Android based Digital Steganography Application using LSB and PSNR Algorithm in Mobile Environment

Affiq S.M. Shaiden
Institute of Computer Science & Digital Innovation, UCSI University

Islam, Shayla
Institute of Computer Science & Digital Innovation, UCSI University

Subramaniam, Kasthuri
Institute of Computer Science & Digital Innovation, UCSI University

https://doi.org/10.5109/4480724

出版情報：Evergreen. 8 (2), pp.421-427, 2021-06. Transdisciplinary Research and Education Center for Green Technologies, Kyushu University
バージョン：

Android based Digital Steganography Application using LSB and PSNR Algorithm in Mobile Environment

Affiq S.M. Shaiden[1], Shayla Islam[2,*], Kasthuri Subramaniam[3]

[1,2,3] Institute of Computer Science & Digital Innovation, UCSI University, 56000 Cheras, Kuala Lumpur, Malaysia

E-mail: shayla@ucsiuniversity.edu.my

(Received January 7, 2021; Revised April 26, 2021; accepted April 26, 2021).

Abstract: Data security plays an important and integral part in communication technology. The demand for data security remains as high as ever as technologies evolve, especially in this era of rapid changing technology. A method of securing data can be seen steganography, which is the art of hiding data. This paper proposes for two algorithms, which are Least Significant Bit (LSB) and Peak Signal to Noise Ratio (PSNR), to be combined and utilized together to create an Android based Digital Steganography Application. As such, the contributions in this paper will benefit the field of data security particularly in the mobile environment as to the implementation of the two algorithms.

Keywords: steganography; LSB; PNR; Android

1. Introduction

In an age and era where data transfers are in the billions, it is of the utmost importance that that very data is protected and secured, hindering unauthorized users from having access to your data, mostly the confidential ones, for example, a groundbreaking formula you have just discovered and spent years to complete that you have yet to patent. This led to the discovery of information security, where means to protect your information were developed such as cryptography, zero knowledge proofing and steganography [1-10) 32)]

Aiding to the movement of data transfers comes a mobile platform that is compact in shape but efficient in nature: smartphones. Smartphones have been developed for years and arguably, has as of now hit its maturity in terms of design and hardware[11-12)]. Due to this fact, smartphones have become a splendid substitute for bulky laptops and static, personal desktops as smartphones nowadays are powerful and efficient enough for mobile practicality that does not sacrifice performance. In addition, with all this technology granted on the tips of our fingers, it has made data a whole lot easier to be accessed, processed and transferred. Thus, the need for information security is in order [12-16) 33)].

The art of hiding information inside a cover image, or steganography, is a technique that has been used for years and has an abundant history behind its purpose and techniques of implementation[16-28)]. This paper propose an Android based application which grants its users the ability to insert information into a cover image by way of LSB algorithm that will be of quality and undetected by the human eye thanks to PSNR measurements. A wider cover files can also be used to allow for variety in the cover image. The end product can then be of use on any communication platform under the user's demands. This allows for information security to be implemented on communication platforms such as WhatsApp, Twitter, Facebook and Instagram[29)].

2. Methodology

The application starts with the process of encoding. User selects a cover file and inputs a desired password for decrypting purposes later. User then inputs the desired text message into the cover file and the application encodes the information with the LSB algorithm. The application then runs through the PSNR value check to see if the resulting image satisfies the optimal value for PSNR. If it passes, the application displays the resulting image and saves the image before ending the process.

The decoding process then begins with the user selecting the steganography image. The user then is required to input the password that protects the steganography image from unauthorized access. If the password is verified, the user is allowed to decrypt the steganography image and the hidden information is displayed. If the password does not match, the application requests for password input again. The process thus ends. Fig. 1 displays the flowchart of the application below:

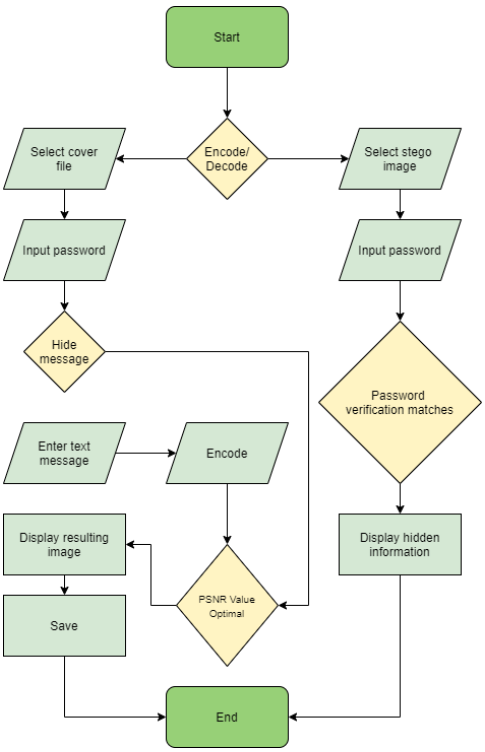

Fig. 1: Flowchart of the proposed application

2.1 Android

Android is an operating system for smartphones and is a common operating system as it is used on most smartphones in the market nowadays. Android's key feature is that it is an open-source operating system, meaning that it is free and accessible to anyone who wants to use it. This is the main reason as to why millions of applications are Android based and carries a low-price tag [27]. Android was also chosen as the steganography process is broken down into 3 stages as shown in Fig. 2 are mainly:

1. A cover file is selected; this can range from an imagefile or an audio file or even a text file.
2. The cover file goes through steganography. The method will differ for each application as approach to digital steganography is different. These methods can vary from the conventional LSB algorithm to modern algorithms where a combination of algorithms is utilized, for example, a mix of DWT and LSB algorithm.
3. Lastly, the end result is produced. The cover file is ready for decryption by the intended recipient. At this stage, an extra layer of security can be added which prompts recipients to input a password in order to gain access to the cover file.

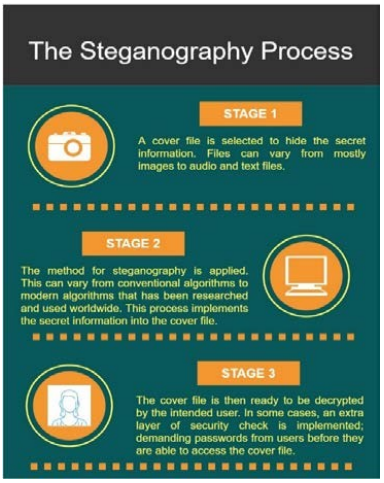

Fig. 2: The steganography process from beginning to end

The objective is clear cut; only authorized people are able to see the hidden message. Steganography is a completely different method when compared to cryptography, where cryptography makes a message unreadable, however, the message is still revealed and exposed to anyone. The art of digital steganography works by altering bits that are considered least significant (in the conventional method). The altered bits are replaced with different information, although, invisible in nature after the steganography is applied as illustrated in Fig. 3.

The desired operating system for the proposed work mainly because of its wide array of graphical user interfaces (GUI) that are easy to create and user-friendly. In addition, Android based operating system is a lot developer-friendly as iOS requires developers to adhere to strict requirements before they are able to publish their application online. As such, with all the factors trumping iOS, Android was chosen for flexibility and feasibility.

Fig. 3: Comparison of cover images before (left) and after (right) steganography is applied

2.2 Steganography

Steganography is a traditional method that has been used for centuries to hide information inside a cover file, for example, writing with invisible ink on a typical pen ink letter. A real-world scenario of steganography that can

be of example would be that in the law field. The prosecution would provide, in this case, confidential files to the defense attorney that are representing the victims. What the attorneys do not know, however, is that the files have gone through steganography and contains a different hidden number for every file. As such, in the case of leaks happening to any third party, the prosecution would be able to immediately detect which attorney has leaked the files as each and every file contain a different number that can only be seen by the prosecutors. This can be clearly illustrated in Fig.4 below:

Fig 4: Illustrates the different hidden number in each confidential files received by the attorneys

As illustrated above, each and every single attorney receives the confidential file. Unbeknownst to them, however, is that the confidential file has undergone steganography in the form of a watermarked steganography which is unique to every file. As such, when a leak occurs, prosecution simply has to decrypt the cover file and find out which watermarked number belongs to which attorney.

2.3 Least Significant Bit (LSB)

Least Significant Bit (LSB) will be the bits that are on the lowest series of numbers in a binary. An example of a Least Significant Bit will be the number one (1) on the rightmost end of a binary, for example, 10000011. In steganography, the last bit, or the last two bits of the series of numbers will be changed in order to insert the secret data. For example, take a bitmap image and change the lowest bits to be the hidden message. By going through this process of changing the LSB, it results in an almost imperceptible change on the way the cover image looks at the end, which can be illustrated by the Fig. 5.

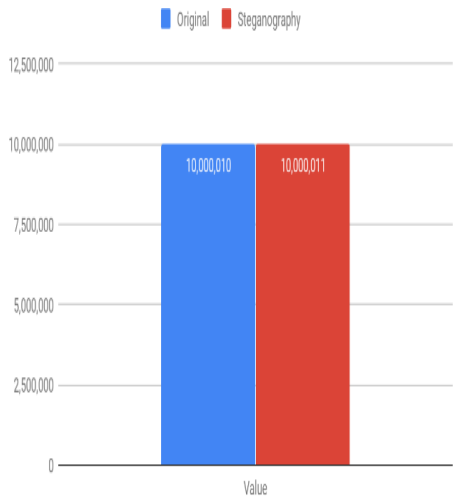

Fig. 5: Bar Chart for Original and Steganography

As seen above Fig.5, by changing the last bits, or even the last 2 bits to embed the secret data into the cover file, in the grand scheme of things, it makes no difference. As such, the human eye will not be able to perceive the difference that has been done onto the cover file, specifically for images.

2.4 Peak Signal to Noise Ratio

Peak Signal to Noise Ratio (PSNR) is the measurement of ratio between signal and noise. It is a method to achieve the optimal power from a signal in relation to the power of the noise that comes along with the representation. PSNR has been implemented into RGB images to differentiate the resultant quality[31]. PSNR can be calculated with the following Eq. 1:

$$MSE = \sum_{M,N} \frac{[I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad (1)$$

Mean-square error (MSE) in the formula is used to compare the quality of image after compression, whereby MSE represents the error between the before and after compression, and PSNR is the measurement when peak error occurs[30]. A good illustration of PSNR can be seen in Fig. 6 where the signal on the left represents the original data of the file. In this case, the cover file that is going to be used for steganography. The noise on the right represents the error made due to compression. The higher the PSNR value, generally, the higher the quality of the reconstructed image and hence, the lesser the chance of the naked human eye to be able to perceive the differencemade by steganography.

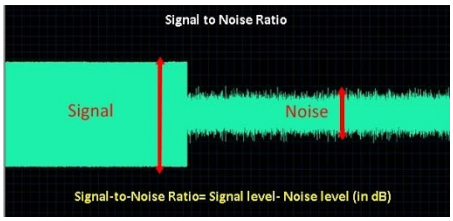

Fig 6: PSNR ratio (in dB)

2.5 System Design

The use case diagram in Fig.7 depicts the three parties involved in the application, whereby the parties being the sender, the receiver and the system itself. The sender is able to select the cover image, encode the image with the hidden message and save the image as a Steganography image. The receiver on the other hand is able to select the Steganography image that has been sent, inputs the password and decodes the Steganography image. The system on the other hand calculates the file size, the image size, shows the image details, converts the image to Bitmap Image (BMP) format, embed the text into the image and extracts the file.

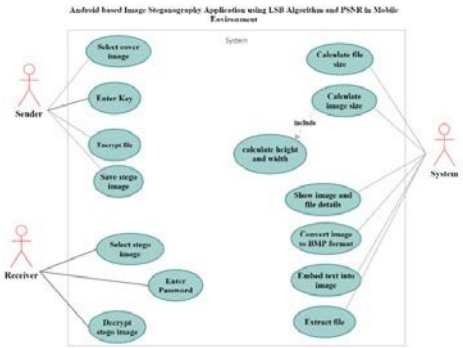

Fig. 7: Use Case Diagram

Based on the fact that the application is Android based, the programming language that was opted for development was Java. Java is one of the best programming languages out there for mobile application development and is an object-oriented language.

Integrated Development Environment (IDE) is utilized to develop the application as it is the official IDE for Google's Android operating system. As such, the move to opt for Android Studio was to focus solely on Android development. Android Studio supports Java and the Java Development Kit (JDK) is attached together in the installation pack. Fig.8 below illustrates how Android Studio looks.

3. Evaluation

This section discusses the procedures implemented in order to allow for quality control and assurance so as to guarantee that the project is delivered accordingly. The design of the User Interface (UI) for the application and the items involved in the implementation of the application is illustrated in Fig.9 and Fig.10 respectively.

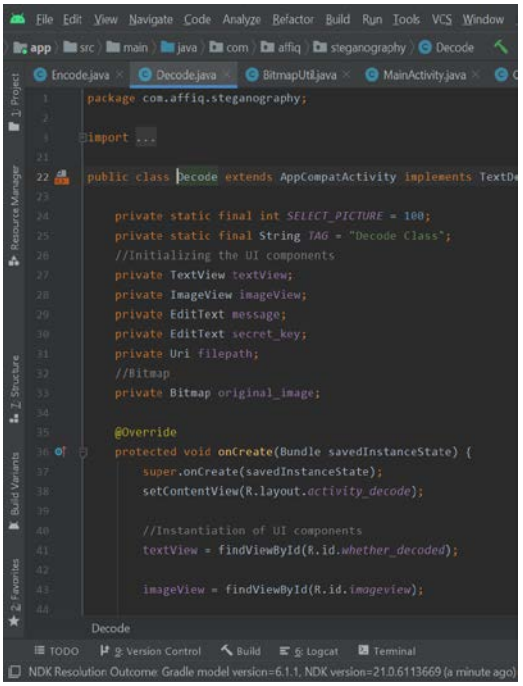

Fig. 8: Android Studio IDE

Fig. 9: UI for encoding

Fig. 10: UI for decoding page

The application is tested frequently prior to major implementations. This is to ensure that the functionalities are executed and without error when the application is run as a whole unit. Upon completion of the application, individual units are tested and integration testing is also done. The application's core functionalities were also put under heavy tests in order to guarantee that the entire system will run as intended.

In this study, multiple individuals volunteered to be part of the User Acceptance Test (UAT) program. These individuals have been briefed and informed regarding the application. As seen below, a list of system deliverables tasks was handed out to these individuals prior to proceeding of the UAT. This UAT was only executed once the application is usable and has satisfied all core functionalities. The UAT system deliverables tasks are as shown in Table 1 below:

Table 1. System Deliverables Tasks.

No.	Area		Item	Status
1.	Encryption	Encryption page	Encryption	Passed
2.	Decryption	Decryption page	Decryption	Passed
3.	SelectCover Image	Encryption page	Selecting cover image	Passed
4.	Save Stego Image	Encryption page	Saving Stego image	Passed
5.	Encryption (Password input)	Encryption page	Set password verification on selected cover image	Passed
6.	Decryption (Password input)	Decryption page	Verify password on selected Stego image	Passed

4. Results

The application has successfully encoded the inputs of images in LSB algorithm and a PSNR check is done to screen the encoded results so that users are aware of its PSNR value, allowing for an informed decision of whether to proceed with the encoded image or to use a different image input that is better suited for steganography. The PSNR value that is measured in dB can be seen in Fig.11 as below:

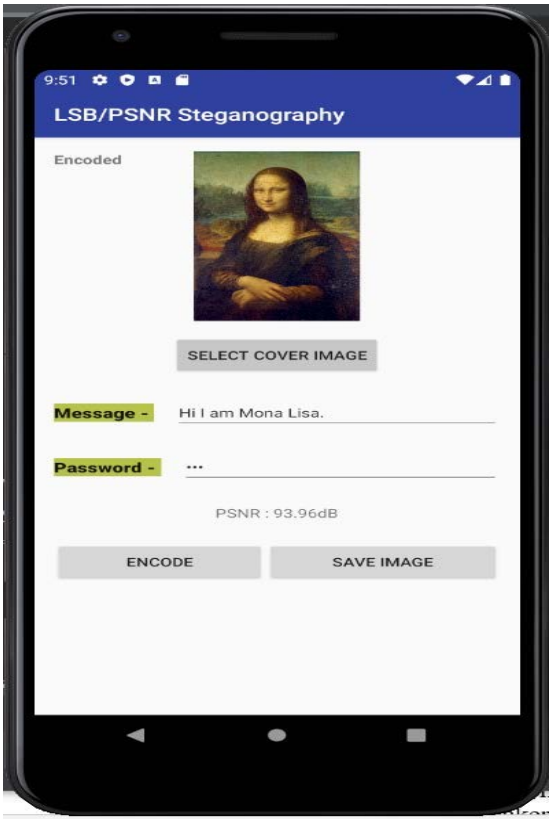

Fig. 11: Encoded image with the PSNR value

The decoding segment of the application has also gone on to show that it is capable of displaying the hidden message that was encoded into the cover image. This is illustrated in Fig. 12 below:

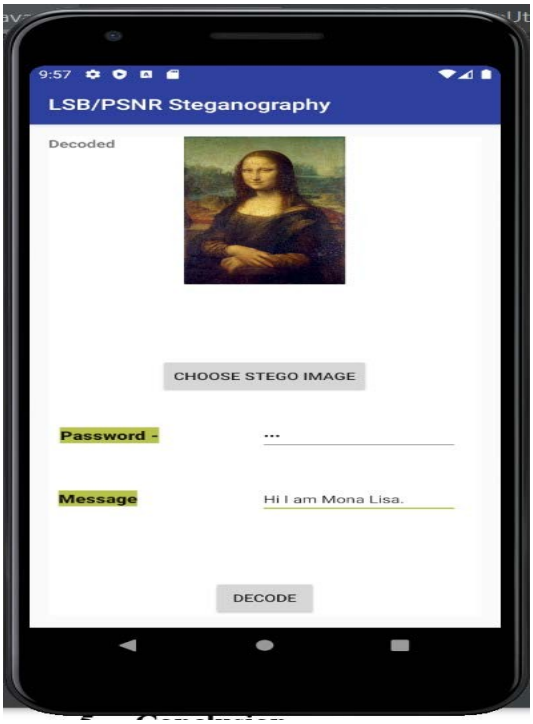

Fig. 12: The decoded image with its hidden message

5. Conclusion

Conclusively, through the use of dual algorithms, LSB and PSNR, on a mobile platform, this goes to show that steganography can be done with ease as users are no longer bound to the hefty personal computers/laptops as opposed to a compact smartphone. The application demonstrated a utilization of image steganography on a mobile environment that passes PSNR standards to ensure that steganography images produced from the application maintain a level of noise that establishes a ground of degree that allows for the steganography image to be invisible to the naked human eye. With the capability of hiding information in cover images to maintain anonymity, users can now use these steganography pictures on social media platforms such as WhatsApp, Instagram or Facebook to communicate with the added advantage of having an extra layer of security that is steganography. This application will be developed and tested amongst individuals in UCSI University, no matter what hierarchy they are on as this application benefits each and every level of hierarchy in the education institution. As mentioned, cover files have been an issue concerning digital steganography on a mobile environment. Hence, in the future, expanding the type of cover files that are open to images, audios, videos, and text will assist in solidifying steganography's position as a means to implement data security in a mobile environment as suspecting cyber criminals and hackers will have to

adapt to the ever changing type of cover files used during data transfers in a communication. Payload issue is without a doubt one of the many future works that has to be researched and developed due to the fact that increasing payload in digital steganography that is much higher compared to the payload that we have today will be groundbreaking. Multitudes of information can be hidden inside a cover file-expanding the use of digital steganography more than ever.

Acknowledgements

Special appreciations to the Centre of Excellence for Research, Value Innovation and Entrepreneurship (CERVIE), UCSI University Malaysia for the conference funding.

References

1) Azmat U., Mohsin, I., (2018). Stego App: Android based Image Steganography Application using LSB Algorithm, 5(9), 862-865.
2) Kumar, V., & Kumar, D. (2010, February). Performance evaluation of DWT based image steganography. In 2010 IEEE 2nd International Advance Computing Conference (IACC) (pp. 223-228). IEEE
3) Tauhid, A., Tasnim, M., Noor, S.A., Faruqui, N., & Yousuf, M. A. (2019). A Secure Image Steganography Using Advanced Encryption Standard and Discrete Cosine Transform. Journal of Information Security, 10(3), 117-129.
4) T., A., Authority., "Android Authority," Android Authority, Available: https://www.androidauthority.com/what-is-android-328706/.
5) B., Slash, "Null Byte," Available: https://null-byte.wonderhowtwo.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/.
6) Prof., Dr. Beatrice de Graaf, "The Anders Behring Breivik Trial," International Centre for Counter-Terrorism, Hague, 2013
7) A., G., B., B., Shailender Gupta, "Information Hiding Using Least Significant Bit," I.J. Modern Education and Computer Science, vol. 6, pp. 27-34, 2012
8) "Peak Signal to Noise Ratio (PSNR)", The MathWorks, United States, 2019
9) D., Z., Alain Hore, "Image quality metrics: PSNR vs. SSIM" in 2010 International Conference on Pattern Recognition, Canada, 2010
10) D. Selvaraj, "Development of a Secure Communication System based on Steganography for Mobile Devices," Frankfurt University of Applied Sciences, Fraknfurt, 2017
11) K. M. R. K. D. G. Prasenjit Kar, "An Android application for Image Steganography," in SEEMS, India, 2018.
12) B. T. Manar Kashnola, "Parallel Execution of the Steganography using SFLA on the Android Platform," in SICME, Mosul, 2019
13) M. S. Hassan Reza, "Enhancing Mobile Cloud Computing Security Using Steganography," Journal of Information Security, vol. 7, no. 4, pp. 245-259, 2016.
14) M. S. M. M. T. P. Arshiya Ansari, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats," International Journal of Computer Network and Information Security, vol. 11, no. 1, pp. 11-25, 2019.
15) D. A. N. Elsie Wangui Ngatia, "Information Security through Improved Image Steganography," Journal of Information and Technology, vol. 1, no. 1, pp. 28-46,2018.
16) S. M. M. D. A Rini Wishnu Wardhani, "Least significant bit steganography method for the digital data protection in the barcode," in AIP Conference Proceeding, India, 2019.
17) Liu L., Y., "Steganography in beatufied images," Journal of Math Bioscience Engineering, vol. 16, no. 4, pp. 2322-2333, 2019.
18) I. Hashad, "A robust steganography technique using discrete cosine transform insertion," in International Conference on Information and Communication Technology, Cairo, 2005.
19) R.M. Chinmaya Dharmadhikari, "Review of digital data protection" EasyChair, India, 2019.
20) P. S. Y. Kinan Sharon Minz, "A Review on Secure Communication Method based on Encryption, "International Research Journal of Engineering and Technology, vol. 6, no. 1, pp. 608-612, 2019.
21) R. G. Sabyasachi Pramanik, "A new encrypted method in image steganography, " IJEECS, vol. 13, no. 3, pp.1412-1419, 2019.
22) A. Abdelmgeiod, "Enhancing PIGPEN Image Steganography Method by using Zigzag Scanning", AJRCOS, vol. 4, no. 1, pp. 103-130, 2019.
23) E. H. R. E. J. K. Christy Atika Sari, "Good Performance Images Encryption using Selective Bit T-DES on Inverted LSB Steganography, "Journal of Computer Science and Information, vol. 13, no. 1, pp. 646, 2019.
24) M. T. Ashraful Tauhid, "A Secure Image Steganography using Advanced Encryption Standard and Discrete Cosine Transform," Journal of Information Security, vol. 10, no. 3, pp. 117-129, 2019.
25) Z. A. B. A. A. S. Jamil Al- Azzeh, "Improving the Security of LSB Image Steganography," International Journal of Informatics Visualization, vol. 3, no. 4, 2019.
26) B. Dominic and R. Crina, "Steganography and Cryptography on Mobile Platforms," ProQuest, Romania, 2013.
27) D. Santus Kumar, D. Nibir, R. Showvon, "Investigation of Factors Influencing the Choice of

Smartphone Banking in Bangladesh", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol. 06, Issue 03, pp 230-239, September, 2019.

28) D. A. Wulandari, M. Akmal, Y. Gunawan, Nasruddin, "Cooling Improvement of the IT Rack by Layout Rearrangement of the A2 Class Data Center Room: A Simulation Study", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol. 07, Issue 04, pp 00-00, December, 2020.
29) A. Rully, L. Yusuf, "Conceptual Framework of Development of Quality Culture in Indonesian Construction Company", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol. 07, Issue 01, pp 144-149, March, 2020.
30) D. Tarek, Y. Shigeo, "System Identification and Adaptive Control of Mass-Varying Quad-Rotor", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol 04, Issue 01, pp 58-66, March 2017.
31) N. Yu, W. Tomoaki, "Social Factors Affecting Innovation Cycle of Liquid Crystal Technologies : A Japanese Case Study", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol. 04, Issue 04, pp. 8-15, December, 2017.
32) A. Fachransjah, T. Y. M. Zagloel, A. Romadhani, "Discrete-Event Simulation and Optimization of Spare Parts Inventory and Preventive Maintenance Integration Model Considering Cooling Down and Machine Dismantling Time Factor", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol. 07, Issue 01, p 79-85, March, 2020.
33) S. Choudhary, A. Sharma, S. Gupta, H. Purohit, S. Sachan, "Use of RSM Technology for the Optimization of Received Signal Strength for LTE Signals Under the Influence of Varying Atmospheric Conditions", EVERGREEN Joint Journal of Novel Carbon Resource Sciences & Green Asia Strategy, Vol 07, Issue 04, pp 00-00, December, 2020.