*Advances in Social Science, Education and Humanities Research, volume 410*
**1st International Multidisciplinary Conference on Education, Technology, and Engineering (IMCETE 2019)**

# Improvement of Steganography Technique: A Survey

1st E Ardhianto
*Computer Science Departement,*
*BINUS Graduate Program – Doctor of Computer Science*
*Bina Nusantara University*
Jakarta, Indonesia
*Faculty of Information Technology, Universitas Stikubank*
Semarang, Indonesia
ekaardhianto@edu.unisbank.ac.id

2nd H L H S Warnars
*Computer Science Departement,*
*BINUS Graduate Program – Doctor of Computer Science*
*Bina Nusantara University*
Jakarta, Indonesia

3rd B Soewito
*Computer Science Departement,*
*BINUS Graduate Program – Doctor of Computer Science*
*Bina Nusantara University*
Jakarta, Indonesia

4th F L Gaol
*Computer Science Departement,*
*BINUS Graduate Program – Doctor of Computer Science*
*Bina Nusantara University*
Jakarta, Indonesia

5th E Abdurachman
*Computer Science Departement,*
*BINUS Graduate Program – Doctor of Computer Science*
*Bina Nusantara University*
Jakarta, Indonesia

***Abstract*—The improved technology in information security, now day has been being still developed. This, cause of the object called data which still has an important role in communications. There are two kinds of security technique, they are called steganography and cryptography. This paper will discuss growth of steganography technique from 2015 to 2019. The data obtained from journals and identified as a systematic literature review. The results are that improvement in steganography still developed by modifying the algorithm, combining the method and threating at parallel processing. Future, utilization of steganography is still needed, considered that communication channels are growing fast and sophisticated.**

***Keywords: improvement, steganography technique, survey***

## I. INTRODUCTION

In the Information Security field, hiding data is one thing that has an important role. Many papers discuss steganography. Generally, they write that steganography comes from Greek, they are consist of two words, they are "steganos" which means hidden and "graphy" which means writing. Steganography is a process to hide message [1], some assume if steganography is a shape of art and science [2 - 4]. This technique was introduced by Herodotus in the ancient Greece era, where written messages coated using wax as cover [3]. The aim of steganography is hiding existence of message through another media called cover [1]. Finally, steganography takes advantage of human visual system which does not realize the existence of the message inside the cover.

One thing which different is cryptography, cryptography focuses on how to get rid of message meaning [4]. In cryptography, messages processed using one or combination of method which do not need a cover. Cryptography processes are known as encryption and decryption. Encryption is a mechanism to make messages come as meaningless, and Decryption is the opposite. The purpose of cryptography is giving meaninglessness into messages, even though human visual system can see the message but it meaningless.

The growth of computer devices seems rapidly, communications and data transfers will be an important thing to be observed. Hardware and software now support to accelerate the data's process. This, seen from some papers discuss development steganography or cryptography or combining both using a parallel processing method. This paper will present a review among paper which has a topic like hiding data using steganography, securing data using cryptography, or combination both and paper which discusses the processing both using parallel method. The collected data are papers published between 2015 and 2019.

## II. METHOD

Figure 1 shows several steps that used.

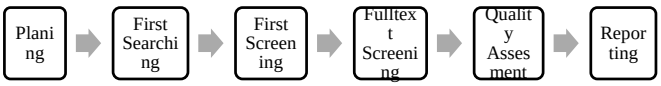


Figure 1, steps of Literature Review

### *A. Planning*

The first step is Planning, topic and research question are determined here. In this review, the topic of study is steganography, cryptography, and processing steps. The following are the Research Question (RQ) used.

- RQ1: is there any method developing in steganography and cryptography between 2015 to 2019?
- RQ2: What are the dominant measuring instrument in steganography from 2015 to 2019?
- RQ3: Is there any possibility of further developing in steganography?

*B. First Searching and Screening*

The first searching phase first does papers searching through google scholar site. In this phase, "parallel steganography" is used as term of searching. The searches are limited only papers which only published between 2015 to 2019. The result showed, there 4.780 papers as journal and proceeding.

*C. First Screening*

From the previous phase, the study continued with the Fulltext screening phase. In this phase, papers are downloaded which related to topic of study. This result 34 papers that can fully downloaded by full paper.

*D. Quality Assessment*

Please, Quality Assessment is stated after the previous step done. In this phase, the Quality Assessment (QA) process implemented using question as followed.

- QA1: is the paper published between 2015 to 2019?
- QA2: is the paper published by reputable journal and how many citation counts?
- QA3: is the paper's topic discuss the topic study?

Quality assessment performed with searching journal which contained the paper through international database portal of rank and quality of journal. In this phase, we accessed website www.scimagojr.com. Results of this phase are 6 papers published by Q2 journal, 16 papers published by Q3 journal, 5 papers published by Q4 journal and 7 papers are published by unranked journal by scimagojr.com. The next process is grouping papers ordered by publication's year. Table 1, shows distribution by scimagojr and publishing year.

TABLE 1. DISTRIBUTION OF JOURNAL RANK

| Publication Year | Quality | | | |
|---|---|---|---|---|
| | *Q2* | *Q3* | *Q4* | *Unknown* |
| 2015 | - | 3 | - | 2 |
| 2016 | 2 | 1 | 2 | 3 |
| 2017 | 1 | 2 | 2 | 1 |
| 2018 | 2 | 5 | 1 | - |
| 2019 | 1 | 5 | - | 1 |

The papers clustered by three categories, steganography, cryptography and parallel mechanism. It results, 5 papers discuss three of them, 5 papers discuss steganography and cryptography, 3 papers discuss steganography with parallel mechanism and 21 papers discuss steganography with many techniques which are developed. Table 2 shows result of the quality assessment of papers.

TABLE 2. RESULT OF QUALITY ASSESSMENT

| No. | Paper's Index | Quartile Category | Cite Counts | Discussion Category | | |
|---|---|---|---|---|---|---|
| | | | | *Cryptography* | *Steganography* | *Parallel Mechanism* |
| 1 | [1] | 3 | 2 | Y | Y | Y |
| 2 | [5] | 4 | 0 | Y | Y | Y |
| 3 | [2] | - | 0 | Y | Y | Y |
| 4 | [4] | - | 2 | Y | Y | - |
| 5 | [6] | - | 1 | Y | Y | Y |
| 6 | [7] | 2 | 27 | Y | Y | Y |
| 7 | [8] | 3 | 3 | Y | Y | - |
| 8 | [9] | 2 | 0 | Y | Y | - |
| 9 | [10] | - | 6 | Y | Y | - |
| 10 | [3] | 4 | 6 | Y | Y | - |
| 11 | [11] | 3 | 2 | - | Y | Y |
| 12 | [12] | 4 | 1 | - | Y | Y |
| 13 | [13] | 2 | 1 | - | Y | Y |
| 14 | [14] | 3 | 1 | - | Y | - |
| 15 | [15] | - | 7 | - | Y | - |
| 16 | [16] | 3 | 0 | - | Y | - |
| 17 | [17] | 3 | 22 | - | Y | - |
| 18 | [18] | - | 10 | - | Y | - |
| 19 | [19] | 2 | 4 | - | Y | - |
| 20 | [20] | 4 | 0 | - | Y | - |
| 21 | [21] | 2 | 3 | - | Y | - |
| 22 | [22] | 3 | 0 | - | Y | - |
| 23 | [23] | - | 1 | - | Y | - |
| 24 | [24] | 4 | 0 | - | Y | - |
| 25 | [25] | 3 | 13 | - | Y | - |
| 26 | [26] | 3 | 10 | - | Y | - |
| 27 | [27] | 3 | 2 | - | Y | - |
| 28 | [28] | 3 | 0 | - | Y | - |
| 29 | [29] | 2 | 5 | - | Y | - |
| 30 | [30] | 3 | 0 | - | Y | - |
| 31 | [31] | 3 | 1 | - | Y | - |
| 32 | [32] | 3 | 0 | - | Y | - |
| 33 | [33] | 3 | 0 | - | Y | - |
| 34 | [34] | 3 | 0 | - | Y | - |

Symbol description: "Y" = the paper discusses the topic according column, "-" = the paper does not discuss the topic according column.

## III. DISCUSSION

*A. Method Development in Steganography and Cryptography*

There are some method was developed in steganography and cryptography since 2015. Paper [6] apply RSA and DWT in cryptography and steganography, the process runs in parallel by dividing the algorithm using Compute Unified Device Architecture (CUDA) block. The parallel mechanism also can run using tools from OpenCV [1]. The parallel mechanism also can implemented into processor, like in [2] research. Another parallel mechanism has been implemented in hardware using Field Programmable Gate Array (FPGA) device [5]. Parallel processing gives an advantage in production speed of stego image processing.

Other paper implemented this mechanism with splitting message object and cover object into several blocks and proceed them in one time, at last the pieces of blocks were joined as the cover image which contained the message object. This process performs in both encode and decode [7].

Combining steganography and cryptography also developed by several papers. A new approach has been being developed to improve message security levels using cryptography and steganography. It implements caesar and vigenere cipher for encryption process and continued with hiding ciphertext using Least Significant Bit (LSB) mechanism in steganography [8]. Encryption using combination of Advanced Encryption System (AES) and compressing message data using Huffman Coding also proposed [9]. Some survey papers mention that combining cryptography techniques and steganography still being developed continuously. [3, 10].

The developing mechanism also performed in steganography and parallel processing mechanisms. From papers obtained, this combination abandons cryptography mechanism. Commonly steganography using LSB technique. One of them divided message and cover into several cores, then hiding message process implemented in parallel. Finally to make a complete stego image, pieces of cores were combined [11]. The parallel mechanism also implemented into FPGA device with creating instruction sets [13] and creating AVX instruction for vectorization [14]. The parallel mechanism in steganography also proposed hiding messages into audio files by calculating histogram and inserting message in parallel processes [12]. The advantages of steganography using parallel mechanisms besides less processing time also eliminate dependency on serial processes [12].

The progress on the other papers purpose modifications in steganography methods. Many researchers contribute to steganography by combining or modifying steganography method, one of them is LSB. A paper purposed an implementation LSB technique performed by considering bit message value before hiding into RGB image as cover [15], LSB also used for hiding messages into the edge of watermark image [17]. Modification LSB also performed with combining using Hash algorithm [18]. Utilization of LSB also combining by generating prime random number to determine message coordinate [20]. Multiple Input and Multiple Output (MIMO) technology with equal distribution modulation Orthogonal Frequency Division Multiplex(OFDM) also combined with LSB [21]. LSB process also applied with calculating the DWT value [23, 30]. Implementation of LSB also developed with counting determinant matrix value to transforms matrix value [33], there is also purposing LSB substitution's implementation with counting value of Pixel Value Differencing (PVD) and Exploiting Modifiction Directing (EMD) [29].

### B. *Popular Measurement Instrument in Steganography*

The research quality needs to be confirmed, so it needs a measurement mechanism that produces quantitative number. Based on obtained papers, The most top three measurement instrument are PSNR, MSE and time calculation. Table 3 shows the measurement mechanism that commonly used.

TABLE 3. VARIETY OF DOMINANT MEASUREMENT INSTRUMENT

| No. | Measurement Instrument | Number of Articles Used |
|---|---|---|
| 1 | Peak Signal to Noise Rasio (PSNR) | 13 |
| 2 | Mean Squared Error (MSE) | 6 |
| 3 | Time Calculation | 8 |
| 4 | Point Distance Histogram (PDH) | 1 |
| 5 | RS Analysis | 1 |

Mean Square Error (MSE) is used for measuring the common distortion of image quality. MSE Calculation of stego image is taken from the average of squares intensity of input and output images. Peak Signal to Noise Ratio (PSNR) is a quantitative measure to identification image quality based on pixel difference between original cover and stego image [33]. MSE and PSNR are calculated by equation as follows.

$$\text{MSE} = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}\left(x_{j,k} - x'_{j,k}\right)^2 \quad (1)$$

[33]

NM is the image dimension. j, k are pixel coordinate. x is original cover. x' is stego image.

$$\text{PSNR} = 10\ \log_{10}\frac{C^2}{MSE} \quad (2)$$

[33]

C is a value in the maximum value of image.

MSE and PSNR value are inversely proportional, this implies that higher PSNR value, lower MSE value. So, it means that if the higher value of PSNR the better the stego image, cause it has lesser error [20]. Measurement using time calculation as the parameter, are used to compare process speed, between recorded time previously and current record time. Most in this paper, time is used for counting speed of parallel mechanism. Point Distance Histogram (PDH) also used as a measurement instrument. It compares input and output images in histogram chart. It compares shape of histograms or number of pixel values that contains in images.

## IV. CONCLUSIONS

Based on the literature review, commonly technique of steganography development was focused on the modification techniques of hiding message into cover, both encode process and decode process. The measurement instruments used in steganography are counting MSE and PSNR when the output is an image. But when developing to speed up the process, measurement instruments commonly use time as parameter. The growth of steganography still being continued, including modification of the algorithm or combing the method. They are developed to give superiority to the steganography's performance. Commonly the proposed methods are still hiding the message inside cover and sending both of them in one stego image. Therefore, it would be better to do further study which focus on how to hide message without hiding the real message into it's cover.

## REFERENCES

[1] Balasubramani A and Rao C S 2016 *International Journal of Applied Engineering Research* **11(9)** 6504

[2] Ahmed M Y and Hasan B T 2019 *ZANCO Journal of Pure and Applied Sciences* **31(2)** 81

[3] Praveenkumar P, Thenmozhi K, Rayappan J B B, and Amirtharajan R 2017 *Research Journal of Information Technology* **9(2)** 46
[4] Gaur M and Sharma M 2015 *International Journal on Recent and Innovation Trends in Computing and Communications* **3(3)** 1344
[5] Desai L and Mali S 2018 *VSLI Design* **2018**
[6] Khatri S, *Mathur* A and Sharma S 2016 *Journal International for Technological Research in Engineering* **4(2)** 424
[7] Rostami M J, Shahba A, Saryazdi S and Nezamabadi-Pour H A 2017 *Computer & Electrical Engineering* **62** 384
[8] Dewangga I G A P, Purboyo T W and Nugraheni RA 2017 *International Journal of Applied Engineering Research* **12(21)** 10626
[9] Sari C A, Ardiansyah G, Setiadi D R I M and Rachmawanto EH 2019 *Telkomnika* **17(5)** 2400
[10] Shrivastava A and Singh L 2016 *International Journal of Advanced Technology and Engineering Exploration* **3(14)** 9
[11] Zhelezov S and Paraskevov H 2015 *Contemporary Engineering Science* **8(18)** 809
[12] Shoaib M, Shehzad D, Umar A I, Khan Z, Dag T and Amin N U 2016 *International Journal of Advanced Computer Science and Applications* **7(10)** 290
[13] Huang C W, Chou C, Chiu Y C and Chang C Y 2018 *Mathematical Problems in Engineering* **2018**
[14] Snasel V, Kromer P, Safarik J and Platos J 2019 *Concurrency Computation Practise and Experience*
[15] Ali T and Doegar A 2015 *International Journal of Advanced Research in Computer Science and Software Engineering* **5(1)** 314
[16] Douglas M, Bailey K, Leeney M and Curran K 2015 *Telkomnika* **13(2)** 125
[17] Darabkh K A, Jafar I F, Al-Zubi R T and Hawa M 2015 *Information Technology and Control* **44(3)** 315
[18] Rafat K F and Hussain M J 2016 *International Journal of Advanced Computer Science and Applications* **7(6)** 45
[19] Fraczek W and Szczypiorski K 2016 *Security and Communication Networks* **9(15)** 2998
[20] Sathyan A, Thirugnanam M and Hazra S A 2016 *IIOAB Journal* **7(5)** 58
[21] ;p;lChen L, Fan Z and Huang J 2016 *International Journal of Electronics and Communications* **70(9)** 1295
[22] Zhelezov S, Dimitrova B U and Parasekovov H 2017 *Journal of Engineering and Applied Science* **12(8)** 8251
[23] Devaraj S A and Wiliam BS 2017 *International Journal of Advanced in Innovative Discoveries in Engineering and Applications* **2(2)** 1
[24] Vinh Q D and Koo I 2017 *Journal of Informations and Communication Convergence Engineering* **15(3)** 151
[25] Duan X, Song H, Qin C and Khan M K 2018 *Computers, Materials and Continua* **55(3)** 483
[26] Hasim M M, Rahim M S M, Johi F A, Taha MS, and Hamad H S 2018 *International Journal of Engineering & Technology* **7(4)** 3505
[27] Marin I R G, Venegas H A M, Romero J R M, Servin J A H, Jimenez V M, and Luna G D I 2018 *International Journal of Pattern Recognition and Artificial Intelligence* **32(1)**
[28] Dewangga I G A P, Purboyo T W and Nugraheni R A 2018 *Journal of Engineering and Applied Science* **13(12)** 4442
[29] Pradhan A, Sekhar K R and Swain G 2018 *Mathematical Problems in Engineering* **2018**
[30] Mathivanan P, Jero S E, Ramu P, and Ganesh A B 2018 *Australasian Physical & Engineering Science in Medicine* **41(4)** 1057
[31] Gao Z and Tang G 2019 *Journal of Internet Technology* **20(1)** 205
[32] Pramanik S, Singh R P and Ghosh R 2019 *Indonesian Journal of Electrical Engineering and Computer Science* **14(3)** 1412
[33] Shehzad D and Dag T 2019 *Transactions on Internet and Information Systems* **13(7)** 3778
[34] Deepikaa S and Saravanan R 2019 *Cybernetics and Informations Technologies* **19(1)** 73