# Implementasi Skema Pembagian Data Rahasia untuk Berkas Suara

Melita – 13519063 (*Author*)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): teresamelita1501@gmail.com

***Abstract*—Salah satu cara untuk mengenkripsi data pada kriptografi adalah dengan skema pembagian data. Kriptografi visual adalah penerapan skema pembagian data yang menggunakan bantuan indra penglihatan manusia untuk mendekripsi pesan dari sejumlah *share.* Makalah ini akan menjelaskan sebuah percobaan penerapan dari skema pembagian data pada berkas suara yang menyerupai konsep kriptografi visual sedemikian rupa sehingga dekripsi dapat dilakukan hanya dari pemutaran sejumlah *share* suara secara tepat bersamaan.**

***Keywords—share; suara; pembagian data; interferensi gelombang***

## I. PENDAHULUAN

Seiring dengan berkembangnya teknologi digital, penggunaan media digital untuk pengiriman pesan pun semakin bertambah banyak. Sekarang, pesan dalam komunikasi melalui media digital dapat dilakukan tidak hanya dalam bentuk teks, melainkan juga dalam bentuk suara dan video. Akan tetapi, data dari pesan tersebut akan dikirim kepada penerima pesan melalui jaringan yang dapat diakses oleh banyak orang, sehingga keamanan dan kerahasiaan data dalam pengiriman pesan menjadi hal penting yang harus diperhatikan.

Ilmu yang mempelajari mengenai penjagaan kerahasiaan pesan disebut dengan kriptografi. Dalam pengiriman pesan, kriptografi dapat memberikan empat layanan, yaitu kerahasiaan pesan *(confidentiality)*, keaslian pesan *(integrity)*, keaslian pengirim dan penerima *(authentication)*, dan antipenyangkalan *(nonrepudiation)*. Kriptografi dapat menjamin kerahasiaan dari sebuah pesan dengan cara melakukan proses yang disebut dengan enkripsi untuk mengubah pesan asli (plainteks) menjadi pesan yang disandikan (cipherteks) sehingga maknanya tidak dapat dipahami oleh pihak ketiga.

Selain dengan melakukan enkripsi, sebuah pesan juga dapat dirahasiakan dengan menggunakan skema pembagian data rahasia. Skema pembagian data rahasia *(secret sharing scheme)* adalah teknik yang dapat membagi sebuah pesan menjadi sejumlah pesan bagian *(share)* yang dapat dikombinasikan kembali untuk merekonstruksi ulang pesan awal. Salah satu bentuk ilmu kriptografi yang menggunakan skema tersebut adalah kriptografi visual yang akan membagi sebuah gambar ke dalam beberapa *share* sehingga data dapat didekripsi cukup dengan menggunakan indra penglihatan manusia. Dalam makalah ini, penulis akan mencoba melakukan implementasi skema pembagian data yang serupa dengan kriptografi visual untuk berkas berbentuk suara sehingga dekripsi dari pesan dapat dilakukan hanya dengan memutar *share* suara secara tepat bersamaan.

## II. LANDASAN TEORI

### A. Skema Pembagian Data

Skema pembagian data adalah salah satu cara perahasiaan pesan dalam ilmu kriptografi yang membagi sebuah pesan rahasia menjadi beberapa pesan bagian sedemikian sehingga jika seluruh atau sejumlah pesan bagian tersebut dikombinasikan, pesan rahasia asli dapat diperoleh kembali. Beberapa istilah yang digunakan pada skema pembagian data adalah sebagai berikut.

1. *Secret*, yaitu pesan rahasia yang akan dibagi.
2. *Share*, yaitu pesan bagian yang merupakan hasil pembagian dari *secret.*
3. *Dealer*, yaitu pihak yang membagi *secret.*
4. Partisipan, yaitu pihak yang menerima *share*.

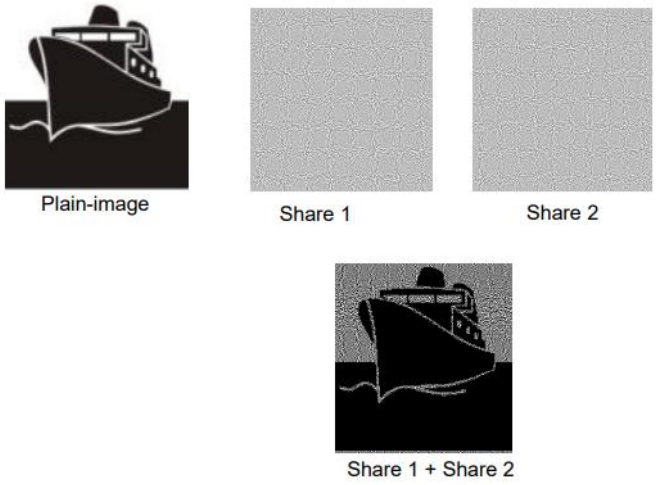
Salah satu contoh skema pembagian data adalah skema ambang Shamir. Skema ini adalah sebuah skema ambang *(threshold scheme)* yang berarti bahwa pesan rahasia M akan dibagi sedemikian rupa sehingga sembarang himpunan bagian dari *share* yang terdiri dari t partisipan dapat merekonstruksi ulang pesan rahasia M, tetapi jika *share* kurang dari t, M tidak dapat direkonstruksi. Proses rekonstruksi ulang dapat dilakukan dengan menggunakan metode interpolasi Lagrange seperti berikut.

$$L_k(x) = \prod_{\substack{i=1 \\ i \neq k}}^{t} \frac{x - x_i}{x_k - x_i}$$

### B. Kriptografi Visual

Kriptografi visual adalah salah satu bentuk skema pembagian data yang dilakukan pada citra. Jenis kriptografi ini akan membagi citra membagi sebuah citra rahasia menjadi

beberapa *share* yang proses dekripsinya dilakukan dengan menumpuk sejumlah *share* dan menerka informasi dari *secret* menggunakan indra penglihatan manusia. *Share* pada kriptografi visual disebut juga dengan *shadow* karena bersifat acak dan tidak bermakna.




**Gambar 1.** Contoh Enkripsi dan Dekripsi Kriptografi Visual

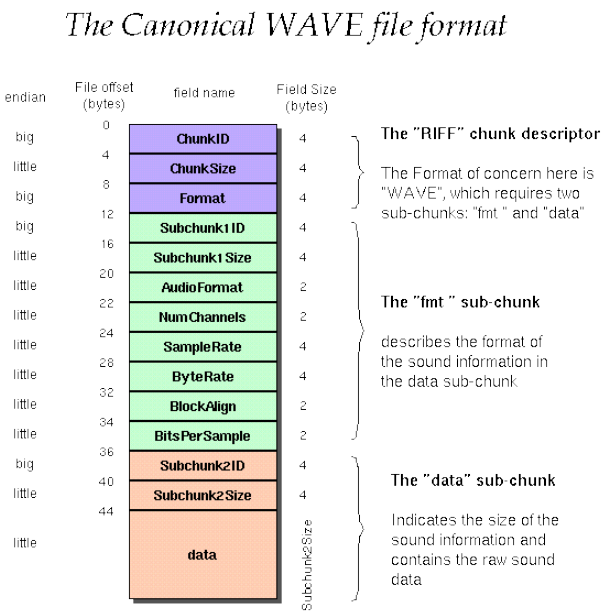
(Sumber: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Visual-Bagian1.pdf)

Dari penjelasan tersebut, dapat dilihat bahwa terdapat beberapa perbedaan antara kriptografi biasa dengan kriptografi visual. Proses enkripsi dan dekripsi kriptografi biasa membutuhkan kunci dan kekuatan komputasi yang tinggi untuk melakukan enkripsi dan dekripsi, sedangkan proses enkripsi dan dekripsi kriptografi visual tidak membutuhkan kunci maupun kekuatan komputasi *(fast decoding). Share* dalam kriptografi visual sudah berperan sebagai kunci.

### *C. Berkas Suara*

Data pada komputer direpresentasikan dalam bentuk *byte.* Satu *byte* terdiri dari delapan buah *bit.* Satu buah *bit* dapat berupa salah sati dari dua buah nilai, yaitu 0 atau 1. Beberapa contoh tipe data yang dapat disimpan di komputer adalah data teks sederhana (.txt), dokumen (.doc, .docx), citra (.jpg, .png), suara (.wav, .mp3, .ogg), animasi (.gif, .apng), dan video (.avi, .mpeg, .mkv). Setiap bentuk data ini direpresentasikan di dalam komputer menggunakan susunan formatnya masing-masing.

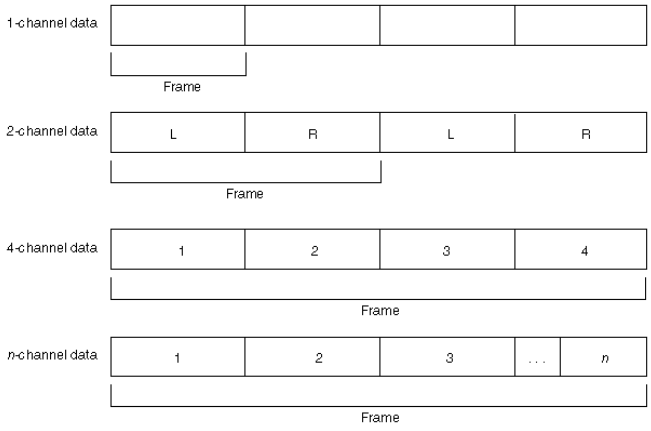
Salah satu format berkas suara yang cukup sering ditemukan adalah format dengan ekstensi .wav. *Waveform Audio File Format (WAV)* adalah format berkas suara yang menggunakan struktur *Resource Interchange File Format (RIFF).* WAV dapat menyimpan data suara yang terkompresi maupun yang tidak terkompresi. Berkas WAV terdiri dari tiga bagian, yaitu *RIFF chunk, format chunk,* dan *data chunk. Header* berkas WAV berisi *metainformation* dari berkas tersebut sebesar 44 *byte.* Isi dari setiap *byte* berkas ini dapat dilihat pada gambar berikut.




**Gambar 2.** Format Berkas WAV

(Sumber: https://www.fatalerrors.org/a/detailed-explanation-of-wav-file-format.html)

Data aktual yang berisi informasi suara disimpan mulai dari *byte* ke-44 sampai akhir berkas. Data tersebut terdiri dari deretan *frame.* Sebuah *frame* memiliki sejumlah *channel* sesuai dengan informasi yang terdapat pada *header* WAV. Jumlah *channel* yang umum digunakan adalah 1 *channel (mono)* dan 2 *channel (stereo).* Setiap *channel* dalam *frame* berisi satu buah angka yang melambangkan amplitudo dari *channel* pada *frame* tersebut. Angka ini dapat berupa angka 8-bit, 16-bit, 24-bit, maupun 32-bit. Khusus untuk 32-bit, angka disimpan dalam format *floating point.*




**Gambar 3.** *Frame* dan *Channel* pada Berkas Suara

(Sumber: https://techpubs.jurassic.nl/manuals/0650/developer/DMSDK_PG/sgi_html/ch08.html)

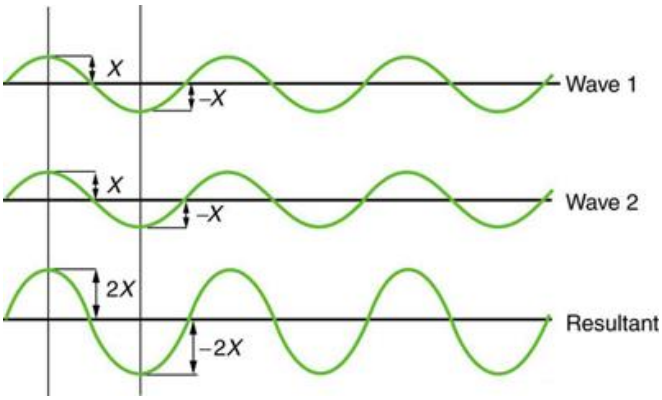
Pemutar berkas WAV akan memutar berkas tersebut sesuai dengan informasi yang terdapat pada *header* berkas. *Samplerate* adalah jumlah *frame* yang diputar setiap detik, sedangkan *channel* adalah titik arah masuk atau keluar suara. Contohnya, berkas WAV dengan *samplerate* 44.100 dua *channel* dapat diputar pada satu *speaker* kiri dan satu *speaker* kanan dengan kecepatan putar 44.100 *frame* per detik pada masing-masing *speaker*.

*D. Interferensi Gelombang*

Karena suara merupakan gelombang, suara juga dapat mengalami fenomena yang disebut dengan interferensi gelombang. Interferensi gelombang terjadi saat minimal dua buah gelombang yang berbeda bertemu. Interferensi gelombang akan menciptakan sebuah gelombang baru yang merupakan penambahan dari semua gelombang yang mengalami interferensi. Terdapat dua jenis interferensi, yaitu:

1. interferensi konstruksi, yaitu interferensi yang terjadi saat dua atau lebih gelombang bertemu dan menghasilkan gelombang dengan amplitudo yang lebih tinggi daripada sebelumnya, dan
2. interferensi destruktif, yaitu interferensi yang terjadi saat dua atau lebih gelombang bertemu dan menghasikan gelombang yang memiliki amplitudo lebih rendah.

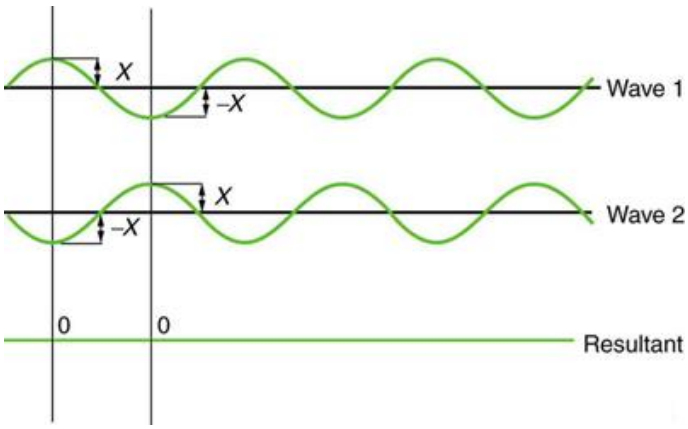
Hampir semua interferensi gelombang yang terjadi adalah campuran dari kedua jenis interferensi tersebut karena gelombang biasanya tidak sama persis. Berikut adalah beberapa contoh penggambaran interferensi pada gelombang.




**Gambar 4.** Interferensi Konstruktif

(Sumber: https://courses.lumenlearning.com/boundless-physics/chapter/interactions-with-sound-waves/)

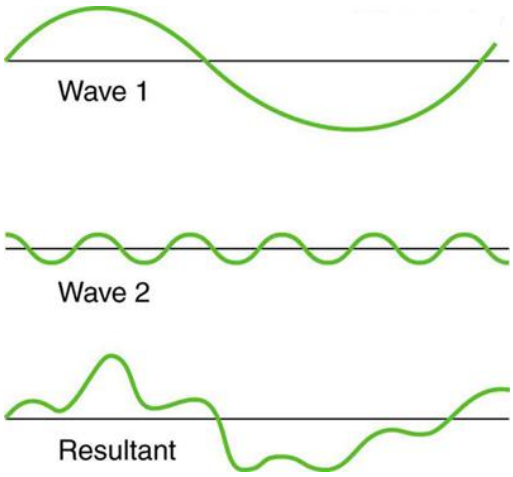
Pada gambar di atas, terjadi interferensi konstruktif sehingga gelombang yang dihasilkan memiliki amplitudo dua kali lipat dari hasil penjumlahan dua gelombang identik.




**Gambar 5.** Interferensi Destruktif

(Sumber: https://courses.lumenlearning.com/boundless-physics/chapter/interactions-with-sound-waves/)

Pada gambar di atas, terjadi interferensi destruktif sehingga gelombang yang dihasilkan memiliki amplitudo nol atau tidak menghasilkan suara sama sekali. Hal ini terjadi karena gelombang satu dan gelombang dua adalah gelombang sinus yang memiliki perbedaan fasa 180 derajat sehingga kedua gelombang meniadakan satu sama lain.




**Gambar 6.** Interferensi Campuran

(Sumber: https://courses.lumenlearning.com/boundless-physics/chapter/interactions-with-sound-waves/)

Pada gambar di atas, terjadi interferensi konstruktif dan destruktif. Hal tersebut terjadi karena kedua gelombang tidak sama persis, sehingga hasil gelombang adalah suara yang baru.

## III. Implementasi

Terdapat tiga buah pendekatan yang digunakan oleh penulis untuk membagi berkas suara menjadi sejumlah *share*, yaitu pembagian sederhana *(simple divide)*, pembagian acak *(random divide)*, dan pembagian interferensi *(interference divide)*.

### A. Simple Divide

Pada pembagian *simple divide*, suara asli dibagi menjadi n buah *share* dalam blok yang berisi m buah *frame* setiap bloknya. Misalnya, suara akan dibagi menjadi 3 buah *share* dengan blok berukuran 500 *frame*, maka *share* pertama akan berisi suara asli pada *frame* 1 – 500, 1.501 – 2.000, dst., *share* kedua akan berisi suara asli pada *frame* 501 – 1.000, 2.000 – 2.500, dst., sementara *share* ketiga akan berisi suara asli pada *frame* 1.001 – 1.500, 2.500 – 3.000, dan seterusnya. *Share* akan hening saat tidak memiliki *frame* dari berkas suara asli.

### B. Random Divide

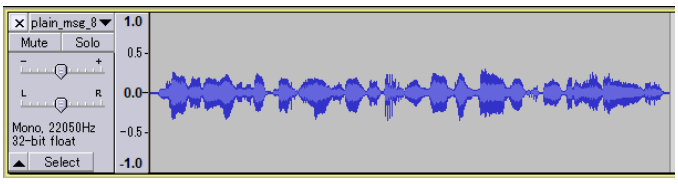
Pada pembagian *random divide*, suara asli dibagi menjadi n buah *share* secara acak. Setiap *channel* dalam setiap *frame* pada berkas suara asli akan diiterasi, dan pada setiap iterasi suara tersebut akan dibagi kepada satu *share* secara acak. *Share* yang tidak mendapat suara asli pada iterasi tersebut akan diberikan amplitudo yang bernilai nol.

### C. Interference Divide

Pada pembagian *interference divide*, suara asli akan dibagi menjadi n buah *share* dengan setiap *share* memiliki amplitudo sebesar m sedemikian sehingga total penjumlahan nilai amplitudo dari semua *share* pada *channel* di *frame* tersebut menghasilkan amplitudo yang sama pada *channel* dan *frame* yang terkait di suara asli. Jenis pembagian ini memanfaatkan sifat interferensi suara yang sudah dijelaskan pada bagian sebelumnya.

## IV. Hasil Pengujian dan Analisis

Pada pengujian, digunakan sebuah berkas WAV yang tidak terkompresi dengan *mono channel* dan ukuran 8-bit per *channel* dalam *frame*. Pemutaran dan penggambaran berkas suara dilakukan menggunakan program Audacity agar suara dapat diputar secara tepat bersamaan. Pranala berkas dan video demonstrasi pengujian disediakan pada bagian lampiran. Berikut visualisasi dari gelombang suara pesan suara asli yang digunakan.

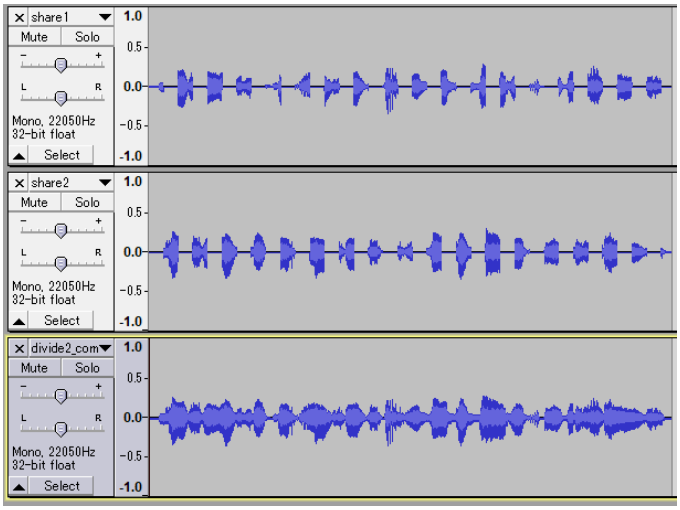



**Gambar 7.** Gambar Gelombang Pesan Suara Asli

(Sumber: dokumen penulis)

### A. Simple Divide

Pada pengujian *simple divide*, suara asli dibagi menjadi 2 buah *share* dan 8 buah *share*. Ukuran blok yang digunakan pada percobaan adalah 2.000 *frame* per blok. Angka tersebut didapat setelah dilakukan beberapa kali percobaan untuk menentukan ukuran yang paling sesuai agar *share* dari berkas contoh sulit dimengerti maknanya. Berikut adalah gambar gelombang *share* dan hasil penggabungannya. Gelombang pertama dan kedua adalah *share*, semetara gelombang ketiga adalah hasil penggabungannya.

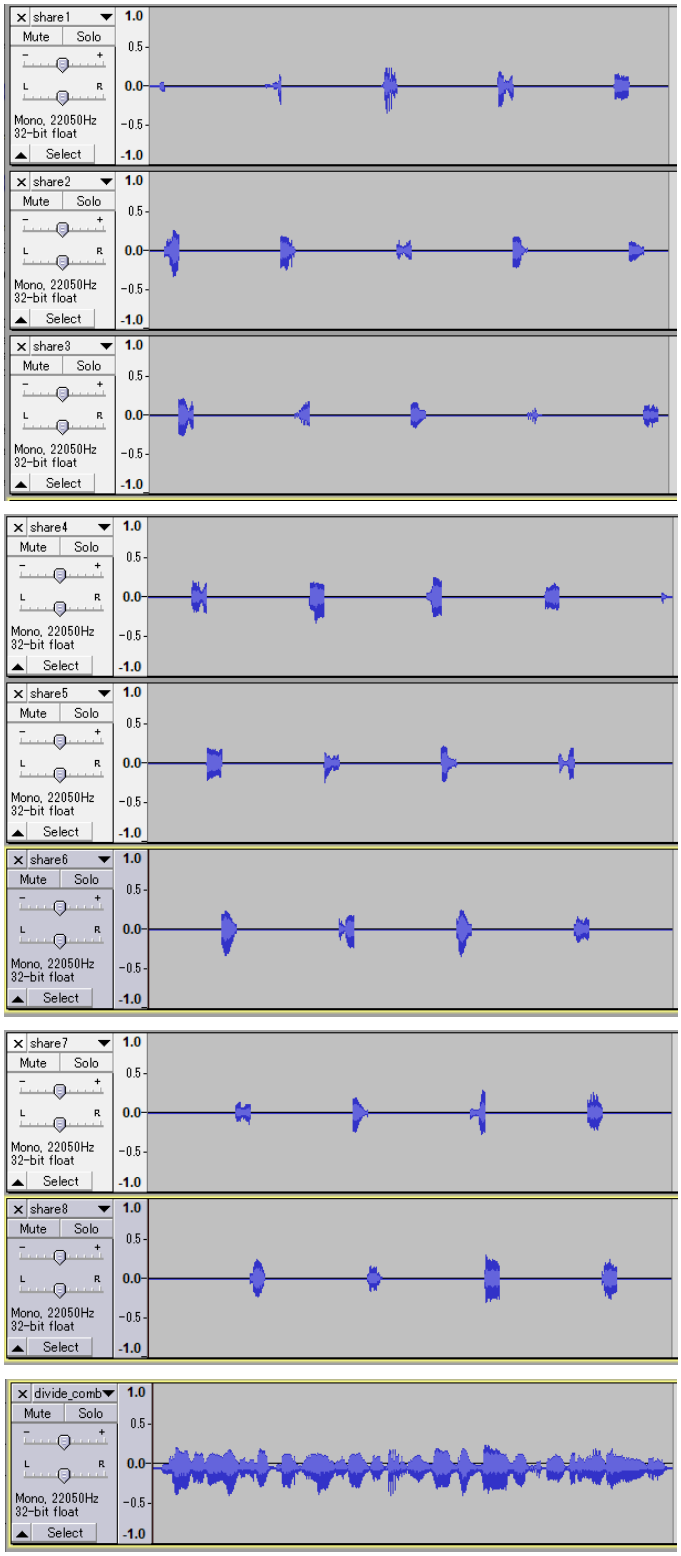



**Gambar 8.** Pengujian *Simple Divide* dengan 2 *Share*

(Sumber: dokumen penulis)

Berikut adalah gambar gelombang dari *share* dan hasil gabungan pada pembagian *simple divide* menjadi 8 buah *share*. Dapat dilihat bahwa lebih banyak bagian yang hening pada setiap *share*. Hal ini terjadi karena skema yang digunakan akan melakukan iterasi pada tiap *share* saat membagi dan memberi bagian pesan suara asli pada *share* tersebut sebesar ukuran blok yang sudah ditentukan sampai iterasi pesan asli selesai. Jadi, potongan suara pesan asli didapatkan dengan hasil memutar bagian *share* pertama, kedua, dan seterusnya lalu kembali dari *share* pertama, kedua, dan seterusnya hingga selesai.

Dari beberapa percobaan yang dilakukan, dapat disimpulkan bahwa kesulitan memahami makna *share* individual ditentukan oleh besar kecilnya ukuran blok dan banyak sedikitnya jumlah *share* yang dihasilkan. Semakin sedikit ukuran blok dan semakin banyak jumlah *share* yang ingin dihasilkan, *share* individu akan semakin sulit dipahami karena *share* hanya mengandung sebagian kecil dari pesan asli.

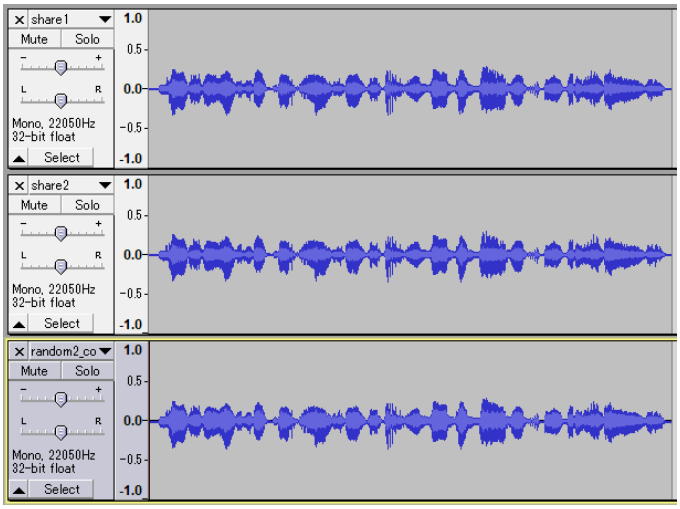



**Gambar 9.** *Share* pada *Simple Divide* dengan 8 Buah *Share* dan Hasil Gabungannya

(Sumber: dokumen penulis)

*B. Random Divide*

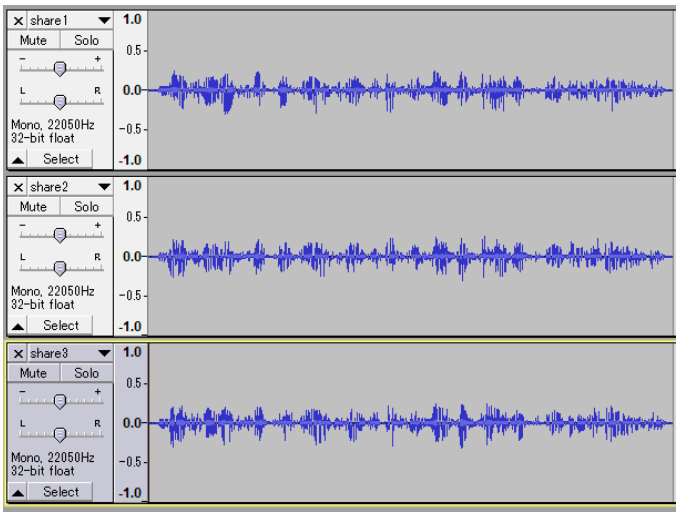
Pada pengujian *random divide*, suara asli dibagi menjadi 2 buah *share* dan 32 buah *share*. Berikut adalah gambar gelombang *share* dan hasil penggabungannya. Gelombang pertama dan kedua adalah *share*, semetara gelombang ketiga adalah hasil penggabungannya.




**Gambar 10.** Pengujian *Random Divide* dengan 2 *Share*

(Sumber: dokumen penulis)

Berikut adalah gambar gelombang dari *share* pertama, kedua, dan ketiga pada pembagian *random divide* menjadi 32 buah *share.*



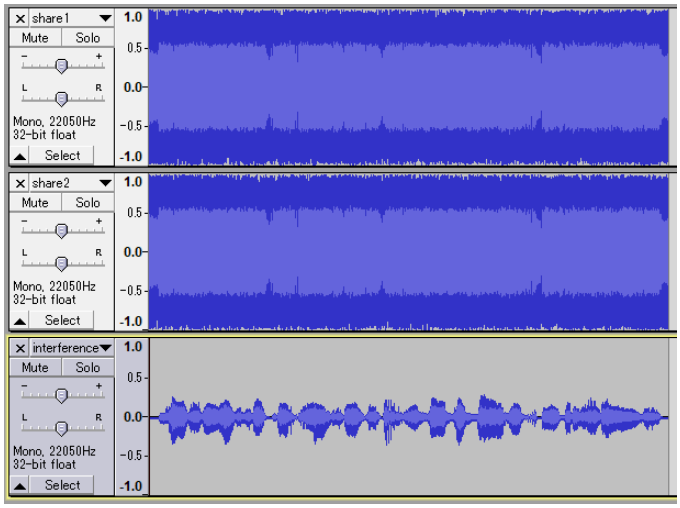

**Gambar 11.** *Share* 1, 2, dan 3 pada *Random Divide* dengan 32 Buah *Share*

(Sumber: dokumen penulis)

Dari gambar tersebut, dapat dilihat bahwa pembagian secara *random divide* tidak menghasilkan bagian kosong seperti pada *simple divide*, sehingga suara asli masih lebih terdengar walaupun lebih sulit dipahami maknanya.

### C. *Interference Divide*

Pada pengujian *interference divide*, suara asli dibagi menjadi 2 buah *share*. Pembagian amplitudo untuk setiap *share* dilakukan dengan menggunakan *random number generator* agar terdistribusi secara acak. Berikut adalah gambar gelombang *share* dan hasil penggabungannya. Gelombang pertama dan kedua adalah *share*, semetara gelombang ketiga adalah hasil penggabungannya.




**Gambar 12.** Pengujian *Interference Divide* dengan 2 *Share*

(Sumber: dokumen penulis)

Dari gambar tersebut, dapat dilihat bahwa *interference divide* adalah skema pembagian yang paling baik dalam menyembunyikan bentuk suara asli pada setiap *share*. Walaupun gelombang terlihat sangat berbeda dari gelombang suara asli, sifat interferensi akan menjumlahkan kedua gelombang tersebut sehingga jika digabungkan akan menghasilkan suara asli yang sama.

### D. *Hasil Analisis*

Dari ketiga cara pembagian *share* berkas suara, yang paling baik dalam merahasiakan *share* adalah *interference divide*, karena walaupun hanya membagi suara menjadi dua buah *share*, *share* tetap sulit dimaknai secara individu. Sementara itu, pembagian *random* untuk jumlah *share* yang sedikit masih menghasilkan *share* yang dapat dimaknai pesannya, begitu juga dengan *simple divide* yang sangat bergantung pada jumlah *share* dan ukuran blok. Selain itu, pada pembagian *simple divide* dan *random divide*, suara asli dapat diterka maknanya walau tidak sempuran dengan sebagian saja dari jumlah *share*.

## V. KESIMPULAN

Seperti pada kriptografi visual, pembagian data berkas suara dapat dilakukan sedemikian rupa sehingga proses dekripsinya cukup dilakukan dengan memutar sejumlah *share* suara pada waktu yang tepat bersamaan. Dari ketiga skema pembagian *share* yang diajukan oleh penulis, cara pembagian yang paling baik adalah *interference divide* yang membagi *share* dengan memanfaatkan sifat interferensi gelombang pada gelombang suara. Skema tersebut dianggap yang terbaik karena tidak perlu membagi pesan suara asli menjadi banyak *share* untuk membuat makna dari *share* individu sulit dipahami. Pembagian *share* dengan *simple divide* dan *random divide* yang diajukan akan semakin baik seiring dengan bertambahnya jumlah *share* dan ukuran blok.

## PRANALA BERKAS PENGUJIAN

https://drive.google.com/drive/folders/1lUKjHo_XesP9GaUvr085coCDjHwBKcKx?usp=sharing

## PRANALA VIDEO YOUTUBE

https://youtu.be/3hEMhblvE4I

## UCAPAN TERIMA KASIH

Pertama-tama, penulis ingin mengucapkan syukur kepada Tuhan Yang Maha Esa karena atas berkat-Nya penulis dapat mengikuti mata kuliah IF4020 Kriptografi ini dari awal hingga selesainya dibuat makalah ini. Penulis juga hendak berterima kasih kepada Bapak Rinaldi Munir selaku dosen pengampu mata kuliah terkait atas bimbingan yang telah diberikan beliau. Terakhir, penulis juga berterima kasih kepada seluruh keluarga dan teman-teman penulis yang telah memberi dukungan selama pengerjaan makalah ini.

## REFERENSI

[1] Munir, Rinaldi. "Pengantar Kriptografi," https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2021-2022/Pengantar-Kriptografi-(2021).pdf. Diakses 20 Desember 2021 04.07 WIB.

[2] Munir, Rinaldi. "Skema Pembagian Data Rahasia," https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2017-2018/Skema-Pembagian-Data-Rahasia-(2018).pdf. Diakses 20 Desember 2021 04.10 WIB.

[3] Munir, Rinaldi. "Kriptografi Visual, Teori dan Aplikasinya," https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/Kriptografi-Visual-Bagian1.pdf. Diakses 20 Desember 2021 04.12 WIB.

[4] Godspeedxiao. "Detailed Explanation of WAV File Format," https://www.fatalerrors.org/a/detailed-explanation-of-wav-file-format.html. Diakses 20 Desember 2021 08.15 WIB.

[5] Sound Devices. "32-Bit Float Files Explained," https://www.sounddevices.com/32-bit-float-files-explained/. Diakses pada 20 Desember 2021 08.42 WIB.

[6] Wildlife Acoustics. "What Is An Audio Channel?" https://www.wildlifeacoustics.com/resources/faqs/what-is-an-audio-channel. Diakses 20 Desember 2021 08.50 WIB.

[7] Lumen. “Interactions with Sound Waves,” https://courses.lumen learning.com/boundless-physics/chapter/interactions-with-sound-waves/. Diakses 20 Desember 2021 09.13 WIB.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 20 Desember 2021

Melita 13519063