**TELKOMNIKA Telecommunication, Computing, Electronics and Control**
Vol. 18, No. 2, April 2020, pp. 1095~1104
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
DOI: 10.12928/TELKOMNIKA.v18i2.14833 

# DWT-SMM-based audio steganography with RSA encryption and compressive sampling

**Fikri Adhanadi, Ledya Novamizanti, Gelar Budiman**
School of Electrical Engineering, Telkom University, Indonesia

**Article Info**

***Article history:***

Received Jul 20, 2019
Revised Jan 16, 2020
Accepted Feb 19, 2020

***Keywords:***

Audio steganography
Compressive sampling
Encryption
Statistical mean manipulation

**ABSTRACT**

Problems related to confidentiality in information exchange are very important in the digital computer era. Audio steganography is a form of a solution that infuses information into digital audio, and utilizes the limitations of the human hearing system in understanding and detecting sound waves. The steganography system applies compressive sampling (CS) to the process of acquisition and compression of bits in binary images. Rivest, Shamir, and Adleman (RSA) algorithms are used as a system for securing binary image information by generating encryption and decryption key pairs before the process is embedded. The insertion method uses statistical mean manipulation (SMM) in the wavelet domain and low frequency sub-band by dividing the audio frequency sub-band using discrete wavelet transform (DWT) first. The optimal results by using our system are the signal-to-noise ratio (SNR) above 45 decibel (dB) and 5.3833 bit per second (bps) of capacity also our system has resistant to attack filtering, noise, resampling and compression attacks.



***Corresponding Author:***

Ledya Novamizanti,
School of Electrical Engineering,
Telkom University,
Telekomunikasi St., Terusan Buah Batu, Bandung 40257, Indonesia.
Email: ledyaldn@telkomuniversity.ac.id

## 1. INTRODUCTION

The era of digital computers and information technology has become part of the modern society's ecosystem today. Various types of digital information can be accessed and shared easily through various types of digital information service providers on the internet. The ease in exchanging digital information is used by a handful of people to intercept, interrupt, and modify the digital contained therein. Therefore, we need a technique that guarantees and secures the security and confidentiality of digital data, namely steganography.

Steganography is the art of hiding messages inside media so the message inside it cannot be realized by other people. In digital steganography, the secret message requires digital media as vessel or host such as image, audio, text, and video [1, 2]. Robustness, security and hiding capacity are the three major performance criteria that revolve around the existing steganography methods [3]. Effective steganography should have the following characteristics: perceptual transparency (i.e. the cover and the stego object must be imperceptible), high embedding capacity, robustness to various types of attacks and high data rate of the embedded data [4].

In research [5, 6] states that the discrete wavelet transform (DWT) method has good imperceptibility and robustness and it is effective in overcoming the most common types of attacks that designed to destroy the secret message that embedded in the audio. Furthermore, in research [7] states that the audio quality result

through the compressive sampling (CS) process can still be heard clearly, while in research [8] states that the image quality result through the CS process can be reconstructed as before after passing the extraction process and Rivest-Shamir-Adleman (RSA) algorithm decryption process. In research [8-11], it was stated that the implementation of RSA encryption improves the security in wavelet domain-based steganography system by applying the encryption process before transmission, and the decryption process is applied after receiving the encrypted data. Furthermore, in research [12] states that the value of p and q in the RSA encryption process must have a certain value so we must carry out several experiments to check the *p* and *q* values are suitable with our proposed system.

In this paper, we implement CS and RSA encryption on a binary image that embedded to improve security, embedding capacity and robustness to audio attacks. First, embed the binary image with the statistical mean manipulation (SMM) method into a digital audio host that has been divided into frequency sub-bands using DWT. The audio was attacked by using nine types of audio attack such as low-pass filter (LPF), band-pass filter (BPF), noise, resampling, time scale modification (TSM), linear speed change (LSC), pitch shifting, and two types of compression with motion pictures experts group, audio layer 3 (MP3) and advanced audio coding (AAC) formats. The structure of this paper consists of several sections. Section 1 describes introduction, section 2 describes research method, basic formulation of audio steganography method and also describes audio steganography system with embedding and extraction procedures, section 3 describes the performance of the audio steganography method, section 4 describes conclusion.

## 2. PROPOSED METHOD

Explaining research chronological, including research design, research procedure (in the form of algorithms, Pseudocode or other), how to test and data acquisition [1-3]. The description of the course of research should be supported references, so the explanation can be accepted scientifically [2, 4]. The audio steganography system is designed using stereo audio with the * *wav* format and 44100 Hz frequency sampling as the host. This type of steganography utilizes the weakness of the human auditory system. Human auditory system is only able to perceive and detect sound with a frequency range of 20 Hz~20 kHz or -5 dB~130 dB [13]. So, the audio components outside from the frequency range cannot be heard. The embedding of a secret message into digital audio changes the quality of the audio. Therefore, in order to choose a good embedding method for steganography system, we must pay attention to several criteria, such as imperceptibility, secure, capacity, speed, and robustness [13, 14]. While, the embedded data or message is a binary image, which is a black and white image.

In general, the confidential information go through two main processes, namely the embedding process and extraction process. The system model scheme proposed in this study is illustrated in Figure 1. First, the binary image goes through the compressive sampling acquisition process, and then encrypted by using the RSA encryption algorithm. The RSA algorithm is explained in [15]. The next step is to perform the embedding process on wavelet domain using SMM into host audio.

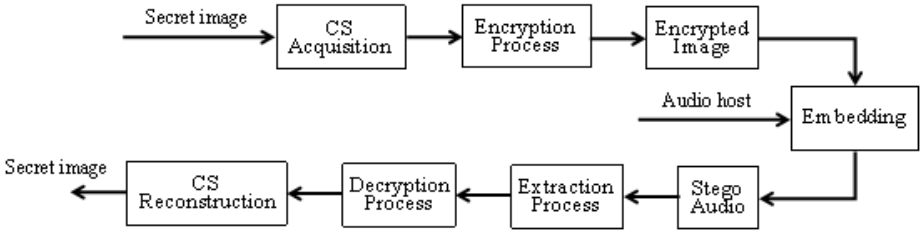



Figure 1. The proposed of steganography system

## 3. RESULTS AND ANALYSIS

### 3.1. Embedding system design

The embedding process of a binary image into a digital audio file on an audio steganography system is being done by using the DWT-SMM method which previously had to go through the CS and RSA encryption process before being embedded. The processed audio file goes through the frequency dividing process that divides the audio signal frequency into a high sub-band and a low sub-band with DWT method, later the low sub-band is chosen as the embedding location. After that, the compressive sampling perform data acquisition from the binary image using bit compression and the output is be encrypted by using RSA encryption algorithm. The encryption process needs an encryption key or public key that has been generated before by using the RSA algorithm.

The next process is embedding after the host audio and the binary image has been processed. The embedding process uses the SMM method that embeds confidential information into low sub-band frequency in a host audio. The reason is based on research [16] which states that embedding the information message at low sub-band frequency can produce better robustness in terms of image distortion caused by LPF. Here's the formula for the SMM embedding technique [17]:
for '1' bit value:

$$x_w(n) = x_{wd}(n) - \mu x + \alpha . w_i \quad (1)$$

for '0' bit value:

$$x_w(n) = x_{wd}(n) - \mu x - \alpha . w_i \quad (2)$$

with $x_{wd}(n)$ is a signal in the wavelet domain, $\mu x$ is the average signal of $x_{wd}(n)$, $\alpha$ is a reliability factor in SMM that ensures the embedding reliability, $w_i$ is embedded message bits information, and $x_w(n)$ is the audio that has been embedded with confidential information. After that, perform inverse to unite the two previously divided sub-bands into whole stego-audio or audio with confidential information message that are successfully embeded into it. The embedding process is shown in Figure 2.

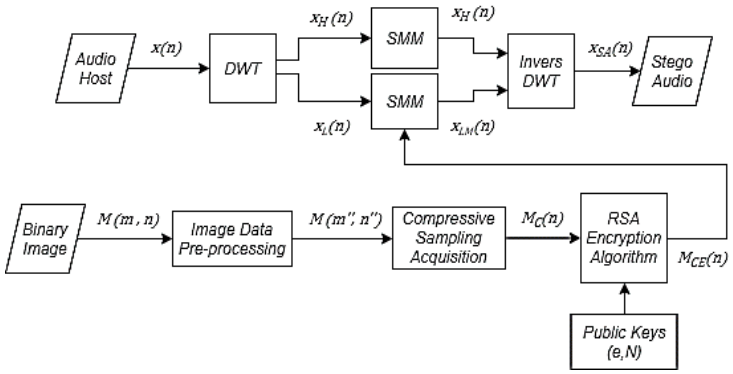



Figure 2. The embedding process flowchart

### 3.2. Extraction system design

The extraction process of a binary image from the digital audio file on audio steganography system is being done by using the DWT-SMM method through a DWT inverse process then decrypted with the RSA decryption algorithm and perform CS reconstruction to reveal the message information. The process is similar to the embedding process, which is to process the stego-audio through the sub-band frequency dividing process with DWT. The low sub-band frequency is processed because the embedded binary image as the message information is embedded at the low sub-band frequency. After successfully extracting the binary image then it has successfully decrypted by using RSA decryption algorithm with a decryption key or private key that has been generated before by using the RSA algorithm. The next process is to reconstruct the bit data of the binary image by using CS, so that the binary image can be revealed again. The model design process is shown in Figure 3.

### 3.3. Pre-processing and CS acquisition process

This stage is done before the data from the information message is embedded into the host audio. Data from the information message that through the acquisition process is a binary image with matrix size $a \times b$. Briefly, the CS acquisition process has successfully compressed the matrix size from the binary image data by the predetermined compression ratio value. So, it can hide the intended data in messages while minimizing its size, enabling us to transfer the data with less overall burden in capacity [18]. CS can be formulated as follows [19]:

$$y = AX + z \quad (3)$$

with $A$ is matrix form of $M \times N$ commonly referred to as sensing matrix who provide the information about $X$, while $z$ is stochastic or an error term that definitely occur with limited energy. The model design process is shown in Figure 4.

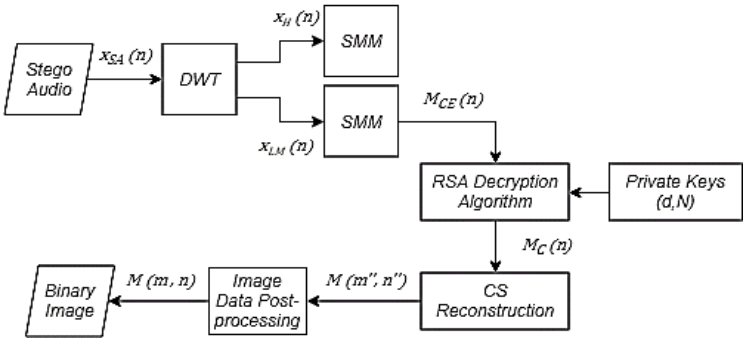



Figure 3. The extraction process

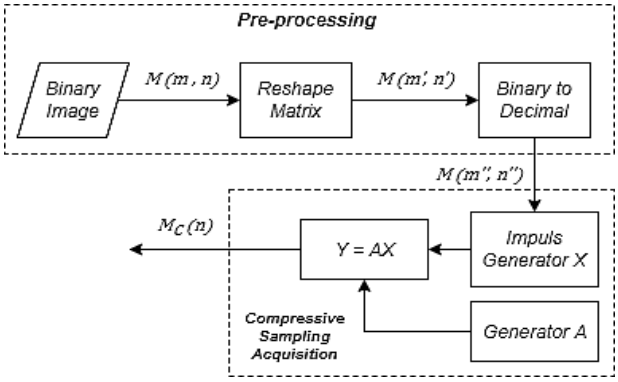



Figure 4. Pre-processing and CS acquisition diagram

The stages of the process are described as follows :

- Read the binary image files in a two-dimensional matrix $M(m,n)$.
- Change the shape of the matrix by setting the matrix column to 8 as input before being processed in CS. So, when entering the CS process, the length of the matrix column becomes 256 with adjusting the row length of the matrix. The output is $M(m',n')$.
- Converts the previously modified matrix into decimal. The output is $M(m'',n'')$.
- Generates impulses with a matrix column length of 256. In the CS concept, the input matrix must be sparse, means that the value 0 often appears.
- Perform scalar multiplication pn the matrix so the output $M_C(n)$ is obtained, namely binary image data that was successfully through the acquisition process.
- The form of the output data from $M_C(n)$ is binary data.

### 3.4. Post-processing and CS reconstruction process

This stage is done after the data from the information message is extracted and decrypted from stego-audio. Data from the information message that through the reconstruction process is a binary image with matrix size $a \times b$. Briefly, the CS reconstruction process has successfully restored the matrix size from the binary image data from the previous process to the original size. Compressible signal can be recovered from a set of few measurements. In fact, this is a key element of CS and how the sensing process relates to the sparse representation determines whether a signal can be recovered or not from the measurements [20]. The model design process is shown in Figure 5.

### 3.5. RSA encryption process

This stage is done before the information data is embedded into the host audio and also after going through the CS process. The purpose of the encryption process is to secure the binary images using a public encryption key. Figure 6 is illustrated that before entering the encryption process, image data in the form of binary data must be converted to decimal. After the encryption process was successful, the data converted back into a binary form. So, it can be processed again to the next stage, which is the embedding process.

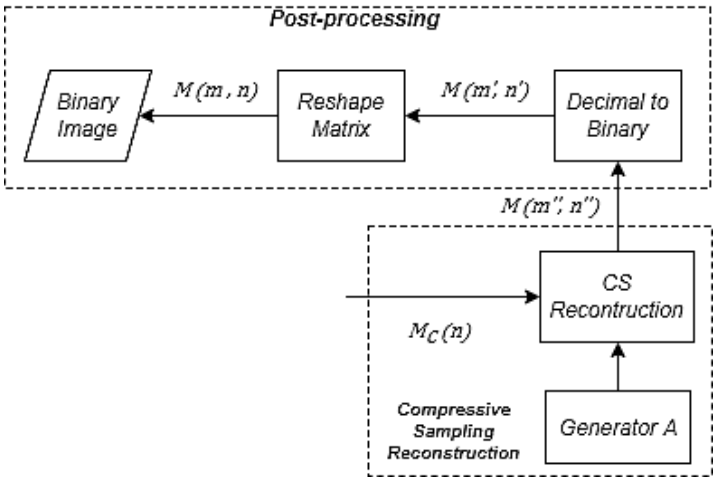



Figure 5. Post-processing and CS reconstruction flowchart

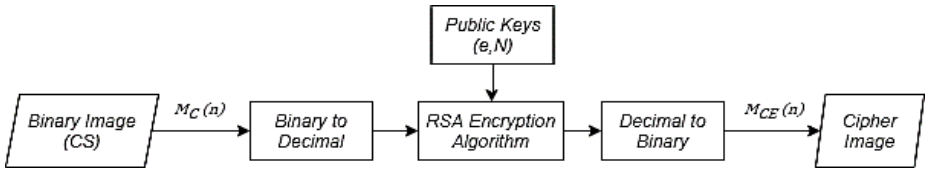



Figure 6. Flowchart of RSA encryption process

### 3.6. Image decryption process

This stage is done after the information data has been extracted from stego-audio. The purpose of the decryption process is to decrypt the binary images that have been extracted using the private decryption key. The decryption process more or less has the same procedure as in the encryption process as shown in Figure 7.

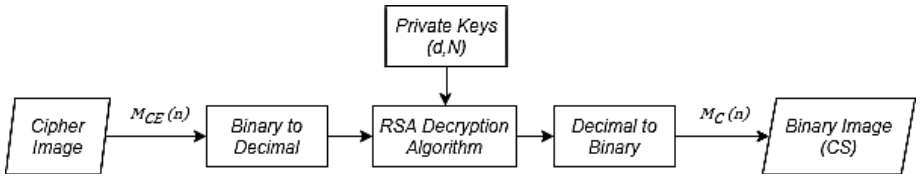



Figure 7. Flowchart of RSA decryption process

## 4. RESULT AND ANALYSIS

System testing is done by using two schemes. The first scheme is done with non-optimized parameters that are more focused towards creating a good imperceptibility from stego-audio and large capacity. The second scheme is done with optimized parameters that focused on creating a good imperceptibility from stego-audio and good robustness against various types of attacks on the stego-audio. The proposed steganography system is evaluated based on the parameters Bit Error Rate (BER), Capacity (C), Objective Different Grade (ODG), Peak Signal to Noise Ratio (PSNR), and Structural Similarity Index Matrix (SSIM). BER value is determined by calculating the percentage of probability of bit error insertion and extraction yield results with an overall bit prior to insertion [21]. Capacity (C) or payload data refers to the number of bits embedded into the audio in a unit time, measured in bits per second (bps) [22]. The objective quality of the modified audio signal which is calculated using ODG. ODG value range starting from -4 to 0. ODG 0 which means the audio quality imperceptible [23]. PSNR is the ratio between the maximum value of the measured bit depth of the image and the amount of noise that affects the signal. PSNR is usually measured in units (dB). The greater the PSNR value, the better the image quality or closer to the original image. SSIM is an index to measure the degree of similarity between the two images, the image after processing compared to the original image. SSIM compares

distortion from luminance, contrast and structural. The SSIM value of 0 means there is no similarity between the two images, while the value of SSIM 1 means that the two images being compared are very identical [24].The test involves five different types of audio such as voice, piano, guitar, drum, and orchestra. The information message that embedded into host audio is a binary image with a size of 64×64 pixel that encrypted by using a pair of keys that have been generated with the RSA algorithm. Figure 8 is a binary image that is inserted into the audio.

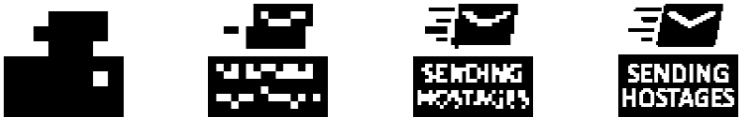
### 4.1. Compressive sampling performance

CS performance testing on binary images is based on the parameter of the bit compression ratio at 0.02 with side parameters that changed starting from using sides 8, 16, 32 and 64. The selection of bit compression ratio is 0.02 because it produces an image compression ratio of 62.52% when compared to the bit compression ratio of 0.025 or 0.03 with the image compression ratio of 75% and 100%. The smaller the percentage compression value of the image, the less the number of constituent bits that affect the computation time. Figure 9 provides a compressed images comparison with different side values.

Based on Figure 9, it can be concluded that the smaller the value side, the quality of the compressed image is getting worse. Side 64 produces compressed images with good quality. This is caused by the bit compression process which reduces the number of bits in the binary insert image.


(a) (b)

Figure 8. Information message



Side = 8 Side = 16 Side = 32 Side = 64

Figure 9. CS compression images comparison

### 4.2. RSA algorithm performance

This stages is done by choosing the key pairs that have been generated with a success level of the encryption and decrypting the binary image. There are 210 pairs of a prime number keys that generated without any key pairs with the same element of prime number. The value of generated prime numbers is in the range of 0 to 50. Based on the simulation, only half of these key pairs that can successfully process encryption and decryption from the steganography system. RSA algorithm has limited functions when combined with the SMM method which plays a role in the embedding and extraction process. The value of $p = 7$ and the value of $q = 11$ is chosen to generate the encryption key pair and its decryption, because that value produces bit error rate (BER) $\neq 0$, and successfully in the encryption and decryption process. The computation time in the encryption and decryption process is shown in Table 1.

The result of the encryption key and the decryption key is successfully generated 7 and 43 by using the value of p and q are selected. Based on the value, the key can be categorized as the key with the number of bits equal to 8. According to [25], the key with the number of bits equal to 32 can be cracked by takes 35.8 minutes. While the key with the number of bits equal to 8 need only takes 1.2μs. It can be concluded that the greater the number of bits in the key, the more difficult to break into. However, the time needed in the encryption and decryption process is lasting longer.

Table 1. The computational time of RSA encryption and decryption

| Process | Computational Time |
|---|---|
| Encryption | 0.001387 second |
| Decryption | 0.020651 second |

### 4.3. Non-optimized parameters performance

In this stage, we are testing this scheme by using a uniform non-optimized parameters for decomposition level (n), length of the frame (Nframe) and threshold (thr) sequentially with 1, 1024 and 0.9 as input values. Relibility factor value (α) is a parameter value that has a different value for each audio. The value of reliability factor for audio type voice, piano, guitar, drum and orchestra based on the order are 0.0015, 0.0055, 0.0035, 0.003 and 0.0035. There are two things that are analyzed, namely the CS influence on

computation time and audio robustness against the nine types of attacks that have been mentioned earlier. Table 2 shows the result of the computation time between CS and without using CS.

From Table 2, the CS utilization can speed up computing time by 30%. It means that the embedding and extraction process is 30% faster when compared to without using CS. Moving on to the average value of BER analysis that obtained from nine types of audio attacks by using non-optimized parameters as shown in Figure 10. Based on the data contained in Figure 8 the average value of BER obtained by each type of audio attack can be categorized as bad value because the average value result touches the number 0.5. If it converted in percentage form, the error in the binary image compiler bit reaches 50%.

Table 2. Computing time comparison

| Scheme | Embedding Time | Extraction Time |
|---|---|---|
| With CS | 1.319 second | 0.801 second |
| Without CS | 1.902 second | 1.117372 second |

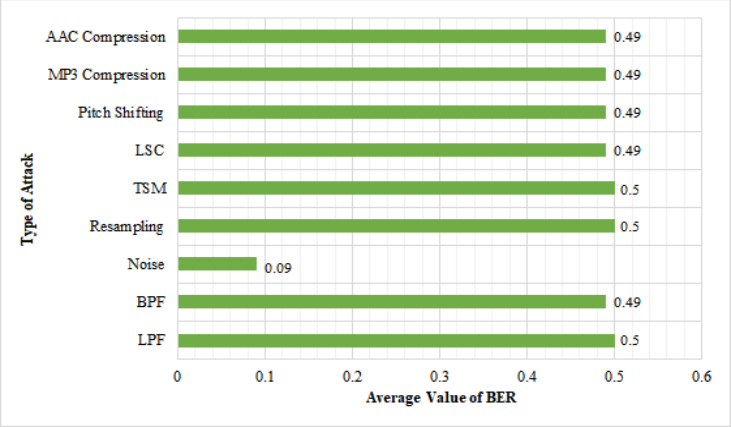



Figure 10. BER result by using non-optimized parameters

### 4.4. Optimized parameters scheme performance

Optimized parameters are obtained by evaluating the highest BER value in non-optimized parameters. So that, the parameters for decomposition level (n), length of the frame (Nframe) and threshold (thr) sequentially with 2, 2048 dan 0.9 as input values. In this scheme, the reliability factor value (α) also changes. The value of reliability factor for audio type voice, piano, guitar, drum and orchestra based on the order are 0.00038, 0.00085, 0.00085, 0.00015 dan 0.00085. There are two things that are analyzed, such as a change in capacity value after using the optimized parameters and audio robustness against the nine types of attacks that have been mentioned earlier. Figure 11 contains a capacity comparison data between using non-optimized and optimized parameters.

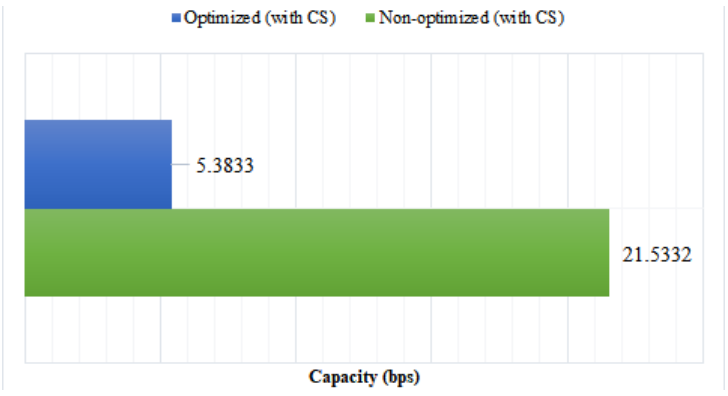



Figure 11. Capacity comparison result between two schemes

Based on Figure 11, It can be seen that there was a decreasing value in capacity. This is because to pursue the steganography criteria with good imperceptibility and have relatively good robustness against audio attack than in terms of capacity must be sacrificed. Figure 12 shows the average value of BER analysis that obtained from nine types of audio attacks by using optimized parameters and non-optimized parameters. Five out of nine types of attacks decreased in the average BER value, while for the noise type attack there was a slight increase. In the case of a TSM attack, LSC attack also pitch shifting did not change at all.

Futhermore, we analyze the optimal parameters in each audio type based on Signal-to-Noise Ratio (SNR) and ODG. The SNR value obtained by each type of audio can reach rates above 40 decibels (dB) with ODG values ranging from -1 to -2. This indicates that the stego-audio result have minimal distortion or it can be said to be almost the same as the original audio file. Table 3 shows SNR and ODG results using optimal parameters.

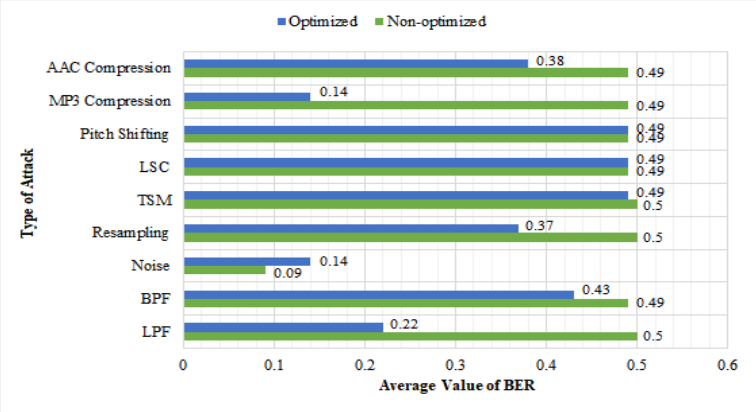



Figure 12. Comparison type of attack on average BER

Table 3. SNR and ODG results with optimal parameters

| Host Audio | voice | piano | guitar | drum | orchestra |
|---|---|---|---|---|---|
| SNR | 45.4526 | 49.6711 | 44.2453 | 58.9779 | 45.9193 |
| ODG | -1.5108 | -2.4067 | -2.0748 | -1.1216 | -2.0543 |

### 4.5. System performance results

The optimal parameters of audio with an attacked condition and the binary image is successfully extracted. PSNR and SSIM values are obtained when BER = 0 is infinite (∞) and 1, it means that extraction of a binary image has been successfully reconstructed and have similarities that are identical to the input image so that such values can be obtained. In the other hand, for attacks that make a tone shift, modification of time and speed on the audio signal produces a poor BER value so that it also affects the PSNR and SSIM values. The data from the analysis are shown in Table 4.

Table 4. System performance results with optimal parameters

| Type of Attack | Parameter | BER | PSNR | SSIM |
|---|---|---|---|---|
| LPF | 12k | 0 | ∞ | 1 |
| | 15k | 0 | ∞ | 1 |
| *Noise* | 40 dB | 0 | ∞ | 1 |
| | 50 dB | 0 | ∞ | 1 |
| MP3 | 128k | 0 | ∞ | 1 |
| | 192k | 0 | ∞ | 1 |
| | 256k | 0 | ∞ | 1 |
| *Resampling* | 24k | 0 | ∞ | 1 |
| *Time Scale Modification* | 1% | 0.482 | 3.192 | 0.036 |
| | 2% | 0.5 | 2.968 | -0.032 |
| *Linear Speed Change* | 1% | 0.493 | 3.018 | -0.019 |
| | 5% | 0.481 | 3.194 | 0.019 |
| *Pitch Shifting* | 1% | 0.494 | 3.018 | -0.022 |
| | 2% | 0.492 | 2.261 | -0.033 |

## 5. CONCLUSION

In this paper, RSA encryption and Compressive Sampling for DWT-SMM-based Audio Steganography has been proposed. The utilization of RSA algorithm in order to increase the security toward binary image said to be successful but also has a limitation in key when combined with the SMM as the embedding and extraction method. The compressive sampling utilization in binary imagery has succeeded in producing a steganography system with a capacity of 5.3833 bps with optimal parameters, and also obtaining a steganography system with 30% faster computation time during the embedding and extraction process. The results with optimal parameters on testing by using proposed method succeeded in obtaining an SNR average value above 45 dB and obtaining ODG values in the range of -1 to -2 and successfully obtain a good level of imperceptibility with the stego-audio quality resembling the original audio.The results with optimal parameters on testing using this method also produce excellent PSNR and SSIM values on extracted images with BER 0 when stego-audio was attacked by using low-pass filter with a range between 12000-15000 Hz, noise with level ≥ 40 dB, resampling with sample rate 24000 Hz, and MP3 compression with bit rate ≥ 128 kilobit per second. However, the proposed steganography system also has extremely low robustness against linear speed change, time scale modification dan pitch shifting attack with an average value of BER is 0.49.

## REFERENCES


[1] A. K. Saxena, S. Sinha, and P. Shukla, "Design and development of image security Technique by using cryptography and steganography: A combine approach," *International Journal of Image, Graphics and Signal Processing*, vol. 10, no. 4, pp. 13–21, 2018.

[2] I. A. Sattar and M. T. Gaata, "Image steganography technique based on adaptive random key generator with suitable cover selection," *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, pp. 208-212, 2017.

[3] F. Djebbar, B. Ayad, K. A. Meraim and H. Hamam, "Comparative study of digital audio steganography techniques," in *EURASIP Journal on Audio, Speech, and Music Processing*, vol. 12, no. 1, pp. 1-16, 2012.

[4] S. E. El-Khamy, N. O. Korany and M. H. El-Sherif, "A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption," *Multimedia Tools and Applications*, vol. 76, no. 22, pp. 24091–24106, 2017.

[5] H. Nikmehr and S. T. Hashemy, "New approach to audio watermarking using Discrete Wavelet and Cosine Transforms," *1st International Conference on Communication Engineering*, 2010.

[6] M. Lihua, Y.Shuangyuan and J. Qingshan, "A new algorithm for digital audio watermarking based on DWT," in *WRI Global Congress on Intelligent Systems*, pp. 229-233, 2009.

[7] M. Zaheer, I. M. Qureshi, Z. Muzaffar and L. Aslam, "Compressed sensing based image steganography system for secure transmission of audio message with enhanced security," *International Journal of Computer Science and Network Security*, vol. 17, no. 7, pp. 133-141,2017.

[8] F. K. Ranjbar and S. Ghofrani, "Evaluation compressive sensing recovery algorithms in crypto steganography system," *International Journal of Image, Graphics and Signal Processing (IJIGSP)*, vol. 8, no. 10, pp. 53-63, 2016.

[9] S. Varghese and L. Kamal, "Enhanced RSA combined with DWT domain watermarking," in *International Journal of Modern Engineering Research*, vol. 2, no. 2, pp. 18-20, 2012.

[10] P. Patel and Y. Patel, "Secure and authentic DCT image steganography through DWT-SVD based Digital watermarking with RSA encryption," in *Fifth International Conference on Communication Systems and Network Technologies*, Gwalior, pp. 736-739, 2015.

[11] S. Saraireh, "A secure data communication system using cryptogaphy and steganography," in *International journal of Computer Networks & Communications*, vol. 5, no. 3, pp. 125–137, 2013

[12] L. Novamizanti, G. Budiman, and I. I. Tritoasmoro, "Designing secured data using a combination of LZW compression, RSA encryption, and DCT steganography," *2015 1st International Conference on Wireless and Telematics (ICWT)*, pp. 1-6, 2015.

[13] X. Wen, X. Ding, J. Li, L. Gao and H. Sun, "An Audio Watermarking Algorithm Based on Fast Fourier Transform," in *International Conference on Information Management, Innovation Management and Industrial Engineering*, vol. 1, pp. 363-366, 2009.

[14] S. Gupta and D. N. Dhanda, "Audio steganography using discrete wavelet transformation (DWT) & discrete cosine transformation (DCT)," *IOSR Journal of Computer Engineering*, vol. 17, no. 2, pp. 32-44, 2015.

[15] E. R. Arboleda, J. L. Balaba, J. C. L. Espineli, "Chaotic Rivest-Shamir-Adlerman algorithm with data encryption standard scheduling," *Bulletin of Electrical Engineering and Informatics*, vol. 6, no. 3, pp. 219-227, 2017.

[16] X.-Y. Liu and X.-Y. Wan, "Wavelet based a new method of digital watermark," *Wavelet Active Media Technology and Information Processing*, 2006.

[17] Y. Lin and W. H. Abdulla, "Audio watermark a comprehensive foundation using MATLAB," Switzerland, *Springer International Publishing*, 2015.

[18] O. F. A. Wahab, A. I. Hussein, H. F. A. Hamed, H. M. Kelash, A. A. M. Khalaf, and H. M. Ali, "Hiding data in images using steganography techniques with compression algorithms," *TELKOMNIKA Telecommunication Computing Electronics and Control*, vol. 17, no. 3, pp. 1168-1175, 2019.

[19] E. J. Cande´s and M. B. Wakin, "An introduction to compressive sampling," *IEEE Signal Processing Magazine*, vol. 25, no. 2, pp. 21-30, 2008.

[20] M. H. Conde, "Compressive Sensing for the Photonic Mixer Device Fundamentals, Methods and Results," *Siegen: Springer Nature*, 2017.
[21] S. Wu, J. Huang, D. Huang and Y. Q. Shi, "Efficiently self-synchronized audio watermarking for assured audio data transmission," *IEEE Trans-Actions on Broadcasting*, vol. 51, no. 1, pp. 69-76, 2005.
[22] A. Malik, G. Sikka, and H. K. Verma, "A high capacity text steganography scheme based on LZW compression and color coding," *Engineering Science and Technology, an International Journa*l, vol. 20, no. 1, pp. 72-79, 2017.
[23] T. Thiede et al, "PEAQ-the ITU Standard for objective measurement of perceived audio quality," *Journal of the Audio Engineering Society*, vol. 48, no. 1, pp. 3-29, 2000.
[24] A. Hore and D. Ziou, "Image quality metrics: PSNR vs. SSIM," *2010 20th International Conference on Pattern Recognition*, pp. 2366-2369, 2010.
[25] W. Stallings, "Data and computer communication," New York: London, 1988.

## BIOGRAPHIES OF AUTHORS

**Fikri Adhanadi** received the Bachelor of engineering degree (S.T.).in telecommunication engineering from Telkom University, Indonesia, in 2019. He was research assistant in Audio Processing Research Laboratory. His research interests are in the areas of signal processing, and watermarking.

**Ledya Novamizanti** received the Bachelor of science degree (S.Si.) in mathematics from Andalas University, Indonesia in 2005. She received the Master of engineering degree (M.T.) in electrical engineering from Telkom University, Indonesia, in 2018. She has been working as a lecturer in Telkom University since 2010. Her current research interests include signal processing, computer vision, and pattern recognition, and artificial intelligence.

**Gelar Budiman** received B.S. and M.S. degree in electrical engineering from Sekolah Tinggi Teknologi Telkom (STTT), Bandung, Indonesia. He has been working as a lecturer in Telkom University since 2008. He has been currently taking doctoral degree in School of Electrical Engineering and Informatics, Bandung Technology Institute (ITB), since 2015. His research interests are in the areas of wireless communication, signal processing and watermarking.