Encryption EXIF Metadata for Protection Photographic Image of Copyright Piracy

By Imam Riadi

WORD COUNT 3721
TIME SUBMITTED 18-JUL-2017 02:49PM
PAPER ID 30576099

ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

Encryption EXIF Metadata for Protection Photographic Image of Copyright Piracy

Hendro Wijayanto[1], Imam Riadi[2], Yudi Prayudi[3]

[#1] hw.wijayanto@gmail.com, [#2] imam.riadi@mti.uad.ac.id, [#3] prayudi@uii.ac.id
[#1] Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia
[#2] Department of Informatics Engineering, Universitas Ahmad Dahlan, Yogyakarta, Indonesia
[#3] Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia

ABSTRACT
Many photographic images that are published to particular interests. This makes it more and more copyright piracy of images. In this study will make a tools and methods that can be used to protect the copyright of the digital image. The most important part of the digital image is a color image composition or texture images and EXIF metadata information contained therein. Image color and texture of the image reflects the beauty of the digital image. While reflecting the EXIF data information from digital image. In the science of cryptography many common cryptographic algorithms to secure data or information from copyright piracy. One of them is the eXtended Tiny Encryption Algorithm (XTEA) which is a cryptographic technique and operates in 64-bit block size and a 128bit key length. EXIF metadata in encrypted with XTEA, then insert it into End of File image, and delete the original EXIF, is expected to secure a digital image of the copyright piracy without changing primary data image. From the results of the encryption-decryption process, EXIF information and pixel digital image can be protected. There is a shrinkage of the size of the file capacity of -25.15% from size of original image, because image have a change in the type of EXIF metadata to JFIF format. This change only in bits header image, so that 74.85% of primary data bits are not changed.

General Terms
Security.

Keywords
EXIF, Metadata, Cryptography, Steganography, Image.

1. INTRODUCTION

In the digital forensics, the image is one of the many objects of digital evidence that can be found in computers, smartphones, internet and file transfer, which can be used as evidence in forensic investigations [1]. When performing a capture with a camera, or create an image file, not just make a color image, but also the date, time, device, and the entire camera configuration is stored therein [2]. Specifically, the images obtained from a camera will have the Exchangeable Image File Format (EXIF), which stores all the information about the camera [3]. Modern digital cameras and smartphone cameras, in addition to store configuration information and the date of the camera, also can store GPS location (latitude and longitude) [4]. Copyright abuse usually frequent manipulation of metadata information. To ensure the original image or not, can be seen from the information EXIF metadata [5].

Techniques are required to secure the EXIF metadata of the changes that are not desired by the holder of a patent on digital image. Cryptography technique is a technique for securing data by way of scrambling for the purpose of data can not be read by third parties. One of the cryptographic algorithm that eXtended Tiny Encryption Algorithm (XTEA).

XTEA algorithm has a concept that operates within a block size of 64 bits and a key length of 128 bits. In the process, this algorithm has a normal size 64round 32siklus. XTEA algorithm also known as the principle that stands out is small, secure, simple and fast [6].

EXIF Metadata encrypts the digital image using an algorithm XTEA then paste them into digital images to the latest data (end of file), is expected to enhance the protection of the EXIF information is digital image copyright information.

2. LITERATURE REVIEW

2.1 EXIF Metadata

Metadata is data information from the data. For example, a Microsoft Word document metadata that contains the date of manufacture, the manufacturer / author, modification date, and so on. In particular, digital image produced by the camera have any kind of metadata called eXchangable Image File Format (EXIF), which was created by the Japan Electronic Industries Development Association (JEIDA) as the camera image formats to ISO standard 12234-1 [5][7][8]. Many companies cameras such as Canon, Sony, Kodak even a camera that uses the EXIF header of the image photographic results. This header is in "application segment" of the JPEG file [9] show in Figure 1.

SOI	Start of Image
SOF0	Start of Frame (Baseline DCT)
SOF2	Start of Frame (Progressive DCT)

ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

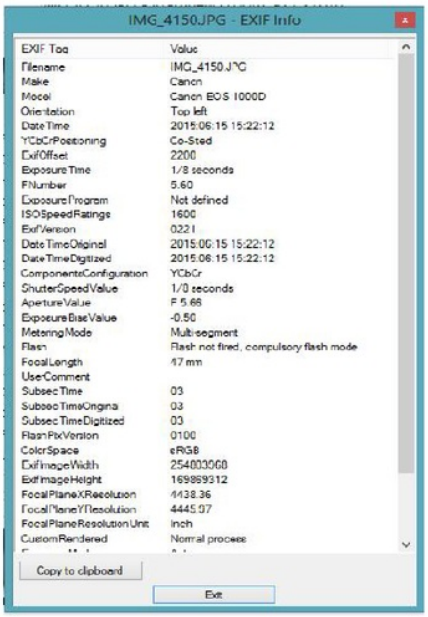
DHT	Define Huffman Table(s)
DQT	Define Quantization Table(s)
DRI	Define Restart Interval
SOS	Start of Scan
RST*n*	Restart
APP*n*	Application specific
COM	Comment
EOI	End of File

Figure 1. JPEG File structure (International Telecommunication Union, 1988)

EXIF metadata in JPEG files can be used to view the data information from the photographic image. In addition it can also be used to ensure the authenticity of the image, knowing the source image and digital image makers [5].

Examples of EXIF metadata in digital image such as an Figure 2 which uses Canon cameras EOS1000D, and tools IrvanView.

(a)



(b)

Figure 2. (a) Digital Image Original (b) EXIF Metadata

Each EXIF information contained in Figure 2(b) has Id Tag, Image File Directory (IFD), Key, and Data Type. [10].

2.2 eXtended Tiny Encryption Algorithm (XTEA)

EXtended Tiny Encryption Algorithm (XTEA) is a symmetric block cipher algorithm that is designed to enhance TEA algorithm. XTEA operate within a block size of 64 bits and a key length of 128 bits. That distinguishes it from TEA is Feistel and scheduling function keys that are used. On the odd round use K [sum & 3], while the round is even used K [sum >> 11 & 3] [11] . In the implementation XTEA algorithm will divide the plaintext into two blocks, each of which has a value of 32bits, which block z and y block. To lock with a length of 128bits divided into four blocks, namely K [0] = 32bits, K [1] = 32bits, K [2] = 32bits and K [3] = 32bits [11], XTEA will process the looping until the round is completed, as shown in Figure 3.

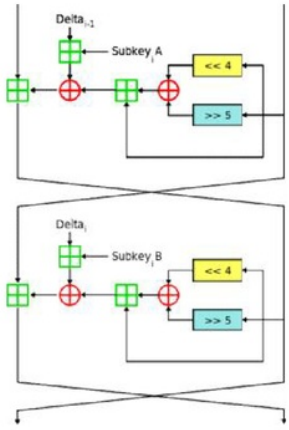


Figure 3. One round Feistel Encryption In XTEA

Figure 3 can be clarified with the information in Table 1

Table 1. XTEA Notation

Symbol	Information
$\boxplus$	Modulus 2^{32}
$\oplus$	OR
$\ll$	Shift to Left
$\gg$	Shift to Right

In the implementation XTEA using delta (√5-1) 232 or can be synchronized with the hexadecimal value 9E3779B9, and always remain in each process, the following is a mathematical calculation of the encryption process on XTEA [11] :

Round 0:
y + = (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3];
(1)
sum + = delta;
Round 1:

ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

z + = (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3]; (2)

The process of running a number of rounds were used, 32 round or 64 rounds. While the mathematical calculations for the decryption process in which XTEA :

Round 0:
z - = (y << 4 ^ y >> 5) + y ^ sum + k[sum >> 11 & 3]; (3)
sum - = delta;
Round 1:
y - = (z << 4 ^ z >> 5) + z ^ sum + k[sum & 3]; (4)
Until now XTEA still said to be safe to do the encryption, but the number of rounds that are used in the process is not deducted from 32 round [6].

2.3 End of File
EOF or End of File is one of the techniques used in steganography. This technique uses a way to insert the data at the end of the file. This technique can be used to insert data size according to needs. The size of the data file that has been inserted together with the size of the file before it inserts the data coupled with the size of the data inserted into the file. In this technique, data is inserted at the end of the file with a specially marked as the start of the identification data and the final identification of the data[13].

3. METHODOLOGY

The increased importance of the security picture is when a photographer took a picture of an object with a digital camera, and wanted to show it to be visible to the general public, this will make the digital image easily recognized and taken up by others. Metadata can be modified and it is possible there will be other parties who claim the photographic work, and this will harm the original image owners.

A photographer who wants to publish his work both through online media as well as file transfer, encryption EXIF beforehand. It is caused when the digital image has been published, it is easily accessible and can easily be done with the aim of changes EXIF copyright abuse. Photographers will be easy to prove to law enforcement if his claimed another party or abused in a way to decrypt the digital images have been published. As for the design of encryption-decryption EXIF metadata using XTEA shown in Figure 5.

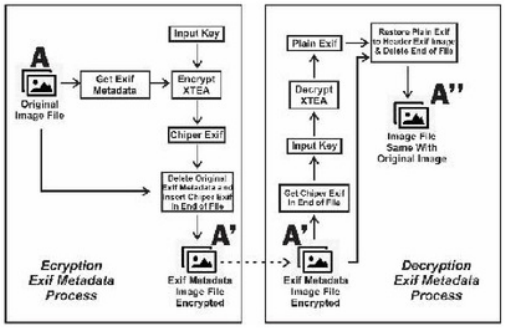


Figure 5. Design of encryption-decryption EXIF Metadata with XTEA

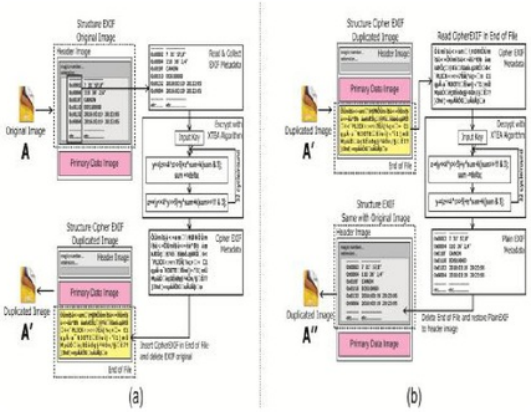


Figure 6. (a) EXIF Metadata processing scheme Encryption Algorithm XTEA

(b) EXIF Metadata processing scheme Decryption Algorithm XTEA

Design in Figure 5 will be implemented in the form of encryption-decryption application using algorithms XTEA EXIF metadata. The process of reading EXIF metadata based on tags id digital images according to the EXIF 2.3 standard released by the CIPA (Camera & Imaging Products Association). There are 310 Id EXIF metadata owned EXIF2.3. All of which are standard for photographic or video image. In this study, all of the metadata contained in the picture will be taken everything to be encrypted. The steps illustrated in Figure 6.

The encryption process is done after reading EXIF metadata of digital images is completed, the process like Figure 6 (a) and is described :

1. Input file digital image.
2. Reading all the information EXIF metadata based tag id (as shown in Figure 6 (a).
3. Input Key with a length of 16 characters, or 128 bits, and the value of Z.

ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

4. Before start the encryption XTEA first to grant that EXIF metadata into two blocks, namely block y and z blocks, each block worth 32 bit, and divide into 4 blocks key lock is K [0], K [1] , K [2], K [3], which also each worth 32 bit.
5. Encryption XTEA by the formula: y + = (z ^ z << 4 >> 5) + sum + z ^ k [sum & 3]; sum + = delta; for each round even, and using the formula: z + = (y << 4 ^ y >> 5) + y ^ sum + k [sum >> 11 & 3]; for every odd round.
6. Stages numbers 4 and 5 be repeated 32 times, to get the cipher EXIF.
7. Remove the original EXIF metadata, and insert EXIF encrypted (cipher EXIF) at the end of primary data digital imagery (end of file). Then formed a new digital image that does not have EXIF information.

For the decryption process EXIF digital image, shown in the schematic Figure 6(b) with the following steps :

1. Input digital image file that has been done encryption EXIF metadata.
2. Doing readings cipher EXIF who are in end of digital image files based on the marker at the end of the image data.
3. Input Key with a length of 16 characters, or 128 bits, and the value of Z.
4. Before decryption XTEA first to grant that EXIF metadata into two blocks, namely block y and z blocks, each block worth 32 bit, and divide into 4 blocks key lock is K [0], K [1], K [2], K [3], which also each worth 32 bit.
5. Decryption XTEA by the formula: z = (y << 4 ^ y >> 5) + y ^ sum + k [sum >> 11 & 3]; sum - = delta; for each round even, and using the formula: y- = (z ^ z << 4 >> 5) + sum + z ^ k [sum & 3]; for every odd round.
6. Stages numbers 4 and 5 in the decryption process be repeated 32 times, to get a plain EXIF.
7. Remove the cipher EXIF at the end of the file and returns plain into the EXIF header image, so that the digital image again have EXIF metadata.

4. RESULTS AND DISCUSSION

In the enhanced security uses the concept of digital image encryption algorithm XTEA EXIF metadata, digital image used is the digital image with JPG / JPEG. This is because only owned by the image EXIF digital camera results with standard extensions JPG / JPEG.

This stage will be conducted trials comparing the original image, image after image after encryption and decryption. These trials include visual analysis based on changes in image pixel color and change the details EXIF metadata and change information in hexadecimal image.

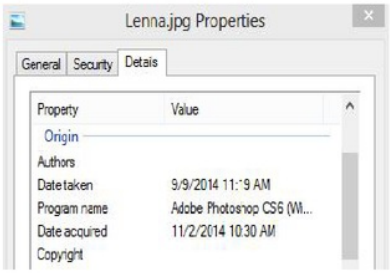
4.1 Visual Analysis

Visual analysis of the process encryption-decryption EXIF metadata using XTEA showed no changes in terms of color and pixel image, this image file Lenna.jpg for example, shown in Figure 7.

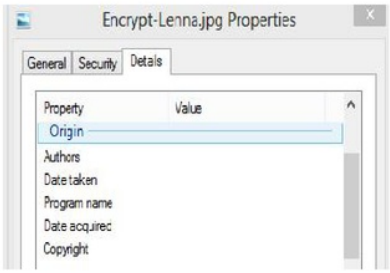
(a) (b) (c)

Figure 7. (a) Original Image
(b) Encrypted EXIF Image
(c) Decrypted EXIF Image

A color image and a depth of color (pixels) has a different layout to the EXIF data in an image. A color image and a color depth of the primary data is located within the digital image, while being in the EXIF header of the image. The process of improving the security of the algorithm EXIF metadata XTEA able to hide and restore EXIF metadata after the encryption-decryption. This is shown in Figure 8. In Figure 8(b) shows that the digital image has been done encryption, does not have EXIF metadata (hidden in cipher form at End of File Image).



(a)



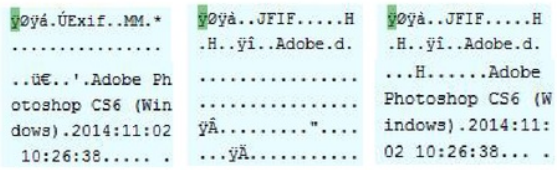
(b)

ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

(c)

Figure 8. (a) Detail EXIF image original
(b) Detail EXIF image after encryption
(c) Detail EXIF image after decryption

Visual analysis can also be based on hexadecimal. In the original image of the camera photography, metadata contained within the image has EXIF metadata types. While the original image is processed using an application or software editor, metadata will be of type JFIF (JPEG File Interchange Format). This difference can be shown in Figure 9.



(a) (b) (c)

Figure 9. (a) Hexadecimal image original
(b) Hexadecimal image after encryption
(c) Hexadecimal image after decryption

Based on the Figure 9, changes occur in the type of digital image metadata header after the encryption-decryption. Changing the type of metadata will affect the shift bit metadata when the metadata is returned into the header image. Although the type of metadata is changed, will not reduce the pixel image and the metadata information.

4.2 Data Capacity Analysis

Changes that occur as a result of shifting bits of data and changes the type of metadata in the header image causes a reduction in the capacity of the size of the digital image. These changes are shown in Table 2.

Table 2. Result of Data Capacity Analysis

Name and File Type	Original Image (*bytes*)	Image After Decryption (*bytes*)	Percentage
Lenna.jpg	54.123	40.799	- 24.62%
Mandrill.jpg	66.925	42.834	- 36.00%
F1.jpg	56.210	42.623	- 24.17%
House.jpg	67.987	53.328	- 21.56%
Splash.jpg	44.317	32.799	- 25.99%
Tiffany.jpg	50.537	38.612	- 23.60%
Sailboat.jpg	75.155	59.137	- 21.31%
Peppers.jpg	58.823	44.748	- 23.93%

The formula calculating the percentage change in each digital image is as follows:

$$\mathbf{N} = \frac{\boldsymbol{A''} - \boldsymbol{A}}{\boldsymbol{A}} \times \mathbf{100}$$

explanation:
N = percentage of chage
A = original image
A'' = image after encryption EXIF Metadata

As for calculating the average value of the percentage change in the whole digital image as follows:

$$\boldsymbol{\beta} = \frac{\boldsymbol{N1 + N2 + N3 + \cdots Nn}}{\boldsymbol{n}}$$

explanation :
β = average percentage of change
N1,N2,N3…Nn = percentage of change every image
n = amount of image sample

Depreciation is the file size of the original image size is influenced by several causes, that is:

1. Change the type of the original EXIF metadata into a JFIF (illustrated in Figure 9).
2. Delete EXIF metadata during the encryption process. So that the digital image does not have EXIF data allocation. This is shown in Figure 10(b) which is the result of the encryption. Where the end of primary data which was originally 54.112 bytes (Figure 10a), dipped to 32.966 bytes after encryption (Figure 10b)
3. Restore CipherEXIF into the EXIF header that has different types of metadata (JFIF) so that the length of the header between the original digital image and after decryption shrinkage. This will affect the total bit length of the image (Shown in Figure 10d).

ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

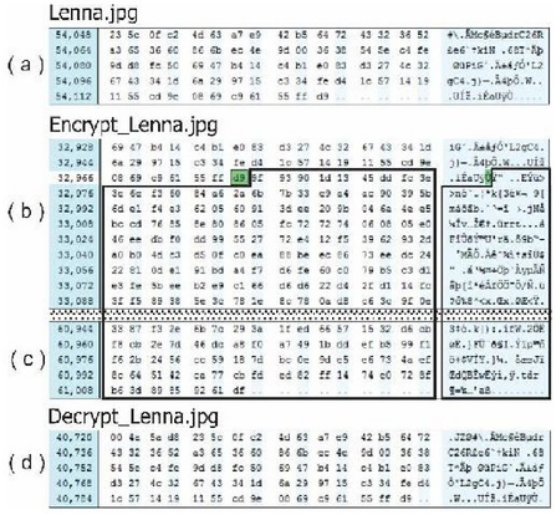


Figure 10. (a) Hexadecimal Image Original.
(b) Hexadecimal After Enkripsi.
(c) End of File CipherEXIF.
(d) Hexadecimal After Decryption.

The percentage of -25.15% shrinkage occurred in the original image header. So 74.85% the image data has not changed. Data that does not change is the primary data, which in this primary data representing the image of the composition of the image. This is reinforced by the histogram analysis result as Table 4.

4.3 Histogram Analysis

Each image has a color composition gray, red, blue and hiijau in each pixel. The composition of colors is what will fill the color values in a single pixel digital image. A color change that occurs in one pixel, will affect the value of the image histogram.

In the process of encryption-decryption digital image EXIF metadata, histogram analysis is needed to know is there any difference in terms of pixels. The results of the analysis are shown in Table 3.

Table 3. Result of Histogram Analysis

Name & File Type	Original Image	Image After Encryption	Image After Decryption	Result
Lenna.jpg	124.06	124.06	124.06	Match
Mandrill.jpg	121.90	121.90	121.90	Match
F1.jpg	179.19	179.19	179.19	Match
House.jpg	161.49	161.49	161.49	Match
Splash.jpg	103.24	103.24	103.24	Match
Tiffany.jpg	211.01	211.01	211.01	Match
Sailboat.jpg	125.26	125.26	125.26	Match
Peppers.jpg	120.44	120.44	120.44	Match

Histogram analysis results in Table 4 are based on the average color of gray (Luminosity) image, with the same amount every stage of encryption and decryption. It membutikan that no changes to the primary data caused encryption-decryption on securing the EXIF metadata

5. CONCLUSION

After doing some things related to the design, testing and analysis of encryption-decryption security EXIF image metadata, EXIF metadata obtained results that can be secured by means of cryptography and steganography algorithms XTEA and inserted into the End of File image. Decryption process will return to the position of the encrypted EXIF header image intact. Pixel image is not affected by the encryption-decryption process, so it does not affect the primary data image. There is variation in the size of the file that caused the different types of metadata. Original image from the camera have EXIF metadata type, after processing by the application or software will turn into JFIF (JPEG File Interchange Format). These changes alter the capacity of the file size by an average of -25.15% from the size of the original image. Amounting to 74.85% the image data has not changed. This proves there is no change in the primary data encryption and decryption process. From these results, EXIF encryption techniques can be used for copyright protection of the photographic image.

Future work can be developed for the process of securing the file type and other types of metadata. This technique can be developed better in order to change the file size can be minimized. So that the original image can be exactly the same bits of the image with the image after decrypted.

6. REFERENCES

[1] S. L. T. S. Ho, *Handbook of Digital Forensics of Multimedia Data and Devices*. John Wiley & Sons, Ltd, 2015.

[2] T. Gloe, "Forensic analysis of ordered data structures on the example of JPEG files," *WIFS 2012 - Proc. 2012 IEEE Int. Work. Inf. Forensics Secur.*, pp. 139–144, 2012.

[3] K. S. John Evans, *Adobe Photoshop Lightroom CC*. Adobe Press, 2015.

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

[5] B. McMicken, "Using EXIF Metadata," *Int. Crime Scene Investig. Assoc.*, pp. 1–20, 2014.

[6] F. Maruf, "Merging of Vigenére Cipher with XTEA Block Cipher to Encryption Digital Documents," *IJCA*, vol. 132, no. 1, pp. 27–33,

ISSN (Online) 2278- 5841
ISSN (Print) 2320- 5156

2015.
[7] K. Malik Mohamad and M. M. Deris, "Visualization of JPEG metadata," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5857 LNCS, pp. 543–550, 2009.
[8] CIPA (Camera & Imaging Product Association), "CIPA DC- 008 - Translation - 2012," 2012.
[9] K. S. P. Rasmus R. Paulsen, *Image Analysis: 19th Scandinavian Conference, SCIA 2015, Copenhagen, Denmark, June 15-17, 2015. Proceedings*. Springer US, 2015.
[10] JEIDA (Japan Electronic Industries Development Association), "Metadata reference tables Standard Exif Tags," 2012.
[11] P. A. Kaminsky, "Intro to Cryptography XTEA Block Cipher," 2013.
[12] G. Sekar, N. Mouha, V. Velichkov, and B. Preneel, "Meet-in-the-Middle Attacks on Reduced-Round," 2011.
[13] I. Khan, S. Gupta, and S. Singh, "A New Data Hiding Approach in Images for Secret Data Communication with Steganography," vol. 135, no. 13, pp. 9–14, 2016.

AUTHORS PROFILES

Hendro Wijayanto, Currently he is a Postgraduate Student at Departement of Informatics Universitas Islam Indonesia Yogyakarta, Indonesia. Learning on Digital Forensic consentration at there university. His research interests include digital forensic, mobile forensic, steganography and cryptography.

Imam Riadi, Currently he is a Ph.D Senior Lecturer at Department of Informatic Ahmad Dahlan University and also at Department of Informatics Universitas Islam Indonesia Yogyakarta, Indonesia. His research interests include digital forensics, cybercrime, malware analysis and network security

Yudi Prayudi, Currently he is senior lecturer at Department of Informatics Universitas Islam Indonesia Yogyakarta, Indonesia. His research interests include digital forensics, cybercrime, watermarking, steganography, malware analysis and network security.

Encryption EXIF Metadata for Protection Photographic Image of Copyright Piracy

ORIGINALITY REPORT

2%

SIMILARITY INDEX

PRIMARY SOURCES

1	Lecture Notes in Computer Science, 2015. Crossref	22 words — 1%
2	Bahrami, Mehdi, and Mukesh Singhal. "A Light-Weight Permutation Based Method for Data Privacy in Mobile Cloud Computing", 2015 3rd IEEE International Conference on Mobile Cloud Computing Services and Engineering, 2015. Crossref	21 words — 1%
3	realideal.com Internet	14 words — < 1%
4	de.wikipedia.org Internet	9 words — < 1%
5	ismc.nga.mil Internet	9 words — < 1%
6	P. Israsena. "On XTEA-based Encryption/Authentication Core for Wireless Pervasive Communication", 2006 International Symposium on Communications and Information Technologies, 10/2006 Crossref	8 words — < 1%

EXCLUDE QUOTES OFF
EXCLUDE MATCHES OFF
EXCLUDE BIBLIOGRAPHY OFF