Scientific Journal of Informatics
Vol. 4 No. 1, May 2017

p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

Watermarking Techniques Using Least Significant Bit Algorithm for Digital Image Security Standard Solution-Based Android

Ari Muzakir[1], Mailan Habibi[2]

[1,2]Computer Science Faculty, Universitas Bina Darma
Email: [1]arimuzakir@binadarma.ac.id, [2]mailan_komering@yahoo.com

Abstract

Ease of deployment of digital image through the internet has positive and negative sides, especially for owners of the original digital image. The positive side of the ease of rapid deployment is the owner of that image deploys digital image files to various sites in the world address. While the downside is that if there is no copyright that serves as protector of the image it will be very easily recognized ownership by other parties. Watermarking is one solution to protect the copyright and know the results of the digital image. With Digital Image Watermarking, copyright resulting digital image will be protected through the insertion of additional information such as owner information and the authenticity of the digital image. The least significant bit (LSB) is one of the algorithm is simple and easy to understand. The results of the simulations carried out using android smartphone shows that the LSB watermarking technique is not able to be seen by naked human eye, meaning there is no significant difference in the image of the original files with images that have been inserted watermarking. The resulting image has dimensions of 640x480 with a bit depth of 32 bits. In addition, to determine the function of the ability of the device (smartphone) in processing the image using this application used black box testing.

Keywords: Watermarking, Least Significant Bit, Digital Images Security

1. INTRODUCTION

Mobile computing technology continues to evolve at this time is shown by the increasing number of smartphone owners. The development of mobile technology is currently more advanced smartphone technology and the personal computer (PC) has more advanced features. Since most smartphones now adopt the Android OS that makes users more familiar because the market is being controlled Android. With the Android makes the user easier to socialize with the media for the greatest android control for ease of sharing and in the presence of Android is not too busy in her appeal must use a PCs or Laptops. At present, the distribution of multimedia products not only be done offline but also online via the Internet. These conditions cause many problems relating to copyright or the copyright of content spread across the internet. One of the intellectual work that we need to protect is in the form of digital goods, such as software and multimedia products such as text, music (in MP3 or WAV format), picture or image (image), and digital video (VCD).

During this time doubling on digital products are already widely carried out independently and freely. Duplicated exactly the same as the original. The copyright holder of digital products is certainly very feel aggrieved because he did not receive royalties from the multiplication effort. Actually, copyright abuse on the field of

multimedia is not just about the duplication and distribution, but also on the label of ownership [4]. To anticipate threats to multimedia copyright need to do the insertion of a code or whatever, that is not visible to the human eye at a glance using watermarking techniques. Digital watermarking is a potentially good tool in enabling content protection [9].

Encryption can offer protection of confidentiality and integrity of the content, and the content is decrypted can be protected using a digital watermark. The processes of embedding watermarking signal into an image without significantly degrade visual quality. The goal of the digital watermark is to provide copyright protection for intellectual property in a digital format. Information or logo that is embedded in an image is called digital watermark image [3, 5]. Watermarking method which is well known to work in the spatial domain is the least significant bit (LSB), which replaces the most significant bits of pixels chosen to hide information [6].

2. METHODS

2.1. Research Methods

The method used in this research is using descriptive method of a paper that describes the actual state of the object under investigation, according to the actual circumstances at the time of the study directly. Descriptive method is a method used to describe or analyze the results of the study but not used to make broader conclusions [7]. Descriptive method is a fact-finding with the proper interpretation [1].

On the development of systems using mobile-D is a software development methodology specifically designed for mobile application development based on agile practices. Mobile-D stages, namely explore, initialize, productionize, Stabilize, and system test and fix [8]. These stages can be seen in Figure 1 below.

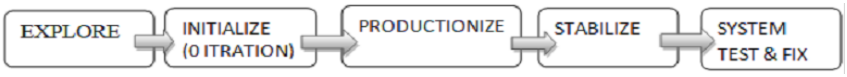


Figure 1. Stages methods of mobile-D [8]

In this study, a process that is done with regard to the process of securing media digital image on android smartphone as shown in Figure 2 below. The purpose of the security process is that these data are the copyright owner, so that people do not know the data has been inserted copyright.

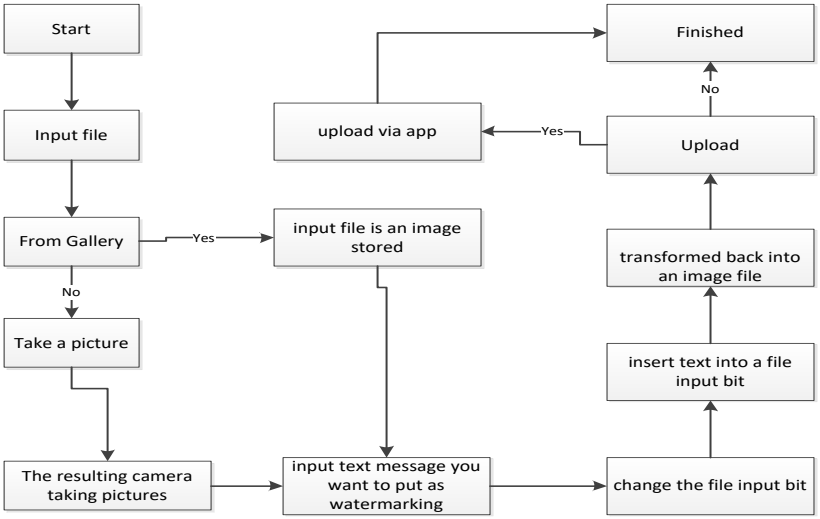


Figure 2. Flow process of watermarking using LSB on smartphones

2.2. Literature review

Digital Watermarking

Watermarking has existed since 700 years ago. At the end of the 13th century, a paper mill in Fabriano, Italy, making paper watermarked or watermark by pressing the print image or writing on the new paper semi-finished [4].

Digital image watermarking is similar to the concept of a physical object with the difference that the techniques used for digital watermarking is not a physical object. In the digital image watermarking, confidential information or logo that is embedded in another image in a way unseen. Confidential information or logo is called watermarks and contains some metadata, such as security or copyright headline data or images. The main image in which the watermark is embedded known as the cover image for include the watermark. Digital image watermarking system basically consists of watermark embedding and watermark detection as shown in Figure 3 [6].

Figure 3. Digital Image Watermarking [6]

***Least Significant Bit* (LSB)**

The most common method of watermark embedding is to embed a watermark into the least significant bit of object coverings. Although the method is simple, LSB substitution has many shortcomings. Although able to maintain transformations like cropping, in addition to one of the unwanted noise but more sophisticated attack that

can only be set LSB bits of each pixel into one fully able to beat the watermark with minimal impact to the object coverings. Once the hacker known algorithms, embedded watermark can be easily changed by him without any difficulty.

LSB are bits which if modified will not significantly affect the colors produced by the combination of the three RGB color components. An LSB bit is contained in the final 4 bits in one byte (8 bits) [2].

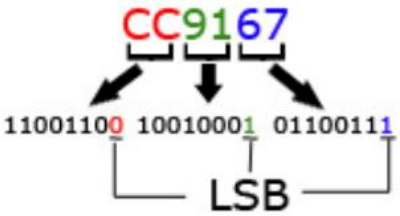


Figure 4. Example of Least Significant Bit (LSB)

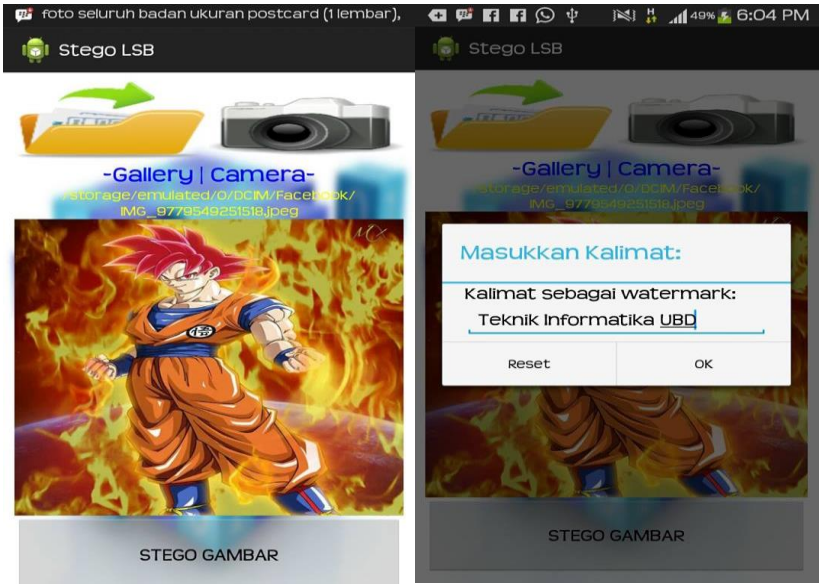
In figure 4 seen bits LSB at 1 pixel of color, planting information can be performed on these bits.
Example:

Preliminary data, three pixels of the image 24-bit
(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
The binary value of the character 'A' is
10000011.
Data after planting the character 'A'
(0010011**1** 1110100**0** 1100100**0**) → 100
(0010011**0** 1100100**0** 1110100**0**) → 000
(1100100**1** 0010011**1** 11101001) → 11

Only bits underlined that experienced changes.

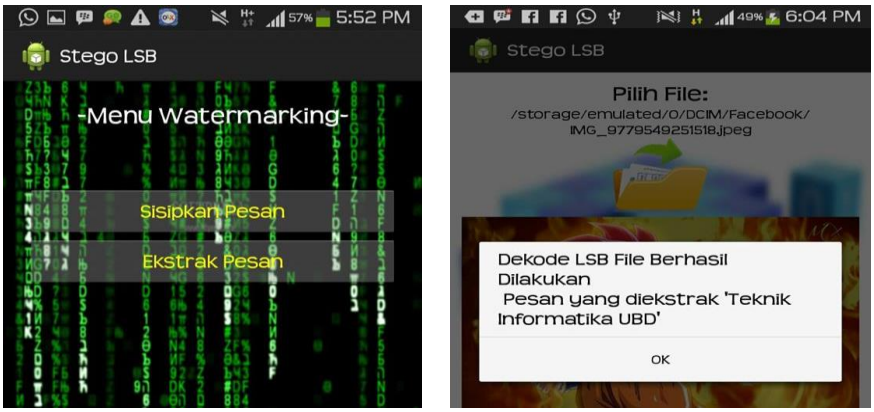
3. RESULTS AND DISCUSSION

Application security image is an application created to secure the data and insert images into a message formatted jpeg images, especially on mobile devices based on Android. The purpose of making application security image is to provide ease and convenience to the smartphone user who likes to take pictures, in this case more confidence smartphone users to store photos in social media because it has been inserted in the picture message. Results of the application made as in Figure 5 and 6 following.



(a) (b)

Figure 5. Results of application security picture (a) the process of taking pictures from the gallery. (b) insert the sentence that will be used as watermark



(a) (b)

Figure 6. Results of application security picture. (a) the menu was available at the time of securing the image (b) decoding process to extract the watermark message

In order for the implementation of truly meet the needs of the testing of the applications are built. Mechanical testing done of alpha testing. Alpha testing is done with a black box testing method. Black box testing focuses functional requirements of software. This test is trying to find fault among others.

(a) Functions that is incorrect or missing,

(b) Interface errors,

(c) Errors in data structures,
(d) Error performance.
The test plan can be seen in Table 1 below.

Table 1. Use of the application menu

Menu tested	This type of testing
Menu inserts a message	black box
Menu extracts message	black box

1. Testing insert a message

Table 2. Tests on the application menu insert a message

Test result		
Menu tested	Which are expected	Information
Menu inserts a message	Message is pasted on the image stored in the gallery	In line with expectations

2. Testing extract message

Tabel 3. Tests on the application menu extract message

Test result		
Menu tested	Which are expected	Information
Menu extracts message	Extract Shown preferred message images to be extracted and stored into memory or uploaded to social media	In line with expectations

The performance of security applications of digital image is tested, in this study only measures of several dimensions such as file type, size of the initial image, message length that will be inserted as a watermark, the final size after the watermark and the LSB, as well as the time of the process used at the time of encryption information , Testing only one file using JPEG images. The results are as shown in Table 4 below.

Table 4. Testing message insertion (by size and message encryption processing time)

File (JPEG)	The initial size (KB)	The length of the message	The final size (KB)	Process Time (sec)
Logo_informatika.jpg	4.74KB	160 character	11.6 KB	3.5 second
		480 character	12.8 KB	4 second
		1000 character	14.6 KB	5 second
		6500 character	29 KB	60 second

4. CONCLUSION

Security applications watermarking technique using images with the least significant bit algorithm based on Android have been built as a security application image using android mobile devices. Although using a smartphone device based on Android but still the message encryption process can be handled properly so as to provide

watermarking JPEG images without visible to the human eye. Process encoder at the time of extraction of the image file that has been given watermarking can be run very easily and quickly depending on the size of the message that is inserted at the time of insertion.

5. REFERENCES

[1] Frederick, Whitney. 1960. *The Element of Research*. New York: Prentice-Hall, Inc.

[2] Johnson NF, Jajodia S. 1998. *Exploring Steganography: Seeing the Unseen. George Mason University.* (Online) (http://www.jjtc.com/pub/r2026.pdf, accessed September 20, 2016).

[3] Katzenbeisser, S. and Petitcolas, F. 1999. *Information Hiding Techniques for Steganography and Digital Watermarking.* Artech House Books.

[4] Munir, Rinaldi. 2004. *Stegnography dan Watermarking*. Bandung. Institut Bandung.

[5] Saraju Prasad Mohanty. 1999. Watermarking of Digital Images. *Submitted at Indian Institute of Science Bangalore*, pp. 1.3–1.6.

[6] Sharma, Puneet. and Rajni. 2012. Analysis Of Image Watermarking Using Least Significant Bit Algorithm. *International Journal of Information Science and Technique (IJIST)* vol.2, No.2, No.4.

[7] Sugiyono. 2010. *Metode Penelitian Kuantitatif Kualitatif & RND*. Bandung: Alfabeta.

[8] VTT Electronics. 2006. Mobile-D™ is VTT's Methodology for Agile Software Development. (Online) (http://agile.vtt.fi/mobiled.html, accessed September 20, 2016).

[9] Woo, C.-S., J. Du, and B. Pham. 2005. *Geometrically Robust Digital Image Watermarking using Scale Normaization and Flowline Curvature.* in IS&T/SPIE 17th Annual Symposium: Security, Steganography, and Watermarking of Multimedia Contents VII. San Jose, CA, USA.