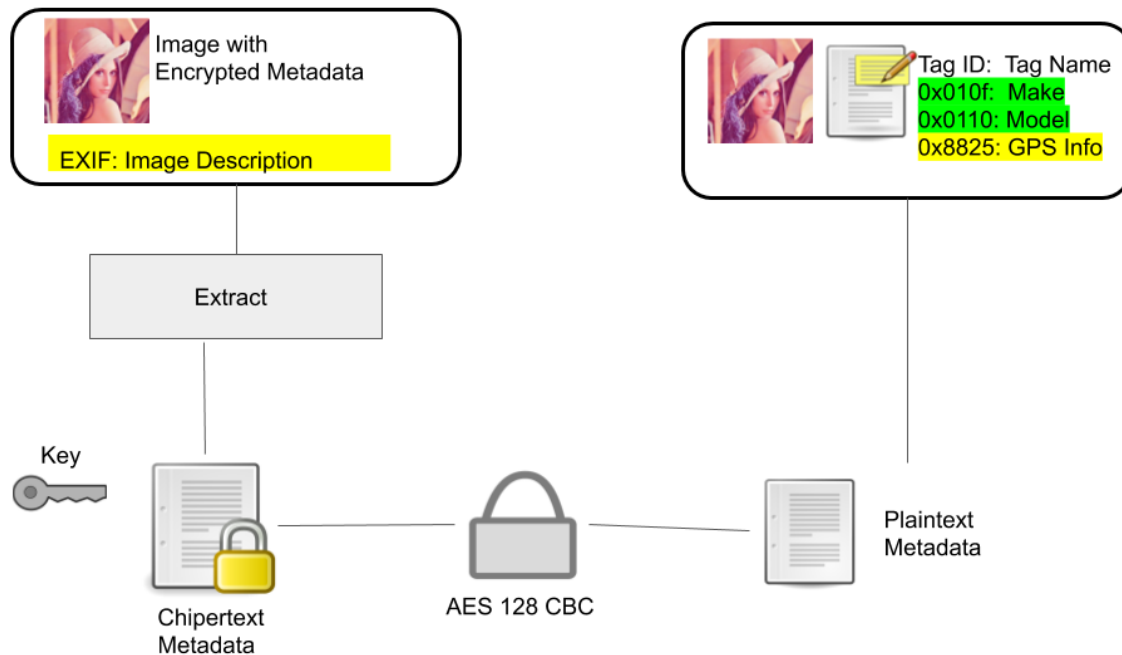


Figure 2: Decryption Process

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.

```
root@lonehawk:~/exif-samples/jpg/gps# cat ExtractedMetadata.txt
Make           : NIKON
Camera Model Name : COOLPIX P6000
Maker Note Version : 2.10
GPS Latitude Ref : North
GPS Longitude Ref : East
GPS Altitude Ref : Above Sea Level
GPS Time Stamp   : 14:41:49.03
GPS Satellites   : 05
GPS Img Direction Ref : Unknown ( )
GPS Map Datum    : WGS-84
GPS Date Stamp   : 2008:10:23
GPS Date/Time    : 2008:10:23 14:41:49.03Z
GPS Latitude     : 43 deg 28' 6.11" N
GPS Longitude    : 11 deg 52' 53.89" E
GPS Position     : 43 deg 28' 6.11" N, 11 deg 52' 53.89" E
root@lonehawk:~/exif-samples/jpg/gps#
```

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.

```
root@lonehawk:~/simua/AES# ls
aespassenc.py backup DSCN0025.jpg ExtractedMetadata.txt
root@lonehawk:~/simua/AES# python aespassenc.py
Enter password:rohan
39L9Q1bQ_NXrV2DE8ecnRQ_N1e2Jr2XapQF4ho8ux2M=
root@lonehawk:~/simua/AES# ls
aespassenc.py backup DSCN0025.jpg ExtractedMetadata.encrypted ExtractedMetadata.txt key.key
root@lonehawk:~/simua/AES# cat ExtractedMetadata.encrypted
gAAAAABd7o9Sq6SAY2kPEE011-pYeMjmsI32Lzq6HrDDnTTcTbV1wTG40YXm9qXczWvtIiu4UyLAXucYKsuAwTjjP69q1AP040pDX3Ec72IOc1p29daL
1j1RjHqz9AajfMEtUfVjL3ach37GesJi7Nj189caRtn9rncFRG_X4FYFBEI3rq2L80jfzLzgbmbZzh22szzK3z53AxiQbF0X0Nw8FYLZK2TCBIxo30tRbh
H-NEsWBM6EBGhdZn7Cyu-cpb98rVi5v2tgoro1YmLkys2NfrTjgnxQLXHfrwDPmuTBvlpSGYtndzMZrZXhwDvhuHHAQBX1Af_X6IGLjXw-3M1KmaAnz_jP
zaNj8e5K5DmC5c_uF214ZfzczqR2bk-Wbh2k_bKwt8cx1Hh-qfxc1Bm08eLNPyokw9OSTtFUV4MntyX6rH32NhFaiJmW8768Lx4xJum_Kst09ZntSLzPxOx
xRqQF4tUebF2j49MctLSV3EqKWSPEqpAmiioq6E23VLzsGbjFLkLf01p_7uLJrsPILFmwuo_ZmNojByhL7eF8Dy_T_aCLroot@lonehawk:~/simua/A
39L9Q1bQ_NXrV2DE8ecnRQ_N1e2Jr2XapQF4ho8ux2M=root@lonehawk:~/simua/AES#
```

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

```

root@lonehawk:~/Exiftool_AES_EXIV/AES# exiv2 -p a img1.jpg
img1.jpg: (No XMP data found in the file)
root@lonehawk:~/Exiftool_AES_EXIV/AES# exiv2 -M*add Exif.Image.ImageDescription Ascii 988 gAAAAABd7ttH_-9qY7Mz0_v
1OR_oQsb0FWwvKD8Y9PFKVL7jZeunpT-JceIvQn15AkM1AyTZL2pIcrnXuYuAkxVgkCtwdnZIDEVLnzVsp
Hx0nysU27Xjox54_kvF27KE_OEUD-Ymo2_VCmuzhvbiEYXWLxeOKZWGVPj0tS2ZFuJTsW1wfQISQqDPuV08
Y8foA03L2HqV4avBip_vALegVnidhIgxMyt2fac-7MFTjchkq_4hkHL7N7Nrc9UVNF0fuydVapcTi8J06HE
PeOsYwHkCpt5_loQJ28COUDLfaKBL07PDIPLEXKFE01hp_5Mbac1C6Zeilrr-XzcIUb2yb1YqQPrqLGoLn
root@lonehawk:~/Exiftool_AES_EXIV/AES# exiv2 -p a img1.jpg
Exif.Image.ImageDescription      Ascii      988      gAAAAABd7ttH_-9qY7Mz0_v
ZeunpT-JceIvQn15AkM1AyTZL2pIcrnXuYuAkxVgkCtwdnZIDEVLnzVspA7kdWA3RqDtMCCbdCNx-uQIEU
UD-Ymo2_VCmuzhvbiEYXWLxeOKZWGVPj0tS2ZFuJTsW1wfQISQqDPuV08_L5P8api7sCN6FQbPzE3Drj81F
Y8foA03L2HqV4avBip_vALegVnidhIgxMyt2fac-7MFTjchkq_4hkHL7N7Nrc9UVNF0fuydVapcTi8J06HE
aKBL07PDIPLEXKFE01hp_5Mbac1C6Zeilrr-XzcIUb2yb1YqQPrqLGoLn5AAL_BkJaGxAGdXykv_ek_ju88
img1.jpg: (No XMP data found in the file)
root@lonehawk:~/Exiftool_AES_EXIV/AES#
root@lonehawk:~/Exiftool_AES_EXIV/AES#
root@lonehawk:~/Exiftool_AES_EXIV/AES#

```

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.

```

root@lonehawk:~/Exiftool_AES_EXIV/AES# exiv2 -p a img1.jpg
Exif.Image.ImageDescription      Ascii      988      gAAAAABd7ttH_-9qY7Mz0_v4uAkwFdwEUBdhal9ZoaksFu6Dy26s58D9m_HM1UHMAXG60xv0Bj
ZeunpT-JceIvQn15AkM1AyTZL2pIcrnXuYuAkxVgkCtwdnZIDEVLnzVspA7kdWA3RqDtMCCbdCNx-uQIEU_SiFlidrykk94h183meqsFq4tbt-VqPafmAJ20tCtZLefJL286p4E
UD-Ymo2_VCmuzhvbiEYXWLxeOKZWGVPj0tS2ZFuJTsW1wfQISQqDPuV08_L5P8api7sCN6FQbPzE3Drj81FPI0DxAYX89GSAyWGTQ18COZYXDI1M1RbJreA31BakxVv06dZ8
Y8foA03L2HqV4avBip_vALegVnidhIgxMyt2fac-7MFTjchkq_4hkHL7N7Nrc9UVNF0fuydVapcTi8J06HE2_watPREd85KCSK_cnyx27Bfu-H44SH1Tps7DxwjuLUS58ySf
aKBL07PDIPLEXKFE01hp_5Mbac1C6Zeilrr-XzcIUb2yb1YqQPrqLGoLn5AAL_BkJaGxAGdXykv_ek_ju88jg161HuV30nuw3b
img1.jpg: (No XMP data found in the file)
root@lonehawk:~/Exiftool_AES_EXIV/AES# cat img1.encrypted
gAAAAABd7ttH_-9qY7Mz0_v4uAkwFdwEUBdhal9ZoaksFu6Dy26s58D9m_HM1UHMAXG60xv0BjU53wYf8QGM2knfdw15e4ZAdm7D2h_Z8qV0-acyf2got655KulP4acnPIH
5M380dttCCbdCNx-uQIEU_SiFlidrykk94h183meqsFq4tbt-VqPafmAJ20tCtZLefJL286p4E4kzXQ12bp99wJ1ofgik1k36jstMwukx8e49Ythi-wal_Xrt61mzrShpInkTM
P8api7sCN6FQbPzE3Drj81FPI0DxAYX89GSAyWGTQ18COZYXDI1M1RbJreA31BakxVv06dZ8Q8yUjrcAf_DhHfDeJHRV7nTpFkncrxaxBkiqCThAA7LMB30wLGLMYfni
cKwMfuydVapcTi8J06HE2_watPREd85KCSK_cnyx27Bfu-H44SH1Tps7DxwjuLUS58ySf8c3pnmj5f9gID80k0L7z2zyv0vHkE8CZx0i2cKq6899yASISAR007
L_BkJaGxAGdXykv_ek_ju88jg161HuV30nuw3bZYN_xicofz39hp9U1ke38R1w8RE-CyaxXxav1T8fhsF_8RTSwcVP_wat@lonehawk:~/Exiftool_AES_EXIV/AES#
root@lonehawk:~/Exiftool_AES_EXIV/AES# python aespassdec.py
0.00853156805838
root@lonehawk:~/Exiftool_AES_EXIV/AES# cat dec_img1.txt
Exiftool: NIKON
Camera Model Name : COOLPIX P6000
Maker Note Version : 2.18
GPS Latitude Ref : North
GPS Longitude Ref : East
GPS Altitude Ref : Above Sea Level
GPS Time Stamp : 14:27:47.24
GPS Satellites : 85
GPS Img Direction Ref : Unknown ( )
GPS Map Datum : WGS-84
GPS Date Stamp : 2008:18:23
GPS Date/Time : 2008:18:23 14:27:07.24Z
GPS Latitude : 43 deg 28' 2.81" N
GPS Longitude : 11 deg 53' 6.46" E
GPS Position : 43 deg 28' 2.81" N, 11 deg 53' 6.46" E

```

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.

```

root@lonehawk:~/Exiftool_AES_EXIV/AES# exiftool img1.jpg > Exif.txt
root@lonehawk:~/Exiftool_AES_EXIV/AES# cat Exif.txt
ExifTool Version Number      : 11.76
File Name                    : img1.jpg
Directory                   : .
File Size                    : 158 kB
File Modification Date/Time  : 2019:12:08 14:47:19+00:00
File Access Date/Time       : 2019:12:10 21:18:22+00:00
File Inode Change Date/Time : 2019:12:10 21:17:58+00:00
File Permissions             : rw-r--r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Image Description            :
Make                         : NIKON
Camera Model Name            : COOLPIX P6000
Orientation                  : Horizontal (normal)
X Resolution                 : 300
Y Resolution                 : 300
Resolution Unit              : inches
Software                     : Nikon Transfer 1.1 W
Modify Date                  : 2008:11:01 21:15:07
Y Cb Cr Positioning         : Centered

```

Figure 8: Original Metadata

```

root@ioneahawk:~/Exiftool_AES_EXIV/AES# exiftool img1.jpg
ExifTool Version Number      : 11.76
File Name                    : img1.jpg
Directory                    : .
File Size                    : 150 kB
File Modification Date/Time  : 2019:12:10 21:27:49+00:00
File Access Date/Time       : 2019:12:10 21:27:49+00:00
File Inode Change Date/Time  : 2019:12:10 21:27:49+00:00
File Permissions             : rw-r--r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Image Description            : gAAAAABd8AXhd5y5zaSK1_wLi4dR5VOAET
aNAD62QnCCpFofbEHi4bx0wC6rkcfbUqzIOyPMQGXN4PujFn3Q4h-qHC-9RtwkTkry09
YjRsSl8k8wyko2wec1B9p0NiiY11zs3kunvrmfidJGgYDdPp3exDKzpjW4gi38vvpH0
XhL4ZMxNSNIIfMy7rCQXZtXSXkCDfNWT5xCmPst3u-j-2rMRD1c3TCKMwi3uf8XUdhBot
9oOp02hT6FHoFtqGF1FItaDqk-BMfNsMfmuIZp1lhfJRmEI7hviUu-4mjrexccG3P1h1
FEY5Z2sj1-cD8Lty9awhWYnr79W-FEG5nderlqowT-tiw_CiaSv0MYW-BiKTDjMtNp
zESBaTlXkt5L1B8_JgF34yDgqcqsIBKVVThoSxGK4HVzO11AQm911dhNAvVZ2KEgmmgj
HggDeYgW0_b33leD4zH5Gd1WB5Nhxpu-Gg9zoMStsq4NNEIyv1cDf0_qJFDHIpb6Gn
bkqbWj3zhT1d-Q_a4ZqDRQCzgjWYfxrFmw8WDeVh_yzfpj8qjpTlgGeMrBIk-Xwl7CeH
2G6gi7TLXGkrXCOP90DQPkBXf0-en1QvoZyZ4TamtFzpw2J1200bQncLqe59aQ9WUqD
-wliyzROyudZ0qQY-Ww6koRLP3ATwoV2ifwuXT9zb77pUeGhitrL0Cebc9Df0duFsc
In4gr0V0qX0021JDn0dvhBSIZAmBGB1GNZTaoE1aw8Arc1xi0BXHmaEk6I3tn5zkexci
wFy87dtPS6Y883k4mXfTpSu5XAprrtUj1sWbFhSgHYDQ01Vo46Afg-uh19x1lg6amfQ07
DlaMv7kITQd3KVhsIN4yNERScteXTzWjLH_qNePnpME_bwhD2Gkjz6RtgDmHagsx4WtF
uUTS7LcwsKfAuc7P8MISgHiqspye3Y-w9yjdS_XVZaZ1VFUUY1EtP_ON3k57PE70v10.

```

Figure 9: Encrypted Metadata

```

root@ioneahawk:~/Exiftool_AES_EXIV/AES# cat dec_Exif.txt
ExifTool Version Number      : 11.76
File Name                    : img1.jpg
Directory                    : .
File Size                    : 150 kB
File Modification Date/Time  : 2019:12:08 14:47:19+00:00
File Access Date/Time       : 2019:12:10 21:18:22+00:00
File Inode Change Date/Time  : 2019:12:10 21:17:58+00:00
File Permissions             : rw-r--r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Image Description            :
Make                        : NIKON
Camera Model Name           : COOLPIX P6000
Orientation                  : Horizontal (normal)
X Resolution                 : 300
Y Resolution                 : 300
Resolution Unit              : inches
Software                     : Nikon Transfer 1.1 W/Latex
Modify Date                  : 2008:11:01 21:15:07
Y Cb Cr Positioning         : Centered

```

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

```
img1_decrypted.jpg x img1_orig_stripped.jpg x
00000000 FF D8 FF DB 00 43 00 05 04 04 04 04 03 05 04 04 B+ .C.....
00000010 04 06 05 05 06 08 0D 08 08 07 07 08 10 0B 0C 09 .....e.....
00000020 0D 13 10 14 13 12 10 12 12 14 17 1D 19 14 16 1C .....gAAAAABd8A
00000030 16 12 12 1A 23 1A 1C 1E 1F 21 21 21 14 19 24 27 ....#.....!!!!.$'
00000040 24 20 26 1D 20 21 20 FF DB 00 43 01 05 06 06 08 $.&..!. .C.....
00000050 07 08 0F 08 08 0F 20 15 12 15 20 20 20 20 20 20 .....
00000060 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .....
00000070 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .....
00000080 20 20 20 20 20 20 20 20 20 20 20 20 20 20 FF C0 00 11 ..... L.
00000090 08 01 E0 02 80 03 01 21 00 02 11 01 03 11 01 FF ..α.ç.!......
000000A0 C4 00 1F 00 00 01 05 01 01 01 01 01 01 00 00 00 -...}......
000000B0 00 00 00 00 00 01 02 03 04 05 06 07 08 09 0A 0B .....
000000C0 FF C4 00 B5 10 00 02 01 03 03 02 04 03 05 05 04 -...}......
000000D0 04 00 00 01 7D 01 02 03 00 04 11 05 12 21 31 41 ...}......11A
000000E0 06 13 51 61 07 22 71 14 32 81 91 A1 08 23 42 B1 ..Qa."q.2üei.#B█
000000F0 C1 15 52 D1 F0 24 33 62 72 82 09 0A 16 17 18 19 .L.R+=§3br.....
00000100 1A 25 26 27 28 29 2A 34 35 36 37 38 39 3A 43 44 .,%&'()*+456789:CD
00000110 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A 63 64 EFGHIJSTUVWXYZcd
00000120 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A 83 84 e f g h i j s t u v w x y z ä å
00000130 85 86 87 88 89 8A 92 93 94 95 96 97 98 99 9A A2 à á â ã ä å ö ç è é ô õ ü ý ö ö
00000140 A3 A4 A5 A6 A7 A8 A9 AA B2 B3 B4 B5 B6 B7 B8 B9 ú û ü ö ç è é ô õ ü ý ö ö
00000150 BA C2 C3 C4 C5 C6 C7 C8 C9 CA D2 D3 D4 D5 D6 D7 |}~`~@~A~B~C~D~E~F~G~H~I~J~K~L~M~N~O~P~Q~R~S~T~U~V~W~X~Y~Z~[~\~]~^~_~`~a~b~c~d~e~f~g~h~i~j~k~l~m~n~o~p~q~r~s~t~u~v~w~x~y~z~{|}~^_`~ab~cd~ef~gh~ijklmnpqrstuvwxyz~{|}~^_`~abcd~efghijklmnpqrstuvwxyz~{|}~^_`~
00000160 D8 D9 DA E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1 F2 F3 |}~`~@~A~B~C~D~E~F~G~H~I~J~K~L~M~N~O~P~Q~R~S~T~U~V~W~X~Y~Z~[~\~]~^~_~`~a~b~c~d~e~f~g~h~i~j~k~l~m~n~o~p~q~r~s~t~u~v~w~x~y~z~{|}~^_`~ab~cd~ef~gh~ijklmnpqrstuvwxyz~{|}~^_`~abcd~efghijklmnpqrstuvwxyz~{|}~^_`~
```

Figure 11: Original Metadata Striped

```
img1_decrypted.jpg x img1_orig_stripped.jpg x img1_enc.jpg x
00000000 FF D8 FF E1 1D 88 45 78 69 66 00 00 49 49 2A 00 B+ B.eExif..II*..
00000010 08 00 00 00 01 00 0E 01 02 00 65 1D 00 09 1A 00 .....e.....
00000020 00 00 00 00 00 00 67 41 41 41 41 41 42 64 38 41 .....gAAAAABd8A
00000030 78 68 64 35 79 35 7A 61 53 4B 31 5F 77 4C 69 34 xhd5y5zaSK1_wL14
00000040 64 52 35 56 4F 41 45 54 61 4E 41 44 36 32 51 6E dR5V0AETaNAD62Qn
00000050 43 43 70 46 6F 66 62 45 48 69 34 62 78 4F 77 43 CCpFoFbEH14bX0wC
00000060 36 72 68 63 66 62 55 71 7A 49 4F 79 50 4D 51 47 6rkcfbUqzI0yPMQg
00000070 78 4E 34 50 75 6A 46 6E 33 51 34 68 2D 71 48 63 xN4PuJfFn3Q4h-qHc
00000080 2D 39 52 74 57 6B 54 6B 72 79 30 39 59 6A 52 73 -9RLWkTKry09YJRs
00000090 53 6C 38 6B 38 77 79 6B 6F 32 77 65 63 31 42 39 S18k9wyko2wec1B9
000000A0 70 30 4E 69 69 59 31 31 7A 73 33 68 75 6E 76 72 p0N1iY11zS3kumvr
000000B0 6D 66 69 64 4A 47 67 59 44 64 50 70 33 65 78 44 mF1dJgYDdPp3exD
000000C0 4B 7A 70 6A 57 69 34 67 69 33 38 76 76 70 68 4F KzpJw14g138Vvph0
000000D0 58 68 6C 34 5A 4D 78 4E 35 4E 49 66 4D 79 37 72 Xh14ZMxNSNIFFMy7r
000000E0 43 51 58 5A 74 58 53 58 68 43 44 66 4E 57 54 35 CQXZtXSXkCDFNwT5
000000F0 78 43 6D 50 73 74 33 75 2D 6A 2D 32 72 4D 52 44 xCmPst3u-j-2rMRD
00000100 31 63 33 54 43 4B 4D 77 69 33 75 66 38 58 55 64 1c3TCKMw13uf8XuD
00000110 68 42 6F 74 39 6F 4F 70 30 32 68 54 36 46 48 6F hBot9o0p02ht76FHo
00000120 66 49 71 47 46 31 46 31 74 61 44 71 6B 2D 42 4D f1qGf1F1taDqk-BM
00000130 66 4E 73 4D 46 6D 75 49 5A 70 31 4C 68 66 4A 52 fnSfMuIZp1LhfJR
00000140 6D 45 49 37 68 76 69 55 68 2D 34 6D 6A 72 65 78 mEI7hv1Uh-4mjrex
00000150 63 63 47 33 50 31 68 31 46 45 59 53 5A 32 73 6A ccG3P1h1FEYSZ2sj
00000160 31 2D 5F 73 44 38 74 54 79 39 34 77 48 68 77 59 1-_sD8tTy94wHhwY
```

Figure 12: Encrypted Metadata

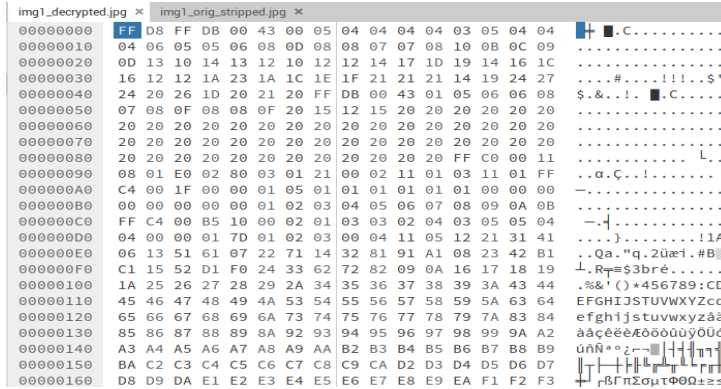


Figure 13: Decrypted Metadata

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

$$(O - D)/O * 100 = P \quad (1)$$

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

img1.jpg
640 x 480
157.9KB

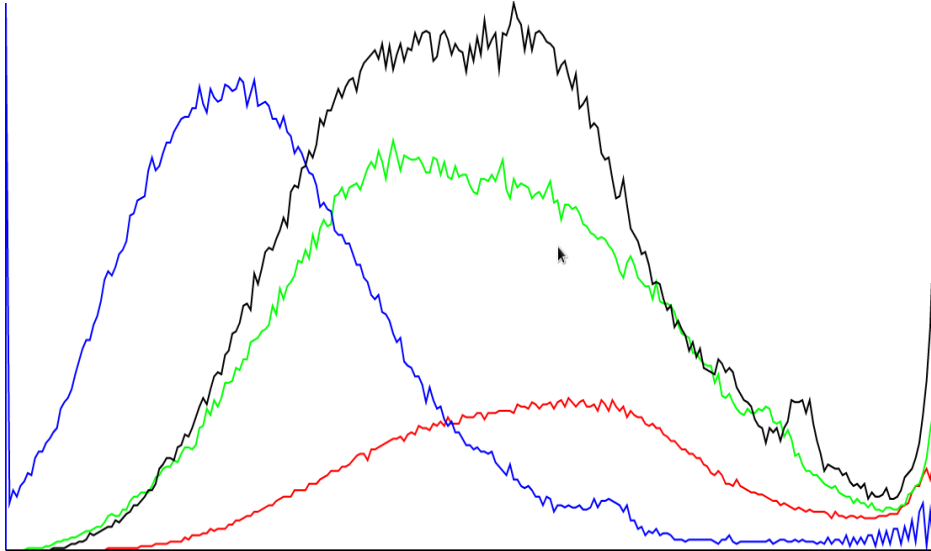


Figure 15: Original Image

img1_enc.jpg
640 x 480
150.4KB

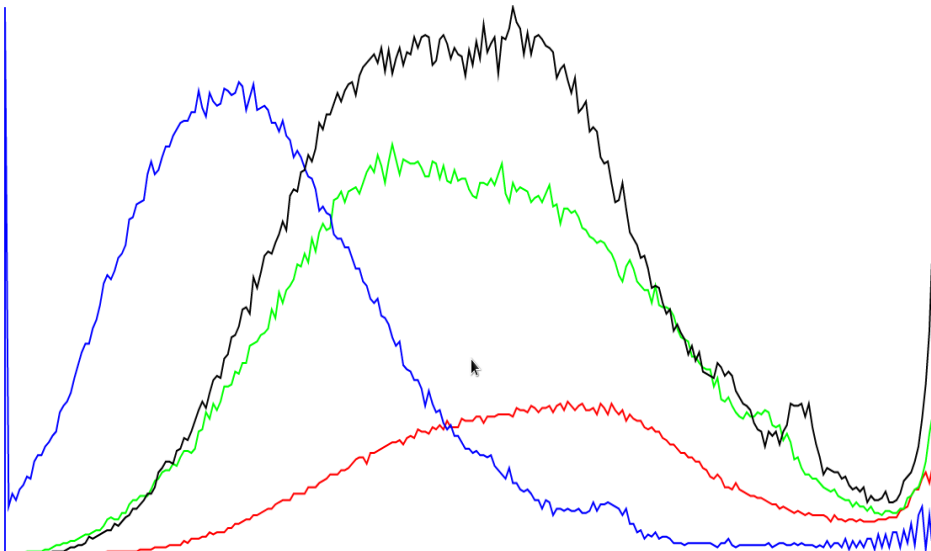


Figure 16: Image with encrypted Metadata

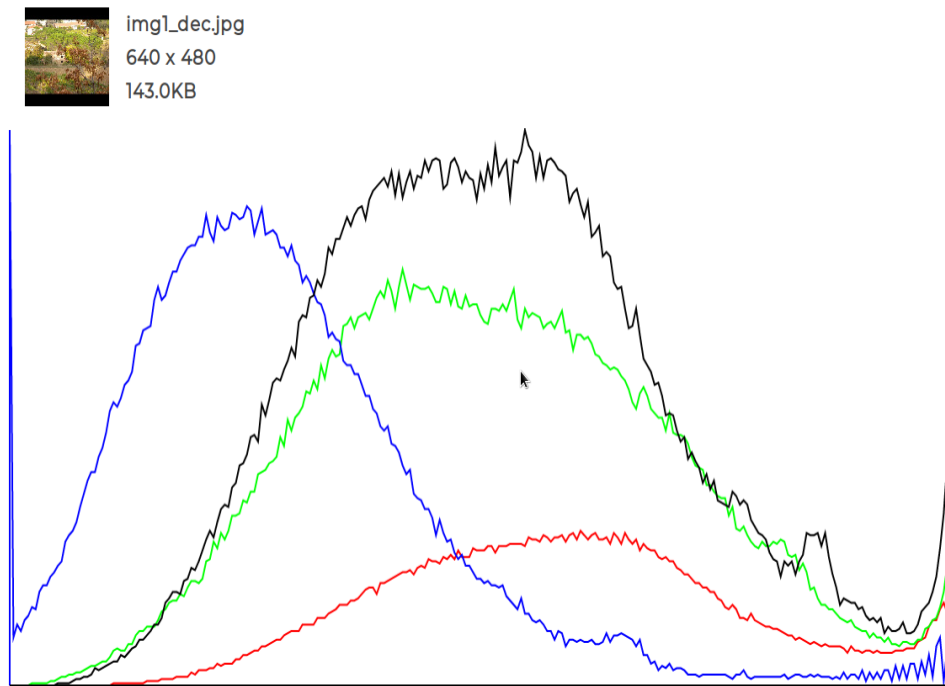


Figure 17: Image with decrypted Metadata

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 (SCOPE5)*, 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.