Steganography on multiple MP3 files using spread spectrum and Shamir’s secret sharing

N. M. Yoeseph, F. A. Purnomo, B. K. Riasti, M. A. Safiie, T. N. Hidayat
Informatics Engineering Program Sebelas Maret University,
Jl. Ir. Sutami 36A Kentingan Jebres Surakarta 57126, INDONESIA
Email: nanangmy@mipa.uns.ac.id

Abstract. The purpose of steganography is how to hide data into another media. In order to increase security of data, steganography technique is often combined with cryptography. The weakness of this combination technique is the data was centralized. Therefore, a steganography technique is develop by using combination of spread spectrum and secret sharing technique. In steganography with secret sharing, shares of data is created and hidden in several medium. Medium used to concealed shares were MP3 files. Hiding technique used was Spread Spectrum. Secret sharing scheme used was Shamir’s Secret Sharing. The result showed that steganography with spread spectrum combined with Shamir’s Secret Share using MP3 files as medium produce a technique that could hid data into several cover. To extract and reconstruct the data hidden in stego object, it is needed the amount of stego object which more or equal to its threshold. Furthermore, stego objects were imperceptible and robust.

1. Introduction
Steganography is art and science to hide a secret message into another media. The hiding of message is done so the third person is not aware of the existence of such message. To improve data security, steganography usually combined with cryptography [1, 2, 3, 4]. According to Tiend and Lin as quoted by [5], the weakness of combination technique of steganography and cryptography is that the data was centralized.

Solution to overcome the weaknesses is by using secret sharing. In this method, secret message processed to produce shares which will be distributed to a number of parties. One of secret sharing technique is \((k,n)\) threshold secret share [6] (Shamir, 1979), or known as Shamir’s Secret Share. Spread Spectrum is a transmission technique using a pseudo-noise code which is independent of the data to modulate a signal with a greater bandwidth than the bandwidth required to transmit the data signals. One of the advantages of Spread Spectrum is its resistance to jamming and interference.

Therefore, a steganography technique is required to hide secret data into several cover object to increases security of the data. In this research, cover object used was MP3 files. It was chosen because of its popularity. To hide data into its cover, the combination of spread spectrum and secret sharing was used. Thus, it can increase the security of data hidden, and simultaneously produce a robust stego object.
2. Analysis
System steganography in the MP3 file created consists of two processes, namely the process to cover data hiding and extraction process and the reconstruction of data from the stego object. In the process of data hiding, secret data is splitted into a number of shares. Splitting is using Shamir's Secret Sharing algorithms. Hiding data using Direct Sequence Spread Spectrum (DSSS). The results of the process of data hiding is several stego objects.

In the extraction process and the reconstruction of data from the stego objects, several stego data are processed to be taken the data which had been hidden. Then stego data is reconstructed to obtain its secret data. The reconstruction process using the inverse of the algorithm Shamir's Secret Sharing.

3. Basic Concepts
In this section, basic theories used in hiding scheme and also in data extraction and reconstruction is presented. In principle, the steganography process is done by adding an addition signal to the original signal. Figure 1 ilustrate the steganography process, where \( y(n) \) is a stego object, \( x(n) \) is cover signal, and \( c(n) \) is the signal hidden.

![Steganography Process](image)

**Figure 1. Steganography Process**

3.1. Direct Sequence Spread Spectrum
Direct Sequence Spread Spectrum (DSSS) used a pseudorandom sequence and a signal modulator to modulating bit stream data. DSSS technique that uses redundancy and scrambles the data before modulated bit stream and reverse the process on the receiving side of recovery is called Direct Sequence [7].

Because a pseudorandom sequence (PN) is used at the transmitter to modulate the signal, the first requirement at the receiver is to have a local copy of this PN sequence. The copy is needed to de-spread the incoming signal. This is done by multiplying the incoming signal by the local PN sequence copy. To accomplish a good de-spreading, the local copy has to be synchronized with the incoming signal and the PN sequence that was used in the spreading process [7].

DSSS signal is indicated by the equation (1).

\[
x(t) = \sqrt{2S} \sin \left[ \omega_0 t + \frac{d_n c_{N+k} N}{2} \right] = d_n c_{N+k} \sqrt{2S} \cos(\omega_0 t)
\]

3.2. Psychoacoustic Auditory Model
Psychoacoustic Auditory Model (PAM) is an algorithm that tries to model human auditory systems. PAM is used to process information from the audio signal and determining its masking threshold. Masking threshold is used to form the stego signal that will be hidden inside the media cover. Stego signal formed from this process will not be detected by the human sense of hearing [7].

The psychoacoustic model used by calculate the doorstep of masking on the critical strip scale to respect to best the physiology of the auditory perception. The DSP of the audio signal is transposed in the scale of Bark by integration of the power in every coins strip. The unique display function is applied for the modeling of the effects of masking of the membrane basilar [8]. Algorithm uses by [8] presented in Figure 2.
3.3. Secret Sharing

The idea of secret sharing is to divide the secret key into several parts, called shares, and share it with some people. Only a subset of those people who can not/are allowed to establish initial key back. The fundamental approach of secret sharing is done by Shamir and Blakley in 1979 with the name (k, n)-threshold scheme. Threshold secret sharing scheme is a protocol between 1+n player (including a dealer and n participant). Dealer distributes partial information (share) on a secret into n participant (distribution) so that (a) each group with a number k participant can know the secret data stored (recovery) in time polynomial, (b) the scheme is declared perfect if the group with the number of members smaller than k will not be able to obtain any information about the secret data stored, (c) the scheme is declared ideal if every size bits of the same shares with confidential data that is hidden [9].

If a secret data, S, will be divided, then S should be changed to polynomial. If S will be divided into n sections (S₁, S₂, ..., Sₙ), then a random coefficient cₙ₋₁ is generated and formed a polynomial equation of degree (n-1), as shown in equation (2).

\[ f(x) = c₀ + c₁x + c₂x² + \cdots + c_{(n-1)}x^{(n-1)} \]  

(2)

Then, shares is calculated according to equation (3)

\[ S₁ = f(1), S₂ = f(2), ..., Sₙ = f(n) \]  

(3)

4. Hiding Scheme

In this research, a system which can do a steganographic process will be built. The medium used as cover is several audio with MP3 filetype. Secret data to be hide is text. The result of the process are multiple audio files which hid the secret data, called stego object. Data hidden in stego object called stego data.

In the Data Hiding, data splitted before it hide into several cover. Splitting is using Shamir’s Secret Sharing algorithm. Hiding process using Direct Sequence Spread Spectrum (DSSS). The result of Data Hiding process are stego objects. Phases in the Data Hiding process are preprocessing data and data hiding. In preprocessing data, secret data is splitted into shares using Shamir’s Secret Share method. Meanwhile, MP3 files which will be uses as cover object is being decoded. Data is hide using Direct Sequence Spread Spectrum (DSSS). Data hiding scheme is shown in Figure 3.
In hiding process, data hiding is done in a segments of signal called frames. Psychoacoustic models used to analysis and calculate masking threshold. PN sequence is generated and modulated with shares. Using masking threshold and modulated signal, new signal with secret data is created in frequency domain. New audio signal is created by adding secret data signal and MP3 cover object. Hiding process scheme is presented in Figure 4.

5. Experiments
The steganography system using MP3 files as cover. It has ability to hide secret data into multiple cover. Besides that, the system can extract and reconstruct hidden secret data from several MP3 files. To reconstruct data correctly, it requires a minimum number of shares at least equal to its threshold. In extraction data, not all stego data could be recovered with 100% accuracy. It is because of multiple factors that affect quality of the embedded stego data, such as the number of audio components replaced, and the gain affect. Data reconstruction done to get secret data from its shares. The result was secret data hidden in the cover.

5.1. Functionality test
The testing was done by hiding secret data into several MP3 files, then extraction and reconstruction process was done to retrieve hidden data. Meanwhile, threshold value was also varied to know the affect to the retrieved data. The data hidden into the cover is 1080 bits. Variations made to the amount of cover and its threshold value. In this test, Bit Error Rate (BER) is calculated from recovered data. Functionality test result is shown in Table 1.
Secret data hide in its cover is 1080 bits. Threshold shows the minimum number of shares required to successfully construct secret data. Stego object shows the number of stego object extracted to get its stego data (share). Bit Error Ratio (BER) shows error rate between the secret data which reconstruct...
from stego object and secret data which is hidden in cover. The result shows that to reconstruct data correctly, the minimum number of shares required is at least equal to its threshold.

### Table 1. Functionality Test Result

| No | Data (bits) | Cover | Threshold | Stego Object | BER (%) |
|----|-------------|-------|-----------|--------------|---------|
| 1  | 1080        | 5     | 5         | 4            | 37.5    |
| 2  | 1080        | 5     | 5         | 5            | 0       |
| 3  | 1080        | 6     | 5         | 4            | 54.7    |
| 4  | 1080        | 6     | 5         | 5            | 0       |
| 5  | 1080        | 6     | 5         | 6            | 0       |
| 6  | 1080        | 6     | 6         | 4            | 62.5    |
| 7  | 1080        | 6     | 6         | 5            | 62.5    |
| 8  | 1080        | 6     | 6         | 6            | 0       |

#### 5.2. Audio Quality Test

Audio quality testing was done by measuring audio quality of cover before and after hiding process. Parameter measured was Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). In experiment, audio quality tested by comparing MSE and PSNR of a pair of cover-stego object. Variation done in the value of bits which to be hide, i.e. 360, 420, 600, and 1080 bits.

MSE value of the average for the fourth sample was 0.023. MSE is small enough shows that the audio quality before and after data hiding has not changed much. While the average PSNR for the fourth sample is 129.426 dB. This suggests that the process of data hiding have an effect that is small enough to change the audio quality of the cover is used.

#### 5.3. Robustness Test

Robustness test was done by applying modification to stego object using StarMark for Audio (SMFA). With the change of signal of stego object, the data hidden is expected to change so it could not be reconstruct. The robustness of data from modification shows robustness of algorithm from modification type that applied. Modification on stego object called attack. The type of attack applied on stego object was single attack.

After being attack, extraction and reconstruction process will be doing on stego object. If secret data in stego object was still could be retrieve, it means that the data in stego object is robust against that type of modification applied.

The result of robustness test is presented in Table 2. Data in stego object before the attack and data after the attack applied is compared. If data is changed, showed by the increase of BER, then the attack had change the data hidden in cover object. On another word, stego object is not robust to this type of attack. Meanwhile, if BER is 0, then the attack has no effect to the data hidden.

### Table 2. Robustness Test Result

| Type of Attack     | Effect on Data        | Type of Attack | Effect on Data | Type of Attack | Effect on Data |
|--------------------|-----------------------|----------------|----------------|----------------|----------------|
| AddNoise           | BER increase when Strength>700 | Amplify        | BER increase when Factor>300 | Invert          | BER increase 100% |
| AddDynNoise        | BER increase when Strength>20   | Normalizer1    | Effects        | FFT_Invert     | BER increase 100% |
| Operation       | No Effects | Normalizer2 | CopySample | BER increase | FlippSample | BER increase |
|-----------------|------------|-------------|------------|--------------|-------------|--------------|
| AddFFTNoise     | No Effects | Normalizer2 | CopySample | BER increase | No Effects   | No Effects   |
| NoiseMax        | No Effects | Compressor  | No Effects | CopySample   | FlippSample | No Effects   |
| AddBrumm        | No Effects | BassBoost   | No Effects | Exchange      | No Effects   | No Effects   |
| FlippSample     | No Effects | RC_HighPass | No Effects | CutSample    | BER increase| No Effects   |
| RC_LowPass      | No Effects | RC_LowPass  | No Effects | ZeroCross    | No Effects   | No Effects   |
| Stat1           | No Effects | Stat2       | No Effects | ZeroLength1  | No Effects   | No Effects   |
| Stat2           | No Effects | Stat2       | No Effects | ZeroLength2  | No Effects   | No Effects   |
| Smooth1         | No Effects | Smooth2     | No Effects | ZeroRemove   | No Effects   | No Effects   |
| Smooth2         | No Effects | Smooth2     | No Effects | ZeroRemove   | No Effects   | No Effects   |

6. Conclusion
Steganographic system is constructed by combining a spread spectrum technique with Shamir's Secret Sharing can perform data hiding inside some of the audio files to MP3 format as the media cover. Based on the functionality testing, steganography system can extract and reconstruct the secret data in stego stego object only when the object is used as an input amount is greater or equal to the threshold value.
The audio quality of media cover before and after hiding the data has not changed much, judging from the average value of MSE, ie 0,023, and amounted to 129.426 dB PSNR. Of the 29 types of attacks are simulated using StirMark Benchmark for audio, data stored in the object Stego has a resistance of 72.41%, or able to survive from the 21 of 29 types of attacks.

References
[1] Rao BR, Kumar PA, Rao KRM, Nagu M 2010 Indian Journal of Computer Science and Engineering, 1(4), pp.327–332
[2] Atoum MS, Al Rababaa MS, Ibrahim S, Ahmed OA 2011 International Journal of Computer Science and Network Security, 11 (5) p 184-188
[3] Khan MdS, Bhasker VV, Nagaraju VS 2011 International Journal of Computer Application (0975-8887) 33(4)
[4] Negrat AM and Kumar A 2010 In Proceedings of the 10th WSEAS International Conference on Signal Processing, Computational Geometry and Artificial Vision p 13–16
[5] Chan KFP 2011 Proceedings of the Information Security for South Africa Johannesburg
[6] Shamir A 1979 Communications of the ACM 22(11), p 612–613. Available at: http://portal.acm.org/citation.cfm?doid=359168.359176
[7] Garcia RA 1999 Digital Watermarking of Audio Signal Using A Psychoacoustic Auditory Model and Spread Spectrum Theory, Master Thesis, School of Music University of Miami, Florida.
[8] Barkouti W, Salhi L, Cherif A 2011 An International Journal (SIPIJ) 2(2)
[9] Lv C, Jia X, Tian L, Jing J, Sun M 2010 Fourth International Conference on Network and System Security, doi:10.1109/NSS.2010.82