Watermarking Using LSB Shifting to Document Protection

by Suhendro Irianto

Submission date: 15-Jan-2020 09:58PM (UTC+0800)
Submission ID: 1242210606
File name: Watermaking_Using_LSB_Shifting_to_document_protection.pdf (551.2K)
Word count: 2601
Character count: 14005

ISSN 2277-3061
Volume 15 Number 12
INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

Watermarking Using LSB Shifting to Document Protection

Wasilah[1], Suhendro Y. Iriant[2]o,and Dona Yuliawati[3]
[1,2,3]Faculty of Computer Science, Darmajaya Informatics and Business Institute
Jl. Z.A Pagar Aam No.93, Bandar Lampung, Indonesia
Email: silamurni@gmail.com, suhendroirianto@ymail.com,donayuliawati@gmail.com

ABSTRACT

The original signature or document. The application demonstrates that it can be used to protect a document or signature from fraud by an authorize person. Criminal can be considered as Harmful act or omission against the public which the State wishes to prevent and which, upon con eviction, is punishable by fine, imprisonment, and/or death. No conduct constitutes a crime unless it is declared criminal in the laws of the country. Some crimes (such as theft or criminal damage) may also be civil wrongs (torts) for which the victim(s) may claim damages in compensation. Criminals may be happened in every sector and in daily life. Criminal acts may be in the form of copy right fraud and signature forgery. In this work we try to solve or prevent those criminals. By using watermarking technique, the work proposed to introduce new technique to protect document originality quickly and accurately. Watermarking was carried out by inserting an image or text into signature image in order to protect. The work shows that file size produced by integrating the two same files but on different file stored and also produce different file size. Moreover Testing shows that steganography of image file with JPEG format and file image hidden with JPEG format which produced other small size of file from file steganography storage such as BMP and PNG formats.

Indexing terms/Keywords

watermarking, Least Bit Significant, copy right.

Academic Discipline And Sub-Disciplines

Image Processing, Security System

SUBJECT CLASSIFICATION

Computer Science

TYPE (METHOD/APPROACH)

Experimental Research

INTRODUCTION

Fraud or violation to unauthorized copy right always happened repeatedly and become more complicate. Forgery to valuable documents and signature has fatal impact in many sectors. Therefore, protection to valuable documents and signatures is very important and critical. To resolve this problem, we tried to introduce as well as build an application to secure copy right of valuable documents from document scam.In computer vision and image processing, forgery or plagiarism can be overawed by using some techniques such as watermarking, image blending, and contect based image retrieval techniques. Watermarking technique was carried out by inserting a watermark into document or signature. Watermark can considered as digital signature of the owner multimedia products. Moreover, watermark inserted become copy right. Designation given to document by using water marking was carried out, so information inserted will not damage digital data protected. Therefore, to open multimedia product inserted with watermark, he/she does not realize that the product was inserted with watermark or digital signature. Previous researches showed that SVD based watermarking with dither quantization as well as edge detection can be used to produce modified image carried out by using many techniques [5]. Meanwhile, other researchers, water marking method was deployed together with removal DC method in DC audio digital inserted into binary image using an software [6]. The work also using digital watermarking with image RGB and correlation Discrete Cosines Transforms (DCT) method which carried out by comparing floating value [7]. This work using adaptive digital watermarking. Inserting digital image can be used to identify the owner of digital image protected [8]. Implementation of watermarking to protect documents was carried out by using Least Significant Bit (LSB) and use to insert code. The code is an image which considered as watermarking and inserted as a security code. A security inserted was invisible and it does not modify the original image [3].

WATERMARK PROCESSING

Inserting watermarking into an image is encoding. Encoding process can used as well as inserting key or without inserting key [2]. A key was needed in order to only an authorize person able to open documents. Key is also purposed to prevent deleting watermark by unauthorized person.

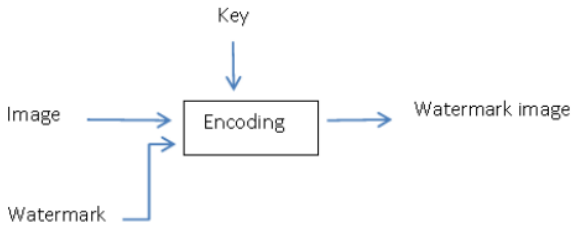

Figure 1. Watermark Process into image digital

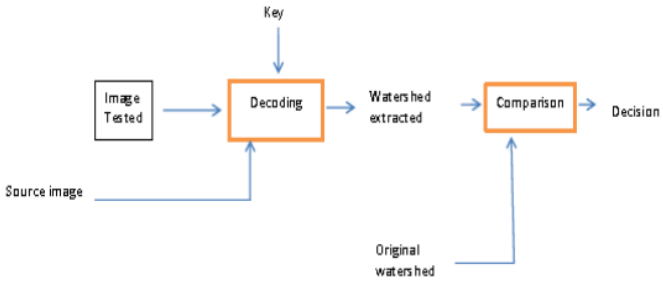

Figure 2. Verification Process in image digital

Verification watermark was carrier out to verify the ownership of document. Watermarking verification consist of two sub-processes namely: watermark extraction and comparison. Extraction process can be called as coding, it proposed to expose watermark from inside the image. Decoding can be carried out by using original image or without original image, decoding was deployed to improve performance of watermarking. Comparison process used to compare watermark revealed with original watermark.

Digital Watermarking

Digital watermarking considered as technique insert information into data using a certain method which cause watermark to be deleted or destroy [1]. Mainly, watermark consists of two types, visible and invisible watermarks [3]. *Visible watermark, this watermark* can see or visible for human being. Visible watermark has characteristic very robust due to its watermark easy to recognize and difficult to delete. In this case, the inserted watermark can be inserted as solid watermark or transparent watermark. This kind of watermark needs cropping to remove from the original image. *Invisible watermark, this kind of watermark* is not visible for human being but can be extracted by using certain computational method. The purposed of invisible watermark is to verify the ownership or verify the integrity image digital or information. It usually when extraction of invisible watermarking need a password which is called watermark key.

Least Significant Bit Hiding (LSB)

Image digital can be defined as a f(x,y) function, the function has M rows and N columns, where x and y are spatial coordinate whilst f is point of (x,y) coordinate. When x and y values, and amplitude f value that has finite discrete value. Incision value between rows and columns (at x,y position) and called as picture elements, image elements or pels or pixels[9]. *Least Significant Bi method considered as* one of watermarking methods that works in Red Green Blue R,G,B) mode. This method was carried out by inserting information into the most right bits from every RGB element. Change in the most right bit will only cause RGB value change 1 of 256 colors. LSB method directly manipulates intensity value from the number pixels. Hiding data can be carried out by replacing data bits in image segment with secret data bits. During replacing process there is one bit lost, and it is called Least Significant Bit (LSB). This LSB will be manipulated to insert watermark [4].

Image Shifting Operation

Shifting operation used to locate watermark or marked image as needed. The following is an equation used in watermark shifting.

$$Y_{step} = Y_{old} + S_y;$$

$$X_{step} = X_{old} + S_x;$$

By using the equation, we can have a new coordinate to locate pixel value of an image. In this work, the equation used to control watermark position relocation in the image. The equation uses Sy and Sx is a pixel, if Sy equal 5 the image shift to 5 pixels up, if Sx equal to 3 the image shifts 3 rights. When Sx and Sy have negative values then image will shift in opposite direction each other. Image rotating algorithm was deployed using transformation affine. It is used as image rotate and rotating used with the following equation:

ISSN 2277-3061
Volume 15 Number 12
INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} \cos(rad) & \sin(rad) \\ -\sin(rad) & \cos(rad) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

By using this equation an image can be rotated as radiant direction. Therefore when image rotated by 45^0 , radiant value will be $\pi/4$ radiant. Whilst, image scaling algorithm can be described when an image can be enlarge or minimized by making every pixel become few pixels. This work scaling was carried out by using ratio. This ratio can be obtained from comparing between high and width by *showing* (viewer), following ate equation of ratio between high and width.

$$S_h = Viewer_h / H$$

$$S_w = Viewer_w / W$$

Where high ratio S_h obtained from division between high viewer and original high. Whilst, width ratio obtained from division between division viewer and original width image.

RESULTS AND DISCUSSION

The algorithm constructed from this work is better algorithm compared to previous algorithms, the algorithm can be explained as follow:

\\ hiding image into image

1. *Input original image*
2. *Convert image into vector*
3. *Conver vektor to binary*
4. *Convert text into vector*
   mat= m x n matix

   Extract RGB component

   Go to 1

\\ restore hiden image inside image

1. *Convert hiden image into vector*
2. *Conver vectori into binary*
3. *Take the most rigth bit from each*

The application built from this work is very useful to hide of Intel logo image into document in order to protect the originality of document. Some outputs produced by this application can be examined on fig.6.

3.1.1. Snapshot Program Display

When the program run, on the screen will shows “beginning menu” this menu displays three sub-menus, namely: File, Steganography, and Help menus. The menu can be illustrated at the following figures:

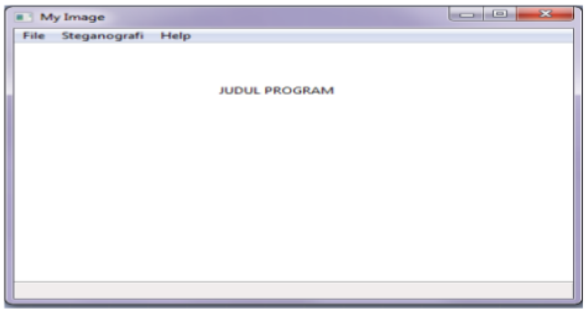

Figure 3. Screenshot Beginning Menu

Steganography Menu

Steganography menu provides watermarking process facilities. This process can be carried out by choosing cover image which has file format such as: PNG, JPEG, and BMB. After choosing file format, then pick hiden image going to hide. Steganography button should be pressed in order to display new image which message hidden inside the image or document. Next step is to save image or document into PNG and BMP formats. Snapshot of steganography menu can be showed at figure 4.

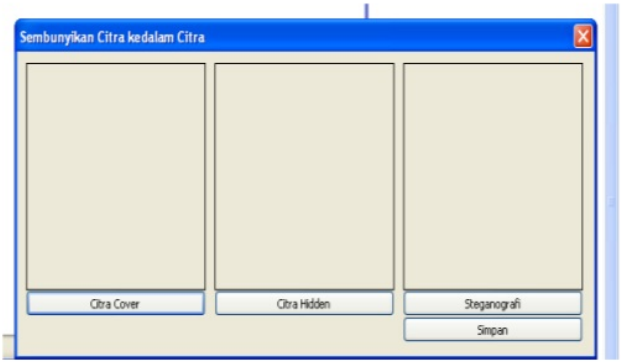

Figure 4. Snapshot of Steganography Menu

Another menu in this application it an inserting watermark into document or signature image , and it is proposed to protect document or signature from unauthorize person . The screenshot can be examined at figure 5.

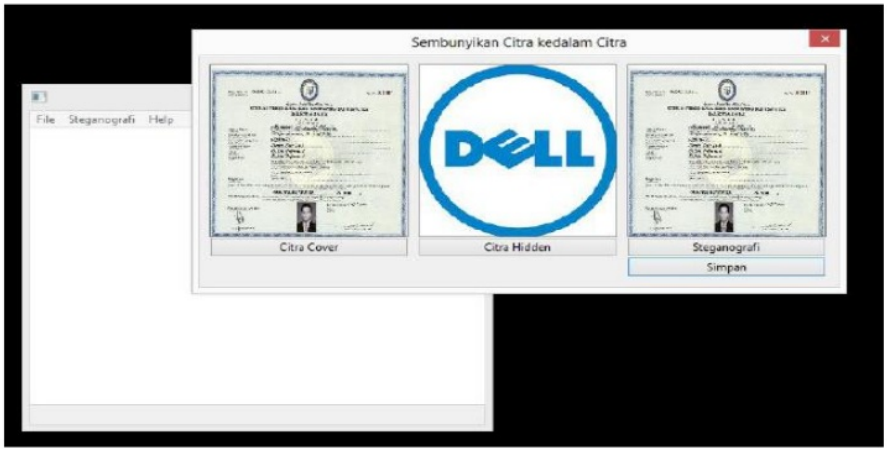

Figure 5. Snapshot of Inserting or hiding logo into document.

Watermark can be considered as a previous image inserted, but it can be re-extracted. Extraction result from document can be illustrated at figure 5.

Figure 6: Snapshot to show hidden logo in the document

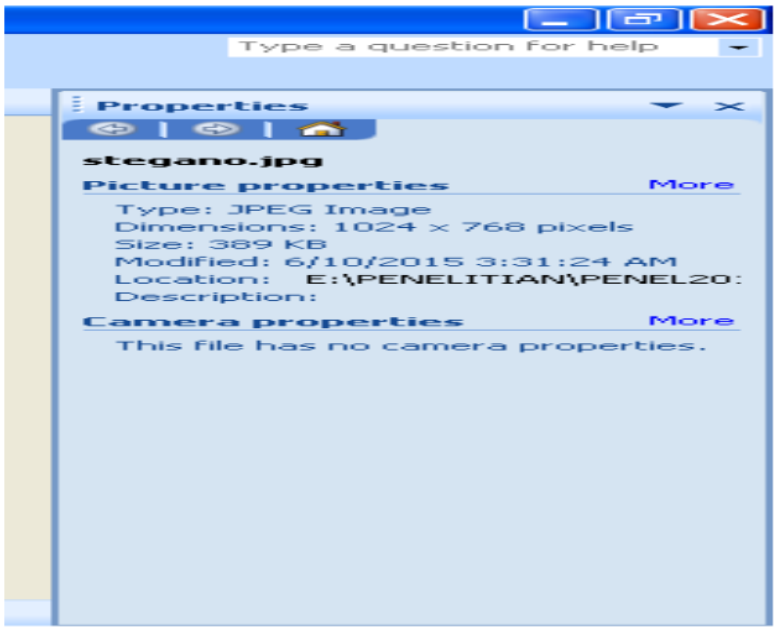

Figure 7: Snapshot size of source filer

The following screenshot at figure 8 is a file source with size 389 Kb , then it is inserted size image of 16.5 .

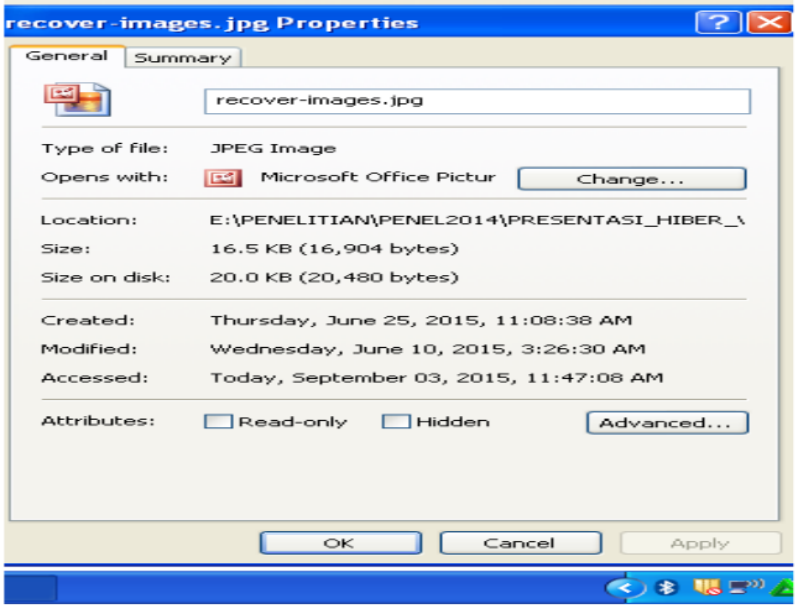

Figure 8: Snapshot of hidden file size

The result of integrating image file with JPEG format is file steganogrphy with size of 94.7 KB.

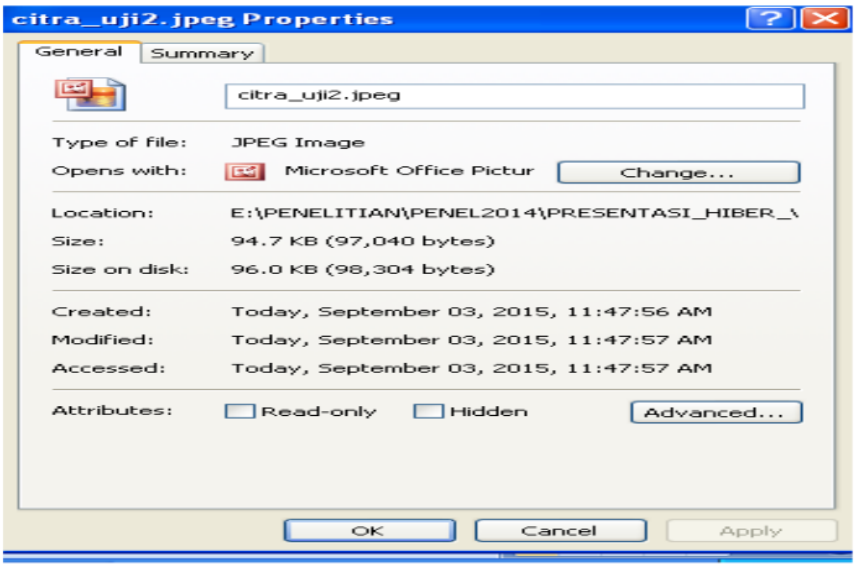

Figure 9. Display of file size Steganography.

Another testing also been carried out to file with BMP and PNG formats. This integration produces different files one and the other as illustrate in table 1, below:

Table 1. The different output files

Source File		Mark File		Output File	
Type	Size	Type	Size	Type	Size
JPEG	389 Kb	JPEG	16.5 Kb	JPEG	94.7 Kb
JPEG	389 Kb	JPEG	16.5 Kb	BMP	2.25Mb
JPEG	389 Kb	JPEG	16.5 Kb	PNG	975Kb

Table 1 shows that file size produced by integrating the two same files but on different file stored and also produce different file size. When extraction process was chosen with PNG and BMP formats. In the steganography image extraction process which has PNG and BMP formats, sequent recovery of hidden image process will be carried out. Due this process, hidden file will appear and will be saved into JPEG, PNG, and BMP formats.

CONCLUSION

The application was built and provides two processes, namely inserting watermark process and extraction process. Inserting watermark process was carried out by some steps: First, input original image then convert to vector form, vector form then converts to binary form. Sequently, input image binary which is hidden inside cover image binary according queue. Finally, converting process to be carried out by changes new binary value to decimal format and new image vector. Watermarked document can be recovered by extraction process which is extracting hidden image. This extraction can be done by some steps, namely: Convert watermark into vector form, then vector form convert into binary form. Based on the extraction, we take the most right bit from each the n^{th} binary vector. Finally, convert to decimal every multiple 8 from binary produced and then arranging process into RGB format of each pixel.

When a watermark inserted into a valuable document such as certificate, charter, cheque, etc. The application expected will assist the authority to protect originality of a document. With this application will use to help improve document security and to protect fraud of unathority person. Testing shows that steganography of image file with JPEG format and file image hidden with JPEG format which produced other small size of file from file steganography storage such as BMP and PNG formats. Due to this, steganography file with JPEG format will reduce and save storage.

Acknowledgment

We would like to thank to the Directorate General of Higher Education, Republic of Indonesia for supporting and funding with **Hibah Bersaing** fund. We also thank to the Research Department of Darmajaya Informatics and Business Institute for providing guiding and allowing us to use their laboratory to finish our work

References

[1] Ajay Goel,O.P.Sahu , Ajay Goel.2011. Improved Digital Watermarking Techniques and Data Embedding In Multimedia. Journals in Science and Technology,Vol. 02, No. 02, 2010, 164-168

[2] Dugelay J. L., , S. Roche, C. Rey, G. Doërr. 2006. Still-image water-marking robust to local geometric distortions.IEEE Trans. on Image Proc., vol. 15, no. 9, Pp. 2831-2842.

[3] Ema Utami.2009. Pendekatan Metode Least Bit Modification Untuk Merancang Aplikasi Steganography Pada File Audio Digital Tidak Terkompresi. Jurnal Dasi. Vol. 10 No. 1, Issn: 1411-3201. (in Bahasa)

[4] Onkar Dabeer, Kenneth Sullivan, And Upamanyu Madhow. 2007. Detection Of Hiding In The Least Significant Bit. IEEE Transactions On Signal Processing, Vol. 52, No. 10.

[5] Chauhan Usha, and Singh Rajeev Kuma. *2016.* Digital Image Watermarking Techniques and Applications: A Survey, Volume 6, Issue 3, Pp. 533-540, ISSN: 2277 128X

[6] Sukhraj Kaur, Navjot Kaur.2015. Performance Evaluation of Digital Watermarking Using DWT, CZT and Negative Selection Algorithm based SVD, International Journal of Engineering and Innovative Technology (IJEIT), Volume 5, Issue 1,Pp.132-139.

[7] Ragini Sharma1 , Er. Surbhi Gupta. 2015. Digital Watermarking with DWT & DCT using Bit Plane Encryption, Vol. 4, Issue 12, Pp. 414-419.

[8] Ryanti Irviantina, Sunario Megawan, Jonni,. Aplikasi Teknik Adaptive Digital Image Watermarking Untuk Proteksi Hak Cipta Citra Digital. JSM STMIK Mikroskil: ISSN.1412-0100: 2015 vol 16 No 1: 113-123. (In Indonesia)

Wasilah recieved her master in computer sciences from Bandung Institute of Technologi, Indonesia in 2007 . Currently she is Ph.D student at Compter Science School , The Univesity of Gajah Mada University, Indonesia. Her interest are document and image security system, audit system, and software Engineering.

Dona Yuliawati recieved her master in Information Technolgy from Darmajya Informatics and Business Institute, Indonesia in 2013. Currently she works as reseacher in Information System Department. Her interest are security system, software engineering , and Visual programming.

Suhendro Y. Irianto received his Master in computers science from The University of Indonesia, Jakarta Indonesia. He got Ph.D degree in image Retrieval from the University of Bradford, United Kingdom in 2008. Currenmtly he works as a researcher in Informatics Engineering department, Darmajaya Informatics and Business Institute, Indonesia. His interests are image retrieval, biometrics, pattern recognition, and multimedia database.

Watermarking Using LSB Shifting to Document Protection

ORIGINALITY REPORT

10%	8%	6%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

3%

★ cirworld.org

Internet Source

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Watermarking Using LSB Shifting to Document Protection

GRADEMARK REPORT

FINAL GRADE

/0

GENERAL COMMENTS

Instructor

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7