International Journal of Engineering & Technology, 7 (3.2) (2018) 760-762

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Application of Invisible Image Watermarking

S Supiyandi[1*], Grace Lamudur Arta Sihombing[2], Henry Kristian Siburian[3], Agung Purnomo[4], Fatkul Anam[5], Endrayana Putut Laksminto Emanuel[5], Dodi Siregar[6], Aditya Halim Putra[7], Folkes E. Laumal[8], Oktaf Brillian Kharisma$_9$, A Akhiruddin[10], R Rosnatang[10], Preddy Marpaung[11], Rizki Ramadani[12], Moch Andry Wikra Wardhana Mamonto[12], Nieke Monika Kulsum[13], S Salle[12], N Nurhayadi[14], Robbi Rahim[15]

[1]*Universitas Pembangunan Panca Budi, Medan, Indonesia*
[2]*Universitas Sisingamangaraja XII Tapanuli Utara, Indonesia*
[3]*Sekolah Tinggi Manajemen Informatika dan Komputer, Medan, Indonesia*
[4]*Bina Nusantara Institute of Creative Technology Malang, Indonesia*
[5]*Universitas Wijaya Kusuma Surabaya, Indonesia*
[6]*Universitas Harapan Medan, Medan, Indonesia*
[7]*Sekolah Tinggi Ilmu Manajemen Lasharan Jaya, Makassar, Indonesia*
[8]*Politeknik Negeri Kupang, Indonesia*
[9]*Universitas Islam Negeri Sultan Syarif Kasim, Pekanbaru, Indonesia*
[10]*Sekolah Keguruan dan Ilmu Pendidikan Mega Rezky, Makassar, Indonesia*
[11]*Universitas Sumatera Utara, Medan, Indonesia*
[12]*Universitas Muslim Indonesia, Makassar, Indonesia*
[13]*Universitas Nasional, Jakarta, Indonesia*
[14]*Universitas Tadulako, Palu, Indonesia*
[15]*Sekolah Tinggi Ilmu Manajemen Sukma, Medan, Indonesia*
**Corresponding author E-mail: usurobbi85@zoho.com*

Abstract

Copyright to an image is very important so that it is not misused by irresponsible parties, many ways can be done to provide copyright information in an image. Watermarking is a technique commonly used to mark a picture that the image already has copyright and whose owner is known, but in addition to visible watermarking there is also an invisible watermarking to indicate an image on a pixel or also in byte code and this is invisible. The Patchwork Algorithm is an algorithm that can be used to give an image to the image as an authenticity image so that many parties cannot claim it and are quite good from various modifications of image, application that has been created are purpose to embedded information as invisible watermarking in the image.

Keywords: *Application Watermarking, Watermarking, Secure Image*

1. Introduction

Information can be something that is very valuable and must be kept confidential [1]–[7]. Examples include information about credit cards, passwords, military strategies, trading strategies, negotiation data, encryption keys, political strategies and others[8]–[10]. One solution to securing information is by steganography[11], [12].

Steganography is a science and art that studies the concealment of confidential data in a media in such a way that its existence is not detected by other parties who are not entitled to the information[13]–[15]. Another method that has a way of working with steganography is the watermarking method which is generally used as an identifier (digital signature) of digital media such as images, audio or video[16]–[20].

Watermarking generally requires a specific key to be able to increase robustness and maintain image quality degradation. Not the same as a watermark for copyright protection, where it must be considered the use of a watermark to insert index data, where index data means a memo that can be read by someone, for example a place and date when a digital photo has been taken[20].

Watermarking is a form of steganography in learning the techniques of storing data (digital) into other digital host data. Besides that, the watermarked data must be resistant to attacks either intentionally or unintentionally to eliminate the watermark data contained therein. Watermarks must also be resistant to various types of digital processing / processes that do not damage the quality of the watermarked data.

Patchwork technique uses redundant pattern encoding and spread spectrum methods to hide information into the entire cover image, in using redundant pattern encoding the message or information that you want to secure on a cover can only be done once because it will occupy a large enough position from the picture[21]–[24].

Copyright © 2018 Robbi Rahim. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

2. Methodology

A. Digital Image

Digital image is a picture on two dimensions, or image can also be interpreted as a collection of points with a certain intensity that form a unity of combination that has both artistic and intrinsic meaning[18].

B. Image Elements

Digital images contain a number of basic elements. These basic elements are manipulated in image processing and further exploited in computer vision. Important basic elements include[25]:

1. Brightness
   Brightness is another word for light intensity. Brightness at a point (pixel) in the image is not real intensity.
2. Contrast
   Contrast states the lightness and darkness in an image. Low contrast images are characterized by most of the composition of bright or partially dark images.
3. Contour
   Contour is a condition caused by changes in the intensity of neighboring pixels.
4. Color
   Color is a perception perceived by the human visual system to the wavelength of light reflected by an object. Each color has a different wavelength. Red has the highest wavelength, while purple has the lowest wavelength

The colors received by the human eye are the result of a combination of light with different wavelengths. Research shows that color combinations that provide the widest color range are red (R), green (G), and blue (B). These three colors are called primary colors, and are often referred to as RGB.

C. Patchwork

Patchwork techniques use the redundant method of encoding and spread spectrum methods to hidden information that is spread throughout the cover image[26], [27]. In using redundant pattern encoding, we must sell message sizes against durability. For example, a small message can be drawn several times on the image so that if the stego-image is generated, there is a high probability that the watermark can still be read. A large message can be pasted only once because it will occupy a large portion of the image area.

This patchwork method will produce a reconstruction image that is very similar to the original, because it only changes certain bits of the image[28]. Suppose a byte in the image represents a certain color, then the change of a bit will not greatly affect the color. This is due to the limitations of the human eye in seeing these color changes.

3. Results and Discussion

The image watermarking application is created using the Visual Basic.Net 2010 programming language with GDI + to process images, here are the results of the application for testing to enter metadata information from the image.

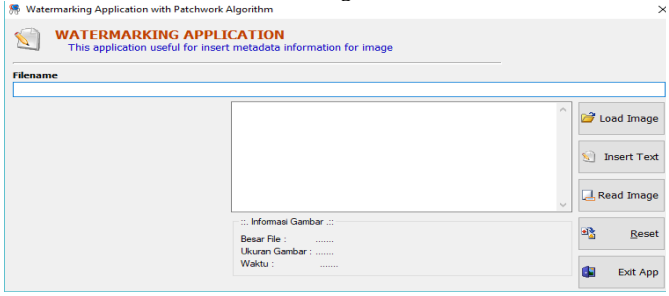


Fig 1: Main Display

Figure 1 is an application prototype made to give watermarks to images by applying patchwork algorithms, the first test is done by inserting information as shown in Figure 2.

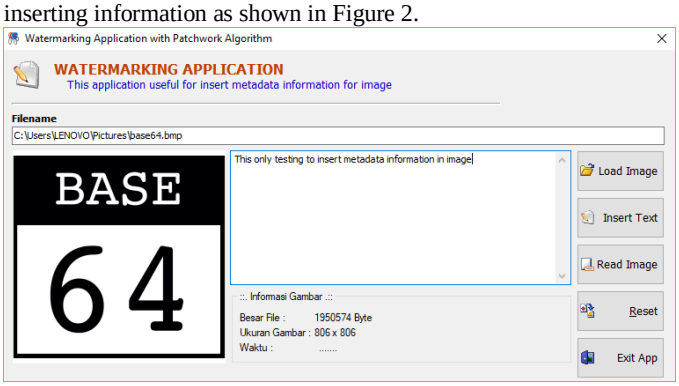


Fig 2: Image and Information

Figure 2 display metadata information from image and a message to be insert into image, for first embedded message into image it can be done using *insert text button*, when the processed are performed it will show message notification that the processed embedded successful.

Extracting information to check whether the image have an information can use *Read Image*, with the process in the button all information in image will be extract and can be read. An experiment were perform for several image with different message and with thus experiment it get how much time to be processed, table 1 are the result.

Table 1: Embedded Experiment Result

No	Filename	Size (KB)	Metadata Information	Time
1	Campus.bmp	123	Sekolah Tinggi Ilmu Komputer Arjuna	0.345 ms
2	Phone.bmp	78	This phone image are licensed to AT&X company for commercial purposes	0.982 ms
3	Wallet.bmp	52	This image are part of company XYZ to promote a wallet from cockroach skin	0.511 ms
4	Laptop.jpg	71	This laptop taken from Tosiba Company for promotion use	1.43 second
5	Bag.jpg	90	This bag created using photoshop	1.12 second

Based on application testing carried out with various types of image files with different messages, from the testing carried out giving metadata to image files using patchwork algorithms that insert information on image files with BMP type is faster to process than image files with JPG type, this occurs because the JPG file has been compressed and the pixel structure is also it takes a longer to be read by the application.

4. Conclusion

Watermarking as a way to identify ownership of an object is very important and many algorithms and methods can be used, invisible watermarking of one type that can be done using patchwork algorithms as a process, the results obtained are also very good and with a fast process as well. The next development can be combined with a compression algorithm so that the metadata provided in the image does not require a larger space without reducing the function of the watermarking.

References

[1] H. Nurdiyanto *et al.*, "Authentication Security in Radio Frequency Identification with IDEA Algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 384, p. 012042, Jul. 2018.

[2] D. Abdullah *et al.*, "Super-Encryption Cryptography with IDEA and WAKE Algorithm," *J. Phys. Conf. Ser.*, vol. 1019, no. 1, p. 012039, Jun. 2018.
[3] S. Sriadhi, R. Rahim, and A. S. Ahmar, "RC4 Algorithm Visualization for Cryptography Education," *J. Phys. Conf. Ser.*, vol. 1028, no. 1, p. 012057, Jun. 2018.
[4] M. Mesran *et al.*, "Combination Base64 and Hashing Variable Length for Securing Data," *J. Phys. Conf. Ser.*, vol. 1028, p. 012056, Jun. 2018.
[5] H. Nurdiyanto, R. Rahim, A. S. Ahmar, M. Syahril, M. Dahria, and H. Ahmad, "Secure a Transaction Activity with Base64 Algorithm and Word Auto Key Encryption Algorithm," *J. Phys. Conf. Ser.*, vol. 1028, no. 1, p. 012053, Jun. 2018.
[6] M. Mesran, M. Syahrizal, and R. Rahim, "Enhanced Security for Data Transaction with Public Key Schnorr Authentication and Digital Signature Protocol," *ARPN J. Eng. Appl. Sci.*, vol. 13, no. 11, pp. 3839–3846, 2018.
[7] R. Rahim, "Man-in-the-middle-attack prevention using interlock protocol method," *ARPN J. Eng. Appl. Sci.*, vol. 12, no. 22, pp. 6483–6487, 2017.
[8] R. Rahim, N. Kurniasih, M. Mustamam, L. Andriany, U. Nasution, and A. H. Mu-, "Combination Vigenere Cipher and One Time Pad for Data Security," *Int. J. Eng. Technol.*, vol. 7, no. 2.3, pp. 92–94, 2018.
[9] H. Nurdiyanto, R. Rahim, and N. Wulan, "Symmetric Stream Cipher using Triple Transposition Key Method and Base64 Algorithm for Security Improvement," *J. Phys. Conf. Ser.*, vol. 930, no. 1, p. 012005, Dec. 2017.
[10] A. Putera, U. Siahaan, and R. Rahim, "Dynamic Key Matrix of Hill Cipher Using Genetic Algorithm," *Int. J. Secur. Its Appl.*, vol. 10, no. 8, pp. 173–180, Aug. 2016.
[11] R. Rahim *et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," *J. Phys. Conf. Ser.*, vol. 1007, no. 1, p. 012003, Apr. 2018.
[12] H. Nurdiyanto and R. Rahim, "Enhanced pixel value differencing steganography with government standard algorithm," in *2017 3rd International Conference on Science in Information Technology (ICSITech)*, 2017, pp. 366–371.
[13] R. Rahim, D. Adyaraka, S. Sallu, E. Sarimanah, and M. M. Rahman, "Tiny encryption algorithm and pixel value differencing for enhancement security message," *Int. J. Eng. Technol.*, vol. 7, no. 2.9, pp. 82–85, 2018.
[14] D. Kaur, H. K. Verma, and R. K. Singh, "A hybrid approach of image steganography," in *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, 2017.
[15] R. Bhardwaj and V. Sharma, "Image Steganography Based on Complemented Message and Inverted Bit LSB Substitution," in *Procedia Computer Science*, 2016, vol. 93, pp. 832–838.
[16] N. Pohan, R. Saragih, and R. Rahim, "Invisible Watermarking Audio Digital with Discrete Cosine Transform," *Int. J. Sci. Res. Sci. Technol.*, vol. 3, no. 1, pp. 21–25, 2017.
[17] X. Li, "Watermarking in secure image retrieval," *Pattern Recognit. Lett.*, vol. 24, no. 14, pp. 2431–2434, 2003.
[18] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3. pp. 727–752, 2010.
[19] A. Swaminathan, Y. Mao, and M. Wu, "Robust and secure image hashing," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 215–230, 2006.
[20] J. Fridrich, *Steganography in digital media: Principles, algorithms, and applications*. 2012.
[21] I. K. Yeo and H. J. Kim, "Modified Patchwork Algorithm: A novel audio watermarking scheme," in *Proceedings - International Conference on Information Technology: Coding and Computing, ITCC 2001*, 2001.
[22] N. K. Kalantari, M. A. Akhaee, S. M. Ahadi, and H. Amindavar, "Robust multiplicative patchwork method for audio watermarking," *IEEE Trans. Audio, Speech Lang. Process.*, 2009.
[23] M. V. R. Krishna and D. Ghosh, "Audio Watermarking In The FFT Domain Using Perceptual Masking," in *the National Conference on Communication*, 2003.
[24] H. Kim, "Robustness Analysis of Patchwork Watermarking Schemes," *Inf. Secur.*, 2006.
[25] R. Gonzalez and R. Woods, *Digital image processing*. 2002.
[26] B. Purna Kumari and V. P. Subramanyam Rallabandi, "Modified patchwork-based watermarking scheme for satellite imagery," *Signal Processing*, 2008.
[27] H. Kang, K. Yamaguchi, B. Kurkoski, K. Yamaguchi, and K. Kobayashi, "Full-index-embedding patchwork algorithm for audio watermarking," *IEICE Trans. Inf. Syst.*, 2008.
[28] I. K. Yeo and H. J. Kim, "Generalized patchwork algorithm for image watermarking," *Multimed. Syst.*, 2003.