JOIN (Jurnal Online Informatika)
Volume 4 No. 1 | Juni 2019 : 24-27
DOI: 10.15575/join.v4i1.292

# Development of National Digital Evidence Metadata

**Bambang Sugiantoro**
Magister of Informatics, UIN Sunan Kalijaga, Yogyakarta, Indonesia
bambang.sugiantoro@uin-suka.ac.id

**Abstract- The industrial era 4.0 has caused tremendous disruption in many sectors of life. The rapid development of information and communication technology has made the global industrial world undergo a revolution. The act of cyber-crime in Indonesia that utilizes computer equipment, mobile phones are increasingly increasing. The information in a file whose contents are explained about files is called metadata. The evidence items for cyber cases are divided into two types, namely physical evidence, and digital evidence. Physical evidence and digital evidence have different characteristics, the concept will very likely cause problems when applied to digital evidence. The management of national digital evidence that is associated with continued metadata is mostly carried out by researchers. Considering the importance of national digital evidence management solutions in the cyber-crime investigation process the research focused on identifying and modeling correlations with the digital image metadata security approach. Correlation analysis reads metadata characteristics, namely document files, sounds and digital evidence correlation analysis using standard file maker parameters, size, file type and time combined with digital image metadata. nationally designed the highest level of security is needed. Security-enhancing solutions can be encrypted against digital image metadata (EXIF). Read EXIF Metadata in the original digital image based on the EXIF 2.3 Standard ID Tag, then encrypt and insert it into the last line. The description process will return EXIF decryption results in the header image. This can secure EXIF Metadata information without changing the image quality**

***Keywords*- The industrial era 4.0, *Metadata* and digital evidence**

## I. INTRODUCTION

The industrial era 4.0 has caused tremendous disruption in many sectors of life. The rapid development of information and communication technology has made the global industrial world undergo a revolution. According to APJII data internet users in Indonesia reached 143 million people, this has the potential for cyber-crime in Indonesia. Crime by utilizing computer equipment, mobile phones are increasing. The information in a file whose contents are an explanation of the file is called metadata. Evidence for cyber cases is divided into two types, namely physical evidence, and digital evidence. Physical evidence and digital evidence have different characteristics. This concept will very likely cause problems when applied to digital evidence. The management of national digital evidence that is associated with continued metadata is mostly carried out by researchers [1]–[6].

Law of the Republic of Indonesia Number 11 of 2008 concerning Electronic Information and Transactions that electronic information and/or electronic documents and/or print results are legitimate legal evidence, the role of digital forensics as a method of proving a digital crime case is very important. As stated in the Explanation of the Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions:

"..... verification is a very important factor, considering that electronic information is not only comprehensively accommodated in the Indonesian procedural law system, but also turns out to be very vulnerable to be changed, tapped, falsified, and sent to various parts of the world in a matter of seconds. Thus, the impact caused can be so complex and complicated."

In various cases that occur today, there is digital evidence that can assist officers in uncovering a criminal case. One of them is through information about the contents of a data or file called file metadata [7]–[11]. Metadata which is data in data and attached to a digital file can be used as a medium to describe all information needs related to chain of custody documentation. However, until now there is no mechanism and means to implement information needs for metadata that supports the need for a chain of custody for evidence [12]–[14].

Given the importance of national digital evidence management solutions in the cyber-crime investigation process the research focused on identifying and modeling correlations with digital image metadata security approaches. Correlation analysis reads metadata characteristics, namely document files, sounds and digital evidence correlation analysis using standard file maker parameters, size, file type and time combined with digital image metadata. National scale design requires the highest level of security. Security enhancing solutions can be encrypted against digital image metadata (EXIF). Perform EXIF Metadata readings that are in the original digital image based on the EXIF 2.3 Standard ID Tag, then encrypt and insert it into the last line (End of File). The description process will return EXIF decryption results in the header image as before. This can secure EXIF Metadata information without changing the image quality.

In the study revealed digital forensic land, images or images are one of the many digital evidence objects that can be found in computers, smartphones, internet, and file transfers, and can be used as evidence in investigations [12], [15]. When capturing using a camera, or creating an

Received: February 11, 2019; Revised: July 17, 2019; Received: July 30, 2019; Published: August 31,2019 

ISSN 2527-1682 (Print)
ISSN 2527-9165 (Online)

image/image file, it not only makes color images, but the date, time, device, and all camera configurations will be stored there [16]–[18]. Information that is in a file/data is called metadata. For example, Microsoft Word document data in which there is a metadata author's name, dates created/modified. This metadata is very useful for investigators. Specifically, images obtained from a camera will have Exchangeable Image File Format (EXIF), which stores all information about the camera [19]–[22]. For modern digital cameras and smartphone cameras, besides being able to save configuration information and camera dates, you can also save GPS locations (latitude and longitude) [23]–[26].

## II. METHOD

The flow of metadata file design with predefined parameters from metadata systems/tools in developing high-security digital evidence metadata analysis for national scale use. Here's a flow of national digital evidence metadata design:

At the analysis stage of the encryption and decryption process carried out with the Extended Tiny Encryption Algorithm on the EXIF file metadata above there are three parts, namely the process of identifying and retrieving EXIF metadata in the original image file before being encrypted and after encryption, the second is the encryption process against EXIF metadata files the image before the image is published, and the third is the decryption process of the EXIF image file metadata to ensure that the image matches the original owner [12].

Then after the evidence is found, then the investigator will check the file metadata using a digital proof system that has a high level of security to be used on a national scale.

## III. RESULT AND DISCUSSION

Standards that handle information or NISO (National Information Standards Organization) explain that metadata is "a structure of information that describes, explains, put in place or makes it easier to find things, use or manage an information source". Metadata is often called data about data or information about information.

Through the metadata contained in digital images, you can find stored information such as information about when pictures were taken, photographers who have taken pictures, equipment used, equipment settings, equipment serial numbers/cameras, lens type, location, flash, and other configurations.

### A. Analysis of EXIF Metadata Description

Exchangeable Image File Format (EXIF) was created by the Japan Electronic Industries Development Association (JEIDA) and is used to describe metadata. Images can have metadata or even do not have metadata. Due to the fact that EXIF information that stores information about images, can cause privacy problems, especially information that describes the time and dates the image was taken, the location of the image was taken, and the authenticity of the image.

### B. JPEG Analysis

Joint Photographic Experts Group (JPEG) is a standard image file committee based on the International Organization (ISO) Standard. JPEG images support up to 24bit of color. The use of image file compression with the lossy method can reduce the size of the image, but the image will be distorted if the compression is too high. Compression can be used to adjust between image files and storage, but the image/image will be affected. Usually only known image files as JPEG. However, there are two different format subsets, namely JPEG / EXIF and JPEG / JFIF.

JPEG is a standard for determining image file codecs (image extensions), and not what defines how images are compressed and decompressed by the flow of the image into a new image. It is the EXIF and JFIF standards that determine the general format used for image exchange (compressed JPEG).

The fact that appears in the field, many Smartphones are purchased by prioritizing the quality of the camera embedded in the Smartphone. As reported by www.petapixel.com written by [27], of the 2 billion smartphone users in the world, 92% used their smartphones to take photos. So, the frequency of JPEG image files is very large compared to other image files.

JPEG / EXIF is the most widely used standard today, considering that JPEG / JFIF has a deficiency in the encode and decode process. JFIF uses the APP0 marker, while EXIF uses the APP1 marker. Extensible Metadata Platform (XMP) which is another standard for storing metadata, also stored in the APP1 segment on EXIF metadata.

### C. EXIF Metadata File JPEG

A JPEG file contains several parts, each part contains a type of data that is limited by 2byte codes called markers. Markers in the form of hexadecimal begin with the code 0xFF and end with a 1byte code that indicates a marker. Some markers only consist of 2byte, the other is followed by 2 bytes which show the length of the payload of data with the next special marker. The length includes 2byte, but not for markers.

### D. EXIF Metadata Manipulation

EXIF metadata can be manipulated, either edited or deleted. Many open-source tools and operating system tools can manipulate EXIF metadata. EXIF metadata that has been edited or deleted cannot be returned without having the original file or backup of EXIF metadata.

### E. Data Integrity Analysis and EXIF Metadata Encryption Security

Several methods are used to analyze encryption, EXIF digital image file metadata, among others [12]:

1. Key Sensitivity Analysis

Key sensitivity is very important in cryptographic systems. Key sensitivity testing aims to see the results of decryption that is done using a different key. If the original image can be decrypted or can look similar using the wrong key, the encryption algorithm that is applied cannot be used.

2. Visual Analysis

Visual analysis techniques are used to see changes visually, both from the image side and from the hexadecimal side. Visual analysis from the image side compares digital images in each step of encryption-decryption. While hexadecimal visual analysis is done to compare hexadecimal data in digital images at each stage of encryption-decryption. In this analysis, you only need the tool image viewer and Hex Editor Neo.

3. Analysis of File Size

Analysis based on the size of the file capacity is done to see how much change occurs in digital images at each stage of encryption-decryption. This is intended to avoid the suspicion of third parties when digital images have been published. The normal threshold for file capacity changes cannot be more than 25% of its original size.

4. Histogram Analysis

The histogram analysis technique is used to see the suitability of color distribution in a digital image. If the digital image histogram has similarities between the original digital image, after encryption and after decryption, it can be said that the consistency of the digital image is maintained even though there are changes in the metadata. This is said to be the encryption process produced while maintaining digital color security in the image.

5. Hashing Analysis

Hashing or hash function is a method used to change text or messages into random characters called message digest Hash is a form of cryptography that is classified into an unkeyed cryptosystem using an algorithm to produce a row of text.

Hash function to check the integrity of the original digital image with a digital image after being decrypted. So that it can ensure that the digital image that has been decrypted is the same as the original digital image.

## IV. CONCLUSION

The development of national digital evidence metadata security must have high-level security standards, so it is recommended to use EXIF metadata encryption by retrieving it based on the id tag by referring to the EXIF 2.3 Standard, then encryption. Then it is inserted into the last line of the image bit. The decryption process returns EXIF encrypted metadata to the header image position.

## V. REFERENCES


[1] A. Kadir, *Pengenalan Sistem Informasi*. Andi, 2003.

[2] A. Abugharsa, A. S. Basari, and hamida Almangush, "A New Image Encryption Approach using Block-Based on Shifted Algorithm," vol. 11, Jan. 2012.

[3] APJII, "Hasil survey," 2018. [Online]. Available: https://www.apjii.or.id/survei2017.

[4] P. Alvarez, "Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis.," *IJDE*, vol. 2, no. 3, 2004.

[5] A. Argawal, "Tools for Managing EXIF Data of your Images," 2014. [Online]. Available: http://www.labnol.org/software/EXIF-data-editors/14210/.

[6] F. Alanazi and A. Jones, "The Value of Metadata in Digital Forensics," in *2015 European Intelligence and Security Informatics Conference*, 2015.

[7] S. Raghavan and S. V Raghavan, "AssocGEN : Engine for analyzing metadata based associations in digital evidence," in *2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering ({SADFE})*, 2013.

[8] S. Raghavan and S. V Raghavan, "Eliciting file relationships using metadata based associations for digital forensics," *{CSI} Trans. {ICT}*, vol. 2, no. 1, pp. 49–64, Mar. 2014.

[9] S. Raghavan and S. V Raghavan, "A study of forensic and analysis tools," in *2013 8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE)*, 2013.

[10] L. Woolcott, "Understanding Metadata: What is Metadata, and What is it For?," *Cat. Classif. Q.*, vol. 55, no. 7–8, pp. 669–670, Sep. 2017.

[11] D. Ratnasari, "Membangun Model Informasi Metadata Untuk Mendukung Chain of Custody Bukti Digital," UII, 2018.

[12] H. Wijayanto, "Peningkatan Keamanan Citra Digital Menggunakan Teknik Enkripsi EXIF Metadata dengan Extended Tiny Encyption Algorithm," UII, 2016.

[13] I. Sebestyen, "{JPEG}: Still image data compression standard," *Comput. Stand. Interfaces*, vol. 15, no. 4, pp. 365–366, Sep. 1993.

[14] B. Sugiantoro and Y. Prayudi, "Metadata Forensik Untuk Analisis Korelasi Bukti Digital," vol. 10, no. 1, pp. 85–89, 2018.

[15] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 3rd ed. Orlando, FL, USA: Academic Press, Inc., 2011.

[16] S. Bajpai and K. Saxena, "Techniques of steganography for securing information: A survey," *Int. J. Emerg. Technol.*, vol. 3, no. 1, pp. 48–54, 2012.

[17] G. K. Birajdar and V. H. Mankar, "Digital image forgery detection using passive techniques: A survey," *Digit. Investig.*, vol. 10, no. 3, pp. 226–245, Oct. 2013.

[18] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[19] P. Clark, "Digital Forensics Tool Testing – Image Metadata in the Cloud," *Dep. Comput. Sci. Media Technol.*, pp. 1–54, 2011.

[20] R. Crossley, E. Asimakopoulou, S. Sotiriadis, and N. Bessis, "A Study on Metadata Tagging for Tracking Original File Information within the Cloud," in *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*, 2013.

[21] L. Drive, M. Hall, C. Hill, K. Woods, A. Chassanoff, and C. A. Lee, "Managing and Transforming Digital Forensics Metadata for Digital Collections," *10th Int. Conf. Preserv. Digit. Objects*, no. November, pp. 203–208, 2013.

[22] L. Febriasyah and I. Riadi, "Analisis Keterlibatan Cyberterorism Menggunakan Metode Analitycal Hierarchy Process (AHP)," UII, 2018.

[23] F. Maruf, I. Riadi, and Y. Prayudi, "Merging of Vigenére Cipher with XTEA Block Cipher to Encryption Digital Documents," *Int. J. Comput. Appl.*, vol. 132, no. 1, pp. 27–33, Dec. 2015.

[24] N. Garnasih and B. Erfianto, "Analisis Perbandingan Performasi Algoritma Kriptografi TEA( Tiny Encryption Algorithm), XTEA , dan XXTEA Untuk Proses Enkripsi dan Dekripsi Data," Universitas Telkom, 2010.

[25] G. Hanchinamani and L. Kulakarni, "A New Approach for Image Encryption Based on Cyclic Rotations and Multiple Blockwise Diffusions Using Pomeau-Manneville and Sin Maps," *J. Comput. Sci. Eng.*, vol. 8, no. 4, pp. 187–198, Dec. 2014.

[26] C. K. Huang *et al.*, "High security image encryption by two-stage process," in *2009 7th International Conference on Information, Communications and Signal Processing ({ICICS})*, 2009.

[27] M. Zhang, "The Importance of Cameras in the Smartphone War," 2015.