



Pendeteksian sinyal DTMF pada domain frekuensi di atas standar untuk pengiriman informasi penting menggunakan metode enkripsi Caesar Cipher

Mohammad Farid Susanto^{1*}, Yoga Budi Permana Putra², Danil Pramudya³

^{1,2,3}Jurusan Teknik Elektro, Politeknik Negeri Bandung

Jl. Gegerkalong Hilir, Ciwaruga, Kabupaten Bandung Barat, Jawa Barat 40559, Indonesia

^{1*}mfarids@polban.ac.id, ²yoga.budi.tkom418@polban.ac.id, ³danil.pramudya.tkom419@polban.ac.id

ABSTRAK

Pesan rahasia merupakan pesan penting yang ditujukan khusus kepada pihak-pihak tertentu, diantaranya pengirim dan penerima sebagai pihak yang berwenang. Dikarenakan pesan itu sangat rahasia, maka informasi tersebut harus dienkripsi terlebih dahulu. Untuk mengetahui isi informasi tersebut diperlukan peran kriptanalis yang ingin mengetahui isi pesan rahasia tersebut. Pesan rahasia pada prinsipnya dapat disadap pada saat proses pengiriman informasi. Untuk itu kriptanalis mencari cara untuk mendapatkan informasi rahasia tersebut, sehingga diperlukan suatu sistem pengamanan. Pada penelitian ini akan digunakan metode dengan cara mengirimkan kode pesan rahasia berupa audio yang dienkripsi dengan Caesar Cipher dan dicampurkan dengan musik sebagai audio pembawa. Kode ini memanfaatkan sinyal DTMF (*Dual Tone Multi Frequency*) di atas standar DTMF yang berisi pesan rahasia terenkripsi. DTMF di atas standar ini dilakukan dengan tiga formula frekuensi kerja baris dan kolom yang digunakan sebagai formula kunci. Hasil penelitian ini menunjukkan pesan rahasia yang memanfaatkan DTMF di atas standar bisa mengirimkan informasi rahasia tersebut dengan tingkat akurasi pesan 96% dan pesan yang ada dalam audio tidak terdengar oleh pendengar.

Kata kunci: enkripsi, Caesar Cipher, DTMF di atas standar, audio pembawa, kriptanalis

ABSTRACT

Confidential messages are important messages that are specifically addressed to certain parties, including the sender and recipient as authorized parties. Because the message is highly confidential, the information must be encrypted first. To find out the contents of this information, the role of a cryptanalyst is needed who wants to know the contents of the secret message. Secret messages can in principle be intercepted during the process of sending information. For this reason, cryptanalysts are looking for ways to obtain this confidential information, so a security system is needed. In this study a method will be used by sending a secret message code in the form of audio encrypted with Caesar Cipher and mixed with music as the audio carrier. This code utilizes a DTMF (Dual Tone Multi Frequency) signal over the DTMF standard which contains an encrypted secret message. DTMF above this standard is carried out with three row and column working frequency formulas which are used as key formulas. The results of this study indicate that secret messages that utilize DTMF above the standard can send confidential information with a message accuracy rate of 96% and the messages contained in the audio are not heard by listeners.

Keywords: encryption, Caesar Cipher, DTMF custom, audio carrier, cryptanalysis

1. PENDAHULUAN

Saat ini, informasi digital dengan mudah diakses melalui internet. Kemudahan dan efisiensi jaringan komputer global untuk komunikasi informasi dan data digital telah mempercepat popularitas media digital, sehingga dengan sangat rentan dilakukan penyadapan pada informasi yang akan dikirimkan [1]. Dalam menjaga keamanan dan kerahasiaan data yang kita miliki, dapat dilakukan langkah preventif apabila terdapat orang yang ingin merusak data tersebut.

Berbagai penelitian telah dilakukan untuk mengatasi permasalahan terkait dengan keamanan dan kerahasiaan data menggunakan musik sebagai media untuk menyembunyikan pesan tersebut. Penelitian yang telah dilakukan sebelumnya yaitu menyisipkan pesan teks melalui audio dengan

enkripsi *Least Significant Bit* (LSB) [2]. Prototipe yang dibuat yaitu menghasilkan sebuah aplikasi yang bisa untuk mengekstraksi pesan yang sudah diberikan audio. Pada penelitian [3] melakukan penelitian terkait dengan proteksi pesan audio dengan implementasi metode enkripsinya yaitu menggunakan *Advanced Encryption Standard* (AES). Penelitian ini memiliki sistem yang dapat memproteksi pesan audio menggunakan metode AES agar dapat diperoleh hasil enkripsi berupa pesan audio yang dapat diputar menjadi pesan audio yang tidak dapat diputar dengan ukuran pesan audio hasil enkripsi lebih besar dari pesan audio sebenarnya dan dapat mengurangi kecurigaan dari pihak lain karena pesan audio yang belum dienkripsi dengan yang sudah dienkripsi formatnya sama. Berdasarkan permasalahan tersebut dan penelitian yang sudah ada, maka dibuatkannya suatu alat untuk mengamankan pesan rahasia yang tidak mencurigakan, relatif mudah, dan aman digunakan pada media komunikasi umum ataupun khusus [4], [5].

Mengacu pada standar rekomendasi ITU-T Q.23, standar yang digunakan pada perangkat telepon tetap atau bergerak menggunakan teknologi DTMF yaitu teknik untuk mentransmisikan digit yang membentuk nomor telepon yang dikodekan dengan 2 nada yang dipilih dari 8 frekuensi yang telah ditentukan sebelumnya [6]. Ke-8 frekuensi tersebut terdiri dari sisi baris 697 Hz, 770 Hz, 852 Hz, 941 Hz, pada sisi kolom 1209 Hz, 1336 Hz, 1477 Hz, dan 1633 Hz, seperti yang ditunjukkan pada Gambar 1. Untuk menekan nomor 1 maka frekuensi yang dikodekan yaitu 697 Hz dan 1209 Hz, jika pada nomor 9 dikodekan dengan 852 Hz dan 1477 Hz, demikian juga pada angka selanjutnya [7].

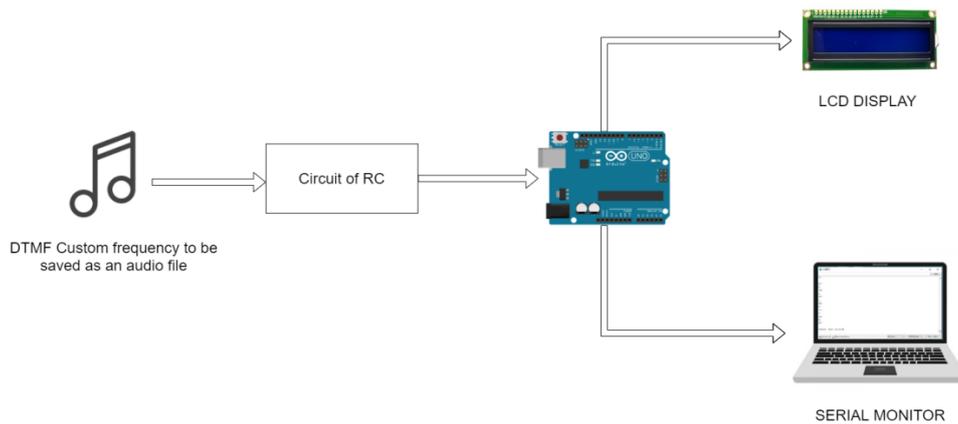
Hz	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C
941	*	0	#	D

Gambar 1. Kombinasi nada DTMF Standar [8]

Maka dari itu dikembangkan sinyal untuk kebutuhan khusus yang dinamakan DTMF di atas standar. DTMF di atas standar yaitu sinyal yang dibangkitkan di luar frekuensi standar, bisa di atas atau di bawah dari frekuensi standar. Pengembangan DTMF di atas standar sangat penting untuk keperluan sinyal *watermarking* yang digunakan di berbagai kebutuhan sinyal informasi, sebagai tanda kepemilikan juga pesan rahasia. Untuk keperluan yang lain pada kebutuhan sinyal DTMF di atas standar sebagai *watermarking*. *Watermarking* sendiri terdiri dari dua jenis, yaitu *visible watermarks* dan *invisible watermarks*. *Visible watermarking* adalah penanda yang terlihat pada dokumen teks, gambar, dan video, sedangkan pada audio terdengar dan menunjukkan kepemilikan [9]. Sedangkan *invisible watermarking* adalah penanda yang tidak terlihat pada dokumen teks, gambar, dan video, sedangkan pada audio tidak terdengar yang mengindikasikan kepemilikan juga [10]. Pada penelitian [11] membuat sebuah aplikasi pengamanan dokumen PDF ini dirancang agar dapat membantu *user* dalam mengamankan data menggunakan teknik *watermarking* yang dapat membantu menunjukkan suatu hak cipta bahwa dokumen yang diunggah adalah milik yang bersangkutan. Penelitian ini berfokus pada pembuatan sistem pengiriman pesan rahasia pada frekuensi DTMF di atas standar yang dicampur dengan audio pembawa yang kemudian mencari spektrum frekuensi yang optimal yang dapat diterima oleh sistem dekoder DTMF di atas standar.

2. METODE PENELITIAN

Metode yang diusulkan adalah pengamanan pesan rahasia dengan metode *invisible watermarking*. Pembuatan keamanan ini memiliki empat tahapan yang masing-masing memiliki peran yang sangat penting dalam keamanan pesan. Berikut proses untuk pengamanan pesan rahasia yang digambarkan dalam proses enkripsi dan dekripsi. Gambar 2 merupakan ilustrasi dari prototipe sistem.



Gambar 2. Ilustrasi pada sistem prototipe

2.1 Proses Enkripsi *Plainteks* ke Dalam Kode ASCII

Enkripsi ini menggunakan metode Caesar Cipher dengan menggunakan indeks ASCII. Enkripsi Caesar Cipher termasuk enkripsi substitusi yang artinya setiap huruf diganti dengan catatan yang sesuai dengan kunci [12]. Cara kerja kunci ini adalah dengan mengganti atau menggeser setiap huruf dalam kalimat pesan dengan urutan huruf yang diinginkan. Jumlah nilai dari kunci ini untuk mengubah urutan huruf disebut kunci untuk proses enkripsi dan dekripsi [13]. Proses penggunaan kode ini dilakukan pada tahap *encoding* dan *decoding* yang dibentuk oleh persamaan-persamaan berikut [14].

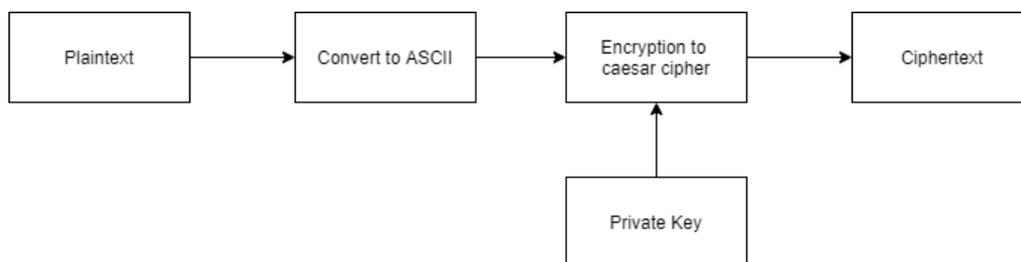
Persamaan enkripsi

$$(Cx) = (Px) + (k) \text{ mod } 26 \quad (1)$$

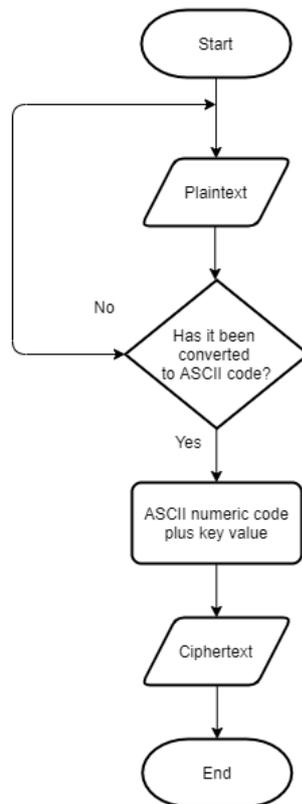
Persamaan dekripsi

$$(Px) = (Cx) - (k) \text{ mod } 26 \quad (2)$$

dimana C adalah *ciphertext*, P adalah *plaintext*, dan K adalah nilai kunci yang digunakan untuk mengganti setiap karakter. Ada beberapa variasi dari algoritma enkripsi Caesar Cipher, salah satunya mengubah modulus yang digunakan dari 26 menjadi 256 sehingga dapat digunakan pada karakter ASCII apapun [15]. Gambar 3 merupakan diagram blok dari proses enkripsi, sedangkan secara diagram alir ditunjukkan pada Gambar 4. Dalam prosesnya, *plaintexts* diinput menggunakan format huruf kapital sehingga format angka desimal dalam ASCII adalah 2 digit per huruf. Kemudian huruf-huruf tersebut dikonversi menjadi angka desimal dalam indeks ASCII dengan menggunakan fungsi "ord()" pada Python. Setelah itu, angka desimal ASCII tersebut dijumlahkan dengan kunci yang telah diinputkan oleh *user* sebagai *sliding key* dari metode Caesar Cipher.



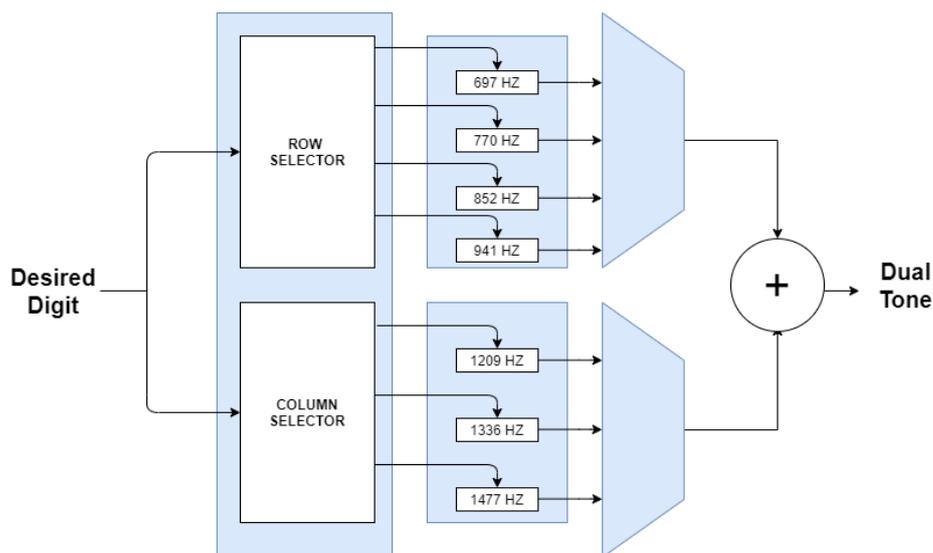
Gambar 3. Blok diagram proses enkripsi



Gambar 4. Diagram alir proses enkripsi

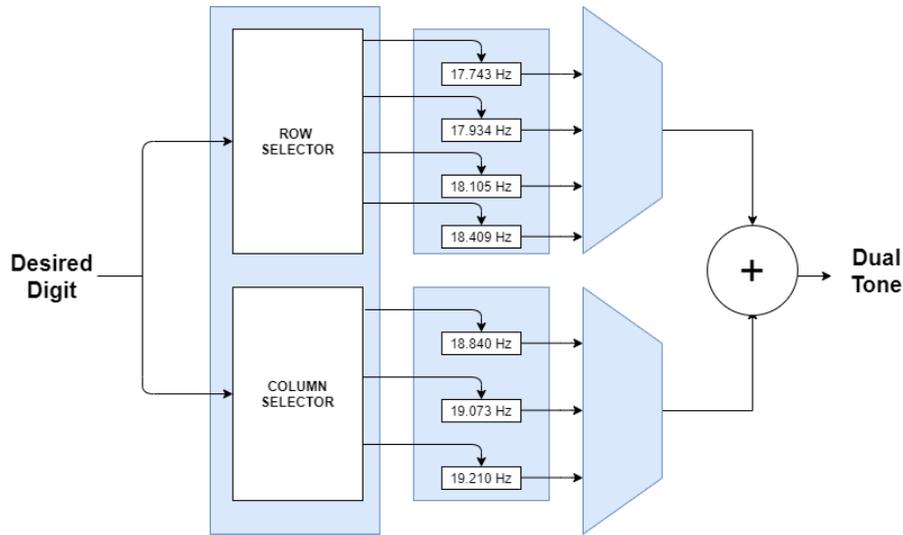
2.2 Proses Encoding pada DTMF di Atas Standar

Proses ini merupakan konversi dari digit yang dienkripsi menjadi sinyal DTMF di atas standar. DTMF di atas standar ini memiliki frekuensi 15000 Hz - 19000 Hz sehingga hanya gema yang terdengar dalam pendengaran manusia. Generator DTMF di atas standar merupakan generator sinyal DTMF yang nilai frekuensi baris dan kolomnya tidak sesuai dengan nilai standar DTMF seperti yang ditunjukkan pada diagram blok generator pada Gambar 5.



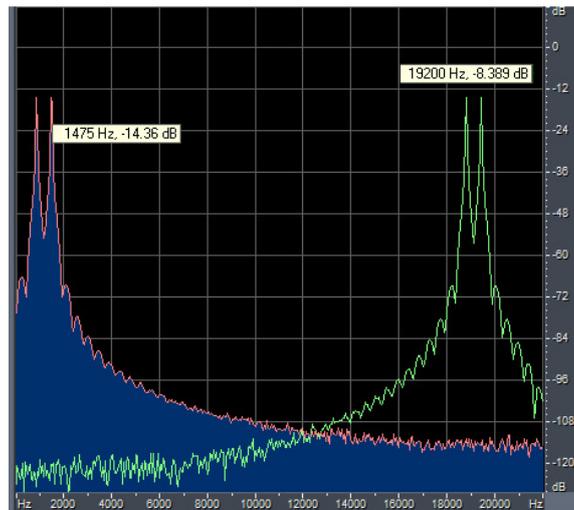
Gambar 5. Blok diagram pembentukan DTMF standar

Gambar 5 menjelaskan blok diagram terkait penginputan dalam pembentukan frekuensi DTMF standar. Maka akan dilihat perbedaan frekuensi dengan DTMF di atas standar pada Gambar 6.



Gambar 6. Blok diagram pembentukan DTMF di atas standar

Berdasarkan perbedaan frekuensi pada DTMF standar dan juga DTMF di atas standar, maka bisa dilihat perbandingan dari perbedaan antara kedua spektrum DTMF tersebut pada Gambar 7.



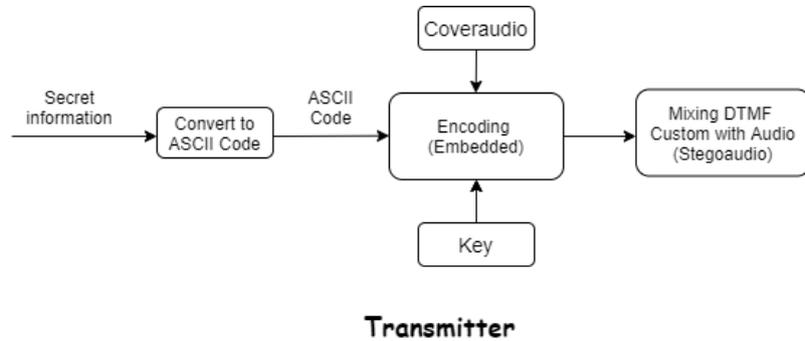
Gambar 7. Perbandingan spektrum pada frekuensi DTMF di atas standar dan standar

Menurut *International Telecommunication Union – Telegraphy* (ITU-T) rekomendasi Q.23 yang direkayasa pada frekuensi yang dihasilkan dapat dirancang sesuai kebutuhan diluar generator DTMF di atas standar. Dalam hal ini direncanakan dalam penelitian seperti pada Tabel 1.

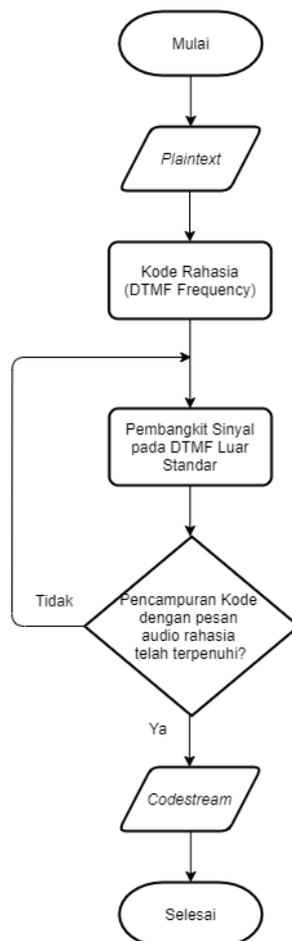
Table 1. Frekuensi DTMF di atas standar

Frekuensi (Hz)	18.840	19.073	19.210	19.480
17.743	1	2	3	A
17.934	4	5	6	B
18.105	7	8	9	C
18.409	*	0	#	D

Penerima dekoder DTMF di atas standar adalah DTMF yang frekuensi kerjanya di atas standar rekomendasi ITU-T Q.23, seperti yang ditunjukkan pada Tabel 1. Frekuensi kerja dekoder menyesuaikan frekuensi generator DTMF di atas standar. Hasil pembangkitan ini digunakan sebagai kriptografi untuk proses pengirim memberikan informasi kepada penerima maka akan digambarkan prosesnya pada Gambar 8. Pada proses pengirim akan digambarkan alur dari pengiriman pesan yang akan disampaikan pada penerima yaitu pada Gambar 9.

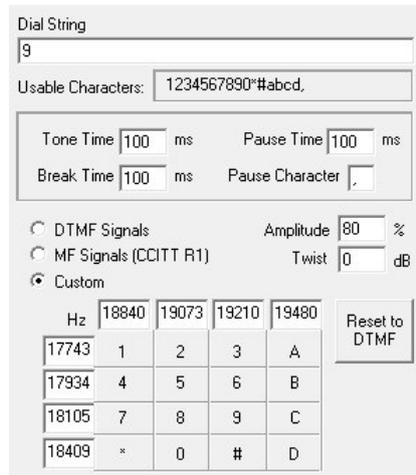


Gambar. 8 Blok diagram proses *encoding* (sisi pengirim) DTMF di atas standar



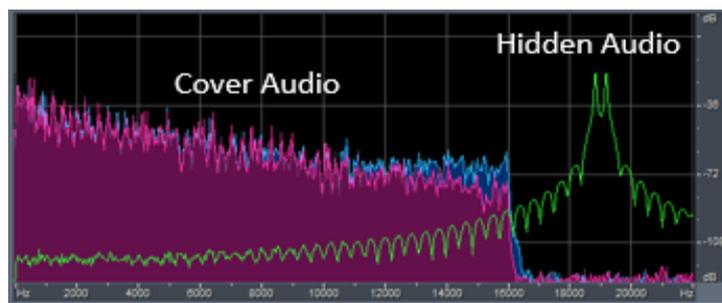
Gambar 9. Diagram alir proses *encoding* (sisi pengirim) DTMF di atas standar

Gambar 10 menunjukkan DTMF di atas standar yang diberi *string* angka *dial* diberi *tone time* 100 ms dan juga *break time* 100 ms untuk frekuensi berada di 18.840 -19.480 Hz.



Gambar 10. Generate sinyal frekuensi DTMF di atas standar

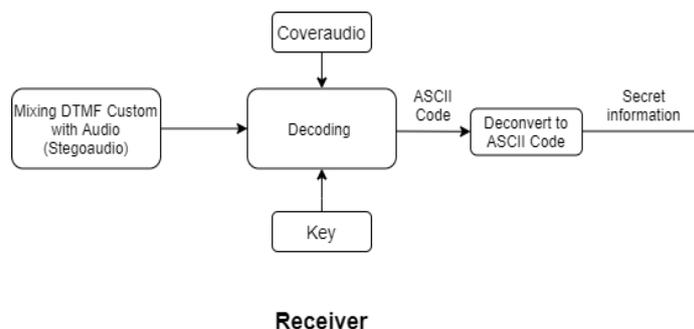
Urutan nomor terenkripsi dimasukkan menggunakan fitur DTMF *generate*. Kemudian setelah menghasilkan sinyal Caesar Cipher DTMF di atas standar dicampur dengan audio dan menghasilkan gambar sinyal seperti pada Gambar 11. Sinyal ini dapat ditransmisikan menggunakan saluran komunikasi arus utama.



Gambar 11. Menampilkan spektrum audio dari frekuensi 200 - 16.000 Hz saat berada dalam spektrum audio tersembunyi dari frekuensi 18.840 Hz dan 19.210 Hz

2.3 Memproses Pengkodean dan Pesan Enkripsi

Dalam proses ini adalah proses mencampurkan sinyal DTMF di atas standar yang berisikan Caesar Cipher telah dimasukkan ke dalam audio menjadi sebuah pesan rahasia lalu masuk ke tahapan dekoding yang sudah berisi *coveraudio* yaitu Teknik menyembunyikan sebuah pesan melalui musik sebagai pembawanya lalu pada proses dekoding ini juga terdapat key yang berisikan kunci dari pesan rahasia tersebut yaitu *caesar cipher*, lalu di dekonversi menggunakan ASCII kode dan di terima oleh LCD Display sebagai output untuk melihat isi pesan rahasia tersebut. Proses ini dilakukan dengan menggunakan mikrokontroler Arduino Uno sebagai dekoder untuk bisa mendeteksi pesan rahasia tersebut.



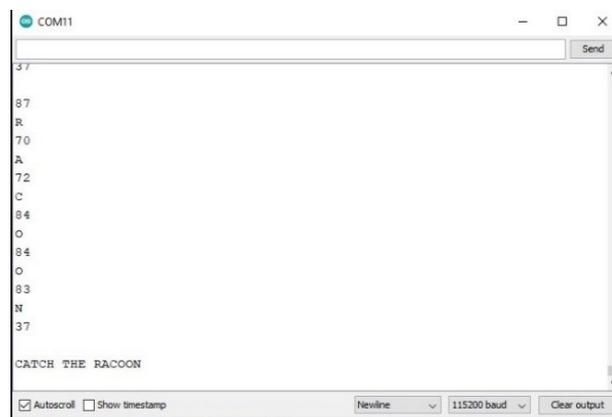
Gambar 12. Diagram blok *decoding* DTMF di atas standar penerima

Dalam proses dekoding, alat dekoder mendeteksi sinyal dengan DTMF yang menggunakan frekuensi tinggi sesuai dengan pengaturan pada mikrokontroler Arduino. Frekuensi yang digunakan adalah kisaran 15000 Hz - 19000 Hz. Hasil dari deteksi ini adalah berupa serangkaian angka. Kemudian urutan angka ini dipisahkan menjadi dua digit setelah itu dilakukan pengurangan sesuai dengan kunci dalam enkripsi. Setelah itu konversi dilakukan dari bentuk angka desimal dua digit menjadi huruf sesuai dengan indeks ASCII sehingga pesan akan ditampilkan melalui LCD.



Gambar 13. Tampilan pesan pada layar LCD

Pesan akan dipantau melalui *serial monitor* pada *software* Arduino Uno sehingga hasilnya dapat dilihat pada Gambar 14.



Gambar 14. Isi pesan pada serial Monitor Arduino Uno

3. HASIL DAN PEMBAHASAN

Berikut ini adalah hasil pengujian *tone time* dan *break time* untuk menemukan spesifikasi terbaik untuk dimainkan melalui ponsel yang dapat dideteksi, diterjemahkan, dan didekripsi dengan baik menggunakan detektor. Gambar 15 adalah diagram blok dan ilustrasi untuk pengujian.



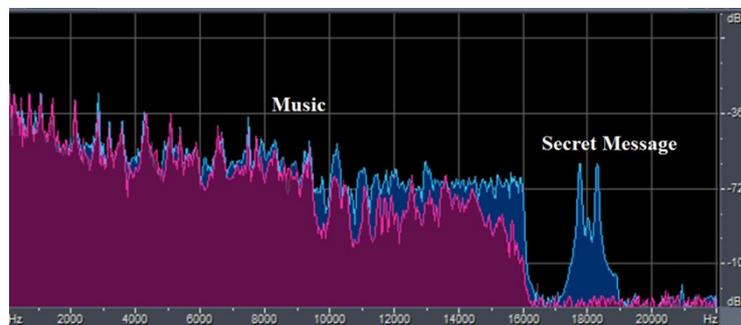
Gambar 15. Ilustrasi pengujian

3.1 Menguji *Tone Time* dan *Break Time*

Pengujian ini dilakukan dengan menghasilkan "CATCH THE RACOON" sinyal pesan dienkripsi ke dalam urutan angka "7270897277378977743787707284848337" yang kemudian diterjemahkan menggunakan DTMF di atas standar. Dalam pengujian *tone time*, sinyal ini dihasilkan dengan mengubah nilai *tone time* dan nilai *tone time* ditetapkan pada 1.500 ms dalam menghasilkan DTMF. Fitur sinyal dalam tes *break time* dalam kode sandi diubah sedangkan satu kali menggunakan 250 ms. Kemudian sinyal dicampur menggunakan musik yang mengandung audio dengan vokal. Dalam musik, amplitudo puncak diatur mendekati -9 dB. File audio disimpan di .wav format untuk pengujian tanpa audio dan .mp3 untuk pengujian dengan pencampuran audio. Selanjutnya, pesan dikirim melalui media komunikasi Whatsapp yang digunakan sebagai media untuk menerima musik yang berisikan pesan rahasia untuk bisa diterima oleh dekoder DTMF.

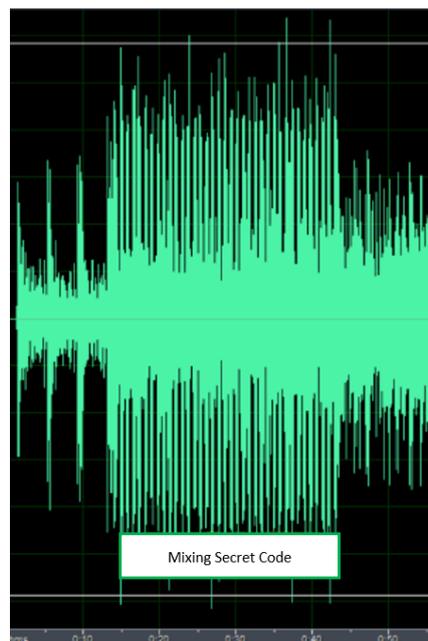
3.2 Spesifikasi Audio

Spesifikasi audio yang digunakan menggunakan salah satu musik yang akan diuji sehingga spektrum dari musik tersebut dapat terlihat dan spektrum dari sinyal informasi rahasia yang berisikan kode Caesar Cipher sudah terlihat dengan jelas model dari spektrum informasinya. Bentuk gelombang yang dihasilkan dapat dilihat pada Gambar 16.



Gambar 16. Bentuk gelombang hasil salah satu musik digunakan dan juga dengan pesan rahasia

Untuk hasil dari spektrum musik dengan spektrum informasi rahasia melalui proses yaitu proses pencampuran antara kedua spektrum tersebut bisa dilihat pada Gambar 17.



Gambar 17. Kode rahasia pencampuran sinyal DTMF

3.3 Hasil Pengujian

Pada hasil tes ini akan menampilkan pengujian *tone time* dan juga *break time* sehingga data yang didapat dalam pengujian ini akan terangkum dalam tabel serta grafik yang tersedia untuk proses perbandingan. Pada pengujian *tone time* ini dilakukan dengan range 10 – 5000 ms untuk bisa membaca *output* pada pesan yang sudah dibaca dan juga presentase tingkat keberhasilannya terlihat pada Tabel 2. Pada pengujian *break time* dengan range 10 – 5000 ms untuk bisa membaca *output* pada pesan yang sudah dibaca dan juga presentase tingkat keberhasilannya terlihat pada Tabel 3.

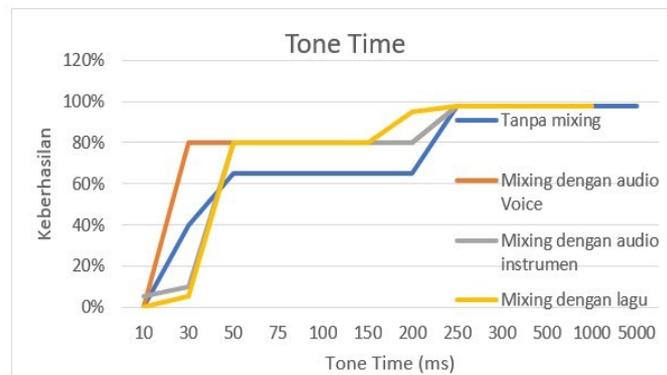
Tabel 2 Hasil pengujian *tone time*

<i>Tone time</i> (ms)	<i>Output</i>	Deskripsi	Keberhasilan (%)
10	Unreadable	<i>Not read by decoder if played through a cell phone</i>	0
30	H0CH THEIH? 'NO	<i>can be detected, only the word "THE"</i>	15
50	CATCH THE RACOS?	<i>The last 3 letters are unreadable</i>	65
75	CATCH THE RACOS?	<i>The last 3 letters are unreadable</i>	65
100	CATCH THE RACOS?	<i>The last 3 letters are unreadable</i>	65
150	CATCH THE RACOS?	<i>The last 3 letters are unreadable</i>	65
200	CATCH THE RACOS?	<i>The last 3 letters are unreadable</i>	65
250	CATCH THE RACOOON	<i>the entire message is read</i>	98
300	CATCH THE RACOOON	<i>the entire message is read</i>	98
500	CATCH THE RACOOON	<i>the entire message is read</i>	98
1000	CATCH THE RACOOON	<i>the entire message is read</i>	98
5000	CATCH THE RACOOON	<i>the entire message is read</i>	98

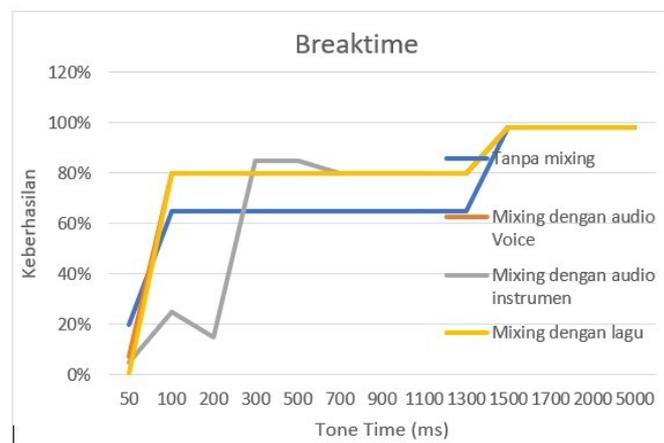
Tabel 3. Hasil pengujian *break time*

<i>Break time</i> (ms)	<i>Output</i>	Deskripsi	Keberhasilan (%)
10		<i>Not detected</i>	0
20		<i>Not detected</i>	0
30	00?	<i>detected but no message</i>	10
50	↑TCDIHE RHO+N	<i>3 final letters unreadable, 2 letters misread</i>	80
100	CATCH THE RACOR	<i>3 final letters unreadable, 2 letters misread</i>	80
200	CATCH THE RACON	<i>3 final letters unreadable, 2 letters misread</i>	80
300	CATCH THE RACON	<i>3 final letters unreadable, 2 letters misread</i>	80
500	CATCH THE RACON	<i>3 final letters unreadable, 2 letters misread</i>	80
700	CATCH THE RACOS?	<i>3 final letters unreadable, 2 letters misread</i>	80
900	CATCH THE RACOS?	<i>3 final letters unreadable, 2 letters misread</i>	80
1100	CATCH THE RACOS?	<i>3 final letters unreadable, 2 letters misread</i>	80
1300	CATCH THE RACOS?	<i>3 final letters unreadable, 2 letters misread</i>	80
1500	CATCH THE RACOOON	<i>the entire message is read</i>	98
1700	CATCH THE RACOOON	<i>the entire message is read</i>	98
2000	CATCH THE RACOOON	<i>the entire message is read</i>	98
5000	CATCH THE RACOOON	<i>the entire message is read</i>	98

Berdasarkan hasil pengujian *tone time* dapat dilihat bahwa pada range *tone time* 250 – 5000 ms akurasi keberhasilannya 98% menunjukkan hasil sempurna dikarenakan outputnya sudah terbaca dengan jelas sehingga bisa didapatkan respon dari grafik pada *tone time* di berbagai kondisi pada Gambar 18. Adapun grafik respon dari *break time* diberbagai kondisi terlihat bahwa hasilnya pada Gambar 19.



Gambar 18. Hasil tes *tone time* dalam berbagai kondisi



Gambar 19. Hasil tes *break time* dalam berbagai kondisi

Pada pengujian *tone time* dapat dilihat bahwa nilai *tone time* dari 30 ms hingga 200 ms sedangkan pada pengujian *break time* 700 ms hingga 1300 ms dapat mendeteksi dan mendekripsi pesan dengan baik jika jumlah digit kurang dari 28 huruf. Hal ini karena 1 digit huruf memiliki 8 bit. Pada alat Dekoder ini, membutuhkan *delay* jika jumlah *password* lebih dari 28 digit huruf karena pekerjaan dari *tool* ini adalah program dapat berjalan ketika ada sinyal DTMF yang masuk. Penundaan ini harus disesuaikan dengan *break time* dan *tone time* yang optimal agar tidak terjadi kesalahan terjemahan. Sehingga *tone time* dengan nilai 300 ms dan *break time* 1600 ms dapat membantu alat dekoder melakukan dekoding, dekripsi, dan penerjemahan dengan baik karena dapat memberikan *delay* pada *tools* untuk menyelesaikan proses dengan baik lalu mendeteksi sinyal DTMF kembali.

4. KESIMPULAN

Sistem dekoder DTMF di atas standar berhasil memecahkan kode dengan tingkat akurasi 98% menggunakan *tone time* dan *break time* optimal 250 ms untuk satu kali dan 1500 ms untuk *break time* meskipun ditumpangkan pada suara, instrumen, dan audio musik vokal. Dengan hasil percobaan tersebut bahwa informasi rahasia yang dikirim tidak terdengar namun demikian bila terdengar informasi tersebut tidak dapat dipahami sehingga dapat digunakan untuk mengirim informasi rahasia dengan metode enkripsi simetris klasik ataupun modern.

REFERENSI

- [1] F. Y. Shih, "Introduction" in *Digital Watermarking and Steganography*, Eds. Fundamentals and Techniques, Taylor and Francis Group, Broken Sound Parkway NW, pp. 1-7, 2017.
- [2] I. G. A. M. A. Jayantia, I. G. N. A. C. Putraa, I. M. Widiartha, A. A. I. N. E. Karyawatia, I. Suhartanaa, and N. A. S. Era, "Pengamanan Audio Rindik Bali Menggunakan Metode Least Significant Bit Berbasis Android," *Jurnal Elektronik Ilmu Komputer Udayana*, vol. 11, no. 2, 2022.
- [3] M. Sihombing, J. N. Sitompul, and T. A. Putri, "Implementasi Metode Kriptografi Advanced Encryption Standard (AES) untuk Proteksi Pesan Audio," *MEANS*, vol. 4, no. 1, pp. 37-45, 2019.
- [4] M. F. Susanto, "Studi Pengembangan Sinyal Dtmf Diatas Standar Digunakan Untuk Sinyal Watermarking," *Prosiding-Seminar Nasional Teknik Elektro UIN Sunan Gunung Djati Bandung*, 2020, pp. 287-298.
- [5] M. F. Susanto, D. N. A. Annisa, and E. J. Pristianto, "Sistem Penguncian Menggunakan Teknologi DTMF Non Standar Berbasis Mikrokontroler," *Prosiding Industrial Research Workshop and National Seminar*, Bandung, 2022, pp. 565-569.
- [6] "Plaintext" 27 may 2020 [online]. Available: <https://www.hypr.com/plaintext/>
- [7] Datasheet, "DTMF Tone Generation and Detection: An Implementation Using the TMS320C54x," Gunter Schmer, Texas Instruments, MTSA, 2020.
- [8] Cool Edit Pro, Version 2 Users Guide Brought to you by Syntrillium Software Corporation P.O. Box 62255, Phoenix, AZ 85082-2255, USA 2018.
- [9] T. Joseph, K. Tyagi, and R. Kumbhare, "Quantitative analysis of DTMF tone detection using DFT, FFT and Goertzel algorithm," *2019 Global Conference for Advancement in Technology (GCAT)*, 2019, pp. 1-4.
- [10] F. Y. Shih, "Digital Watermarking and Steganografi" in *Digital Watermarking and Steganography*, Eds. Fundamentals and Techniques, Taylor and Francis Group, Broken Sound Parkway NW, pp. 221-239, 2017.
- [11] C. H. Loekito, T. Indriyani, and N. F. Rozi, "Aplikasi Pengamanan Dokumen PDF dengan Teknik Watermarking Menggunakan Metode Serpent Cipher," *Jurnal Teknologi dan Manajemen*, vol. 1, no. 1, pp. 28-35, 2020.
- [12] D. Nataliana, F. Hadiatna, and A. Fauzi, "Rancang Bangun Sistem Keamanan RFID Tag menggunakan Metode Caesar Cipher pada Sistem Pembayaran Elektronik," *ELKOMIKA: Jurnal Teknik Energi Elektrik, Teknik Telekomunikasi, & Teknik Elektronika*, vol. 7, no. 3, pp. 427, 2019.
- [13] I. Gunawan, H. S. Tambunan, E. Irawan, H. Qurniawan, and D. Hartama, "Combination of Caesar Cipher Algorithm and Rivest Shamir Adleman Algorithm for Securing Document Files and Text Messages," *In Journal of Physics: Conference Series*, 2019.
- [14] I. W. Utomo, R. Latifah, and R. D. Risanty, "Aplikasi Kriptografi Berbasis Android Menggunakan Algoritma Caesar Cipher Dan Vigenere Cipher," *JUST IT: Jurnal Sistem Informasi, Teknologi Informasi dan Komputer*, vol. 9, no. 2, pp. 142-149, 2019.
- [15] Galilov, 21 Desember 2021. [Online]. Available: <https://github.com/galilov/arduino-dtmf/tree/main/atmega-dekoder-dtmf>.