UNIVERSITAS DIAN NUSWANTORO UDINUS SEMARANG

Technical co-Sponsor :

IEEE

ISBN :
978-1-5386-7486-4
IEEE CATALOG NUMBER :
CFP18CUE-ART

# 2018 iSemantic

3rd International Seminar on
Application for Technology of Information
and Communication

# PROCEEDINGS

## Creative Technology for Human Life

Semarang | September 21st - 22nd, 2018

Email:
isemantic@lppm.dinus.ac.id
Website:
http://isemantic.dinus.ac.id/

PROCEEDINGS ISEMANTIC 2018

ISBN :
978-1-5386-7486-4
IEEE CATALOG NUMBER :
CFP18CUE-ART

Organized by

LPPMUDINUS

**Lembaga Penelitian dan Pengabdian Masyarakat** Universitas Dian Nuswantoro Semarang

**Computer Science Faculty**
**Engineering Faculty**
**Health Faculty**
**Universitas Dian Nuswantoro Semarang**

# PROCEEDINGS

2018 International Seminar on Application for Technology of Information and Communication

(iSemantic)

## Creative Technology for Human Life

September 21st – 22nd, 2018

Universitas Dian Nuswantoro

Semarang, Indonesia

ISBN : 978-1-5386-7486-4
IEEE CATALOG NUMBER : CFP18CUE-ART

# Bit Localization in Least Significant Bit using Fuzzy C-Means

**Atika Mutiarachim[1], Stefano Felix Pranata[2], Basirudin Ansor[3], Guruh Fajar Shidik[4], Ahmad Zainul Fanani[5], Arief Soeleman[6], Ricardus Anggi Pramunendar[7]**
Master of Informatics Engineering, Faculty of Computer Science, Dian Nuswantoro University
Imam Bonjol street 205-207, Lt 2, Semarang. Telp. (024) 3547038, (024) 70793727
E-mail : amutiarachim@gmail.com[1], stefanofelixpranata@gmail.com[2], anzhorhmm@gmail.com[3],
guruh.fajar@research.dinus.ac.id[4], ahmad.zainul.fanani@dsn.dinus.ac.id[5], arief2802@dsn.dinus.ac.id[6],
ricardus.anggi@dsn.dinus.ac.id[7]

*Abstract*—Least Significant Bit (LSB) as one of steganography methods that already exist today is really mainstream because easy to use, but has weakness that is too easy to decode the hidden message. It is because in LSB the message embedded evenly to all pixels of an image. This paper introduce a method of steganography that combine LSB with clustering method that is Fuzzy C-Means (FCM). It is abbreviated with LSB_FCM, then compare the stegano result with LSB method. Each image will divided into two cluster, then the biggest cluster capacity will be choosen, finally save the cluster coordinate key as place for embedded message. The key as a reference when decode the message. Each image has their own cluster capacity key. LSB_FCM has disadvantage that is limited place to embedded message, but it also has advantages compare with LSB that is LSB_FCM have more difficulty level when decrypted the message than LSB method, because in LSB_FCM the messages embedded randomly in the best cluster pixel of an image, so to decrypted people must have the cluster coordinate key of the image. Evaluation result show that the MSE and PSNR value of LSB_FCM some similiar with the pure LSB, it means that LSB_FCM can give imperceptible image as good as the pure LSB, but have better security from the embedding place.

***Keywords— Clustering, Fuzzy C Means, Image Processing, Least Significant Bit, Steganography***

## I. Introduction

Tremendous development of technology is directly proportional with the more risk of technology crime that may arise. That's why security aspect also be concern research search trend in this year [1]. Secure factor is needed to dodge a risk, even more in this IoT era, security system be a big deal and big challenge to solve [2]. There are many crime case that may happened inside technology like theft of important and secret message. To handle it, many researchers vying to find the best of encryption method, based on the time reduce, memory capacity improvement, and the hassle of method in embedding and decrypting the messages. Messages (especially a secret messages) tend to be privacy and usually contains of some important information so should not be receive by unauthorized parties [3].

Information hiding is one of security systems method to embed a message into an object like video, audio, image, fingerprint and etc. This method consist of steganography and watermarking. Steganography divided into linguistic and technical. In watermarking there are robust and fragile. Each method has own characters, advantages and disadvantages. The choice of method should be based on the need of security systems that will be created.

In this research, LSB was combined with Fuzzy C-Means (FCM) to optimize the difficulty level to decrypt the message from an stego-image. FCM is a clustering method, that can cluster one data to two or more cluster, based on their characteristic [4]. In this research, FCM used to cluster the pixel of an image. By using FCM, message will embedded to a random part of an image. This methods aim to looking for a cluster with big number of pixel as place of message, and make the embedded message more secure. It is a novel method for security system, especially in steganography. In future, CM_LSB also can give an improvement as contribution to Internaet of Thing (IoT) security systems.

## II. Related Works

To increase insight, researcher start with analyze and study some related works trend in steganography. Some papers that significantly contributed in this research are summarized in this section.

First the idea of reversible data hiding, [5] use difference expansion and difference histogram shifting method to get high capacity and reversibility in embedding data. Another research is about hybrid concept of data security using LSB and Discrete Cosine Transform (DCT), aims to optimize the security and authentication of data. DCT is an algorithm that used to compress signal and image data [6]. Cryptography and QR code are used to combine the LSB and DCT [7].

In [8] pure LSB compared with LSB-Canny edge detection method to ensure the embedding message process runs perfectly and increase the imperceptible between the original image and the embedded one. Using four *.bmp grayscale image, [9] *.txt message embedded to the image, then be invaded by JPEG compression, gaussian noise, salt and pepper and media filtering, then measured by PSNR and

MSE. The measuring result show that LSB-Canny method get better value of PSNR and MSE than pure LSB.

The next method, [10] use LSB Matching Revisited method (LSBMR) with Sobel as the edge detection of an image. By choosing two pixels from the cover image randomly using pseudo random number generator (PRNG), then embedded the bits on those pixels using stego-key. Not all pixel suitable to adjusted, because the sharp change may be visible to human eye [11]. LSBMR applied to overcome those limitation, by use the edge to embedded information first, then leave the smooth areas based on the capacity of messages. Compared with Enhanced Least LSBMR (EALSBMR), the development of LSBMR, based on PSNR evaluation value [10] LSBMR has a slightly better quality in image and in resisting visual attack than EALSBMR, because LSBMR not adjusted the smooth regions.

## III. Material and Method

Three approaches to design a security system are choose applicable image, select appropriate embedding location and choose best encrypted version [12]. Embedding location of messages is get from clustering result of FCM. Encrypted method that use here is LSB. There are five images that used in this research, with different size and dimension. The image order is start from the left that is rainbow cube as first image, and the right that is stroberi as fifth image.

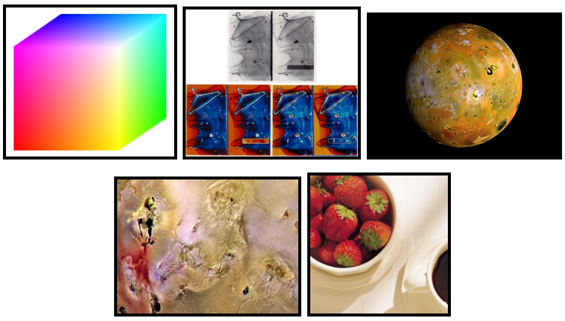


Fig. 1 Five Cover Images

### *A. Proposed Method*

There are many security systems research trends in information hiding. Especially in steganography, using basic principles of LSB algorithm, many study expand this algorithm or combined it with many kinds embedded place of detector method like Sobel, Canny and etc. This research focused on technical digital image steganography, and also expanding the LSB method to be LSB_FCM. In this research, a novel parallels method was applied by combine LSB and FCM. Framework of this research is in figure 2.

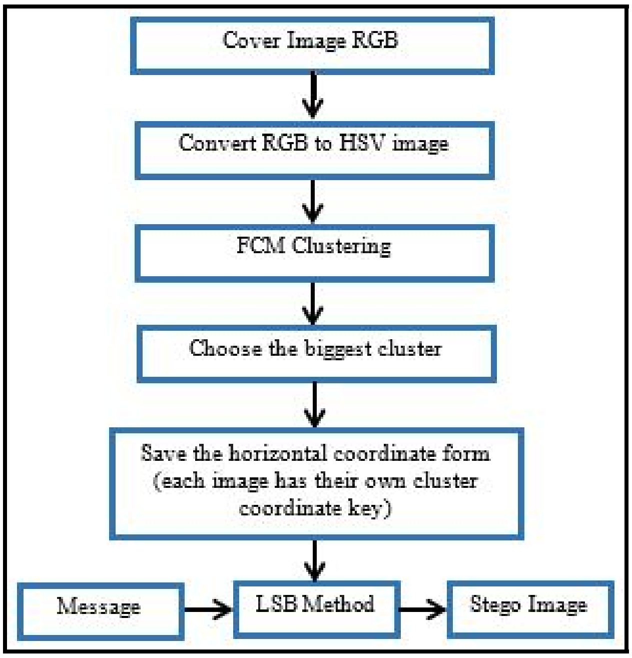

Cover Image RGB
Convert RGB to HSV image
FCM Clustering
Choose the biggest cluster
Save the horizontal coordinate form (each image has their own cluster coordinate key)
Message
LSB Method
Stego Image

Fig. 2 Framework

FCM will cluster the image, then choose the best cluster with biggest capacity, save the cluster coordinate key to embeded the message using LSB. Unspecified cluster help to make the message more secure, because more difficult to guess than if embedded in each edge of image.

### *B. Fuzzy C-Means*

Fuzzy C Means (FCM) is a clustering method which able to grouped a datasets into n cluster, with each data point belonging to each cluster in certain degree. FCM have ability to minimize error in clustering function [5], and the formation of new clusters have close membership values to existing class [13]. Here FCM used to cluster the cover image pixels, then choose the best cluster with more amount of pixel as embedded region.

### *C. Least Sigificant Bit*

Least Sigificant Bit (LSB) is a steganography method which are simple in embedded the bit [14] [15], and imperceptible [9], so there is no contrast and different look beetwen the original image and the embedded image . It's used to embedding the message into the picture, by put the bit of a message to the last bit of each picture pixel.

One RGB pixel, consist of R, G and B value. The value of each R, G and B is beetwen 0-255 or 11111111 and 00000000 or combination beetwen 1 and 0 in biner. From eight biner combination, the last bit or eighth bit of each R,G,B in each pixels are used to be the embedded region of messages. The messages that will be embedded to image, must in form of biner too. LSB is easy to implemented, high perpetual transparency and imperceptibilty because the cover image usually look same with the embedded image.

### *D. LSB_FCM*

LSB_FCM is the combination of embedding message method that use FCM to looking for the best cluster, and use LSB as embedded method. It is a novel combination of data security method, especially in steganography. Application of LSB_FCM in this research as follow:

*Input* : *1) Read RGB cover image*

*Process* : *2) Convert RGB to HSV image*
*3) Cluster HSV image using FCM, divide image pixels into two clusters*
*4) Choose the cluster that has biggest capacity*
*5) Save the cluster coordinate as cluster coordinate key to avoid the coordinate change when the image clustered again. It is also as reference when decrypted the message. Each image has different cluster coordinate key.*
*6) Embed the message into the choosen capacity coordinaet using LSB method*

*Output* : *7) FCM_LSB stego-image*

Two flowcharts in figure three and figure four show the different process in pure LSB and LSB_FCM.

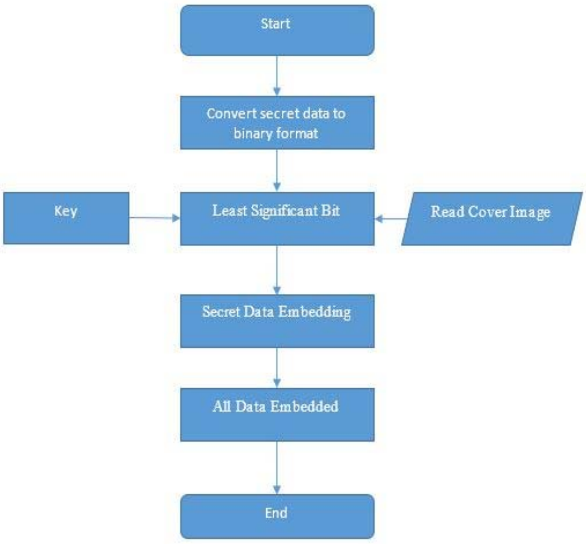


Fig. 3 Flowchart of Pure LSB Process

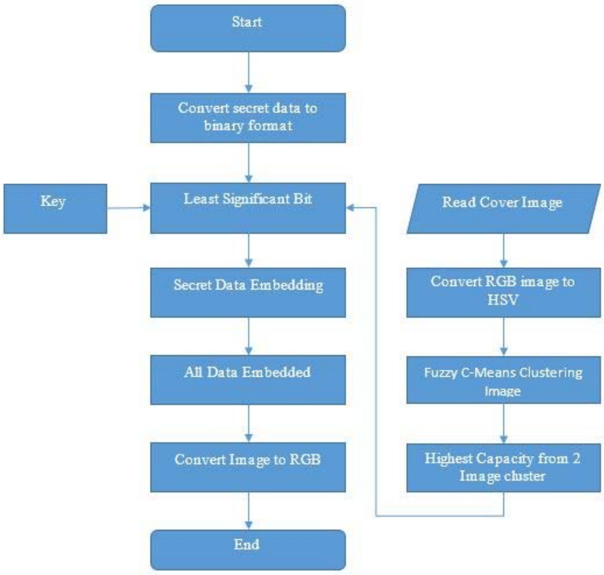
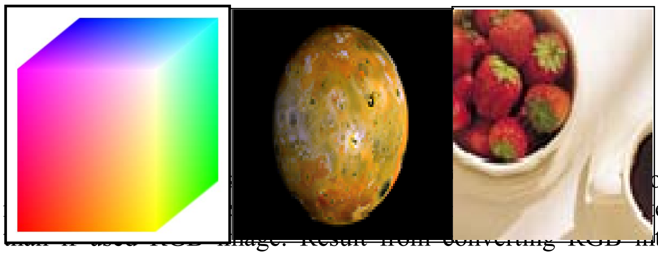


Fig. 4 Flowchart of LSB_FCM Process

## IV. Result and Discussions

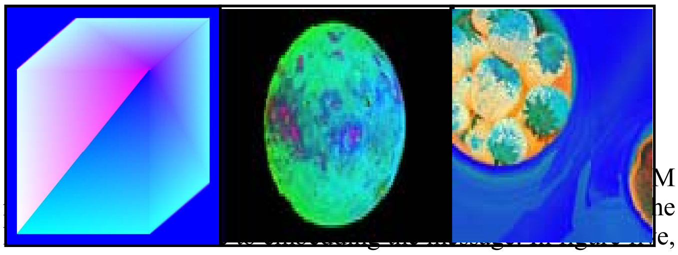
Five standart RGB images are used as the cover images. Below is three from five images that used in this research.



on

er

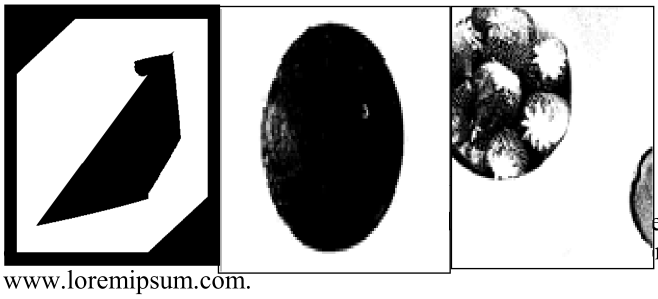
than it used RGB image. Result from converting RGB into HSV images are displayed in figure four.



M

he

to embedding the message. In figure five, the white part of the image indicate the biggest cluster. The horizontal coordinate from the biggest cluster will save as coordinate cluster key. This key also be the reference to decode the embedded message.



en

m

www.loremipsum.com.

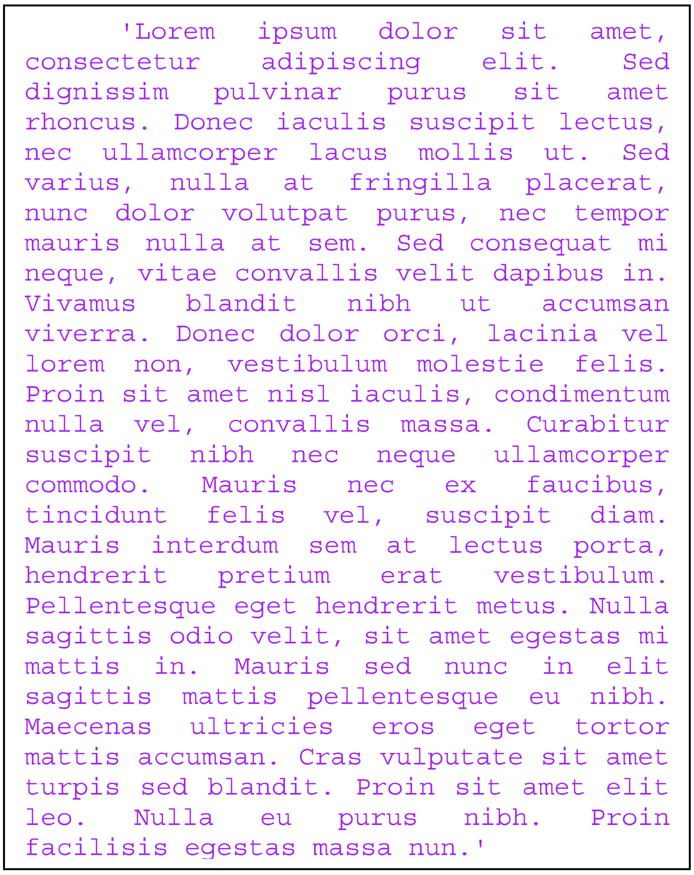

'Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed dignissim pulvinar purus sit amet rhoncus. Donec iaculis suscipit lectus, nec ullamcorper lacus mollis ut. Sed varius, nulla at fringilla placerat, nunc dolor volutpat purus, nec tempor mauris nulla at sem. Sed consequat mi neque, vitae convallis velit dapibus in. Vivamus blandit nibh ut accumsan viverra. Donec dolor orci, lacinia vel lorem non, vestibulum molestie felis. Proin sit amet nisl iaculis, condimentum nulla vel, convallis massa. Curabitur suscipit nibh nec neque ullamcorper commodo. Mauris nec ex faucibus, tincidunt felis vel, suscipit diam. Mauris interdum sem at lectus porta, hendrerit pretium erat vestibulum. Pellentesque eget hendrerit metus. Nulla sagittis odio velit, sit amet egestas mi mattis in. Mauris sed nunc in elit sagittis mattis pellentesque eu nibh. Maecenas ultricies eros eget tortor mattis accumsan. Cras vulputate sit amet turpis sed blandit. Proin sit amet elit leo. Nulla eu purus nibh. Proin facilisis egestas massa nun.'

Fig. 8 The Message

The stego-images are displayed in figure nine. From the embedded process, the result show that there is no contrast look between the cover images and stego-images, it is the main keys in steganography.

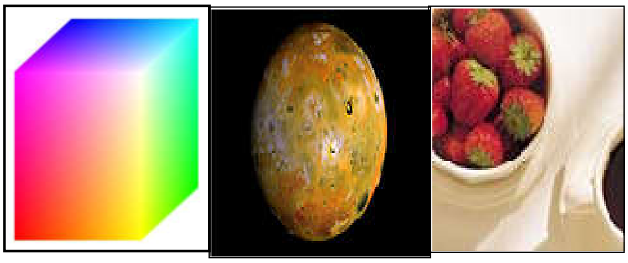


Fig. 9 Stego-images

The bit capacity, byte capacity, iteration, and time execution were calculated from each image. The result show in table I.

TABLE I. LSB_FCM

| Image | Bit | Byte | Iteration | Time |
|---|---|---|---|---|
| 1 | 226089 | 28261 | 3 | 0.32867076 |
| 2 | 142242 | 17780 | 10 | 0.33652582 |
| 3 | 401352 | 50169 | 3 | 0.46154190 |
| 4 | 365709 | 45713 | 3 | 0.37597524 |
| 5 | 1045269 | 130658 | 13 | 0.34054169 |

There is no big change and significant different in the stego-images when compare by the cover image, it is prove by the MSE and PSNR values. In some images, MSE and PSNR from LSB_FCM give sligthly better quality than the LSB stego-images, especially for the MSE values.

TABLE II. MSE AND PSNR

| Image | LSB | | LSB_FCM | |
|---|---|---|---|---|
| | MSE | PSNR | MSE | PSNR |
| 1 | 0.0097 | 68.2611 | 0.0097 | 68.2443 |
| 2 | 0.0159 | 66.0902 | 0.0161 | 66.0634 |
| 3 | 0.0551 | 70.7139 | 0.0055 | 70.7265 |
| 4 | 0.0058 | 70.4413 | 0.0059 | 70.4116 |
| 5 | 0.0030 | 73.2787 | 0.0031 | 73.2426 |

## V. CONCLUSION

FCM_LSB method has a weakness that is because the data that can be embedded is limited to the bit amount of choosen cluster, it can be smaller than embedded place from original LSB method. This limit also can be an advantages, because if the data just embedded on a particular cluster, so it will be more difficult to decode the message when compared with original LSB. People must know the cluster coordinate key of an image to decode the embedding message. There is no contrast look between the cover image and the steo-image, it is really good in steganography. Compare with LSB, MSE and PSNR of LSB_FCM method s

## REFERENCES

[1] K. Panetta, “Gartner Top 10 Strategic Technology Trends for 2018,” *Smarter With Gartner*, 2017. [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2018/. [Accessed: 01-Feb-2018].

[2] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, “Secure integration of IoT and Cloud Computing,” *Futur. Gener. Comput. Syst.*, vol. 78, no. December, pp. 964–975, 2018.

[3] R. M. L. Jr and G. P. Schell, *Sistem Informasi Manajemen*. 2008.

[4] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, “Digital

image steganography: Survey and analysis of current methods," *Signal Processing*. 2010.

[5] J. Nayak, B. Naik, and D. H. S. Behera, "Computational Intelligence in Data Mining - Volume 2," vol. 32, no. November, 2015.

[6] X. Wu, J. Weng, and W. Q. Yan, "Adopting secret sharing for reversible data hiding in encrypted images," *Signal Processing*, vol. 143, pp. 269–281, 2018.

[7] R. Sharma and J. Singh, "Image Authentication Technique Based on Digital Watermarking using Clustering," *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 5.

[8] R. K. Singh and D. K. Shaw, "A Hybrid Concept of Cryptography and Dual Watermarking (LSB_DCT) for Data Security." p. 12, 2018.

[9] A. Susanto and C. A. Sari, "PERLINDUNGAN HAK CIPTA PADA CITRA DIGITAL MENGGUNAKAN," vol. 8, no. 2, pp. 441–448, 2017.

[10] Z. Fouroozesh and J. Al Ja'am, "Image steganography based on LSBMR using Sobel edge detection," *2014 3rd Int. Conf. e-Technologies Networks Dev. ICeND 2014*, pp. 141–145, 2014.

[11] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE J. Sel. Areas Commun.*, vol. 16, no. 4, pp. 474–481, 1998.

[12] M. S. Subhedar and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Comput. Sci. Rev.*, vol. 13–14, no. C, pp. 95–113, 2014.

[13] M. Asyali, D. Colak, O. Demirkaya, and M. Inan, "Gene Expression Profile Classification: A Review," *Curr. Bioinform.*, vol. 1, no. 1, pp. 55–73, 2006.

[14] M. Pavani, S. Naganjaneyulu, and C. Nagaraju, "A Survey on LSB Based Steganography Methods," *Int. J. Eng. Comput. Sci.*, vol. 2, no. 8, pp. 2464–2468, 2013.

[15] V. Verma, Poonam, and R. Chawla, "An enhanced Least Significant Bit steganography method using midpoint circle approach," *Int. Conf. Commun. Signal Process. ICCSP 2014 - Proc.*, pp. 105–108, 2014.