Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

Optimasi Pengamanan Pesan Suara Menggunakan Vernam Cipher Berbasis Algoritma Blum Blum Shub

Agnes Victoria Simanjuntak*, Eliasta Ketaren, Marline S. Paendong
Sistem Informasi, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sam Ratulangi, Manado, Indonesia
Email: [1,*]agnessimanjuntak106@gmail.unsrat.ac.id, [2]eliasketaren@unsrat.ac.id, [3]marline.paendong@unsrat.ac.id
Email Penulis Korespondensi: agnessimanjuntak106@gmail.unsrat.ac.id*
Submitted: **09/03/2026**; Accepted: **25/03/2026**; Published: **31/03/2026**

Abstrak– Perkembangan teknologi informasi yang pesat meningkatkan kemudahan dalam pertukaran data digital, termasuk pesan suara, namun juga menimbulkan risiko keamanan seperti penyadapan dan penyalahgunaan informasi. Oleh karena itu, diperlukan metode pengamanan yang kuat dan andal. Penelitian ini bertujuan untuk mengoptimalkan pengamanan pesan suara dengan mengombinasikan algoritma *Blum Blum Shub* (BBS) sebagai pembangkit bilangan acak kriptografis dengan *Vernam Cipher*. Proses dimulai dengan perekaman suara yang dikonversi ke dalam bentuk digital, kemudian direpresentasikan dalam bentuk biner. Selanjutnya, data dienkripsi menggunakan operasi XOR dengan *keystrea*m yang dihasilkan oleh algoritma BBS. Tahap dekripsi dilakukan dengan menggunakan kunci yang sama untuk mengembalikan data ke bentuk semula. Selain itu, proses pengolahan data melibatkan transformasi sinyal menggunakan *Mel-Spectrogram* sebelum dikonversi ke dalam bentuk biner. Hasil pengujian menunjukkan bahwa sistem mampu menghasilkan *ciphertext* yang tidak dapat dikenali serta memiliki tingkat keacakan yang tinggi. Perbedaan nilai seed menghasilkan *ciphertext* yang berbeda meskipun menggunakan data suara yang sama, menunjukkan tingkat keamanan yang baik. Proses dekripsi berhasil mengembalikan pesan suara ke bentuk semula tanpa kehilangan informasi. Dengan demikian, kombinasi algoritma *Blum Blum Shub* dan *Vernam Cipher* terbukti efektif dalam meningkatkan keamanan pengamanan pesan suara.

Kata Kunci: Blum Blum Shub; Vernam Cipher; kriptografi; pesan suara; keystream; keamanan data

Abstract– The rapid advancement of information technology has facilitated the exchange of digital data, including voice messages, but also introduced security risks such as interception and misuse of information. Therefore, a robust and reliable data security method is required. This study aims to optimize voice message security by combining the *Blum Blum Shub* (BBS) algorithm as a cryptographically secure pseudorandom number generator with the Vernam Cipher. The process begins with recording voice data, which is then converted into digital format and represented as binary data. The encryption process is performed using an XOR operation with a keystream generated by the BBS algorithm. Decryption is carried out using the same key to restore the original data. Additionally, the preprocessing stage includes transforming the audio signal using a Mel-Spectrogram before binary conversion. The experimental results show that the system produces ciphertext that is unrecognizable and exhibits high randomness. Variations in seed values generate different ciphertexts even when the same audio input is used, indicating strong security characteristics. The decryption process successfully reconstructs the original voice message without any loss of information. Thus, the combination of the *Blum Blum Shub* algorithm and the *Vernam Cipher* is proven to be effective for securing voice messages.

Keywords: *Blum Blum Shub*; *Vernam Cipher*; cryptography; voice message; *keystrea*m; data security

1. PENDAHULUAN

Perkembangan teknologi komunikasi dan informasi di era digital telah membawa perubahan signifikan dalam cara manusia berinteraksi dan bertukar informasi. Proses pengiriman dan penerimaan data kini dapat dilakukan secara *real-time* melalui jaringan internet dengan memanfaatkan berbagai perangkat, seperti *smartphone* dan komputer [1]. Kemudahan ini memberikan dampak positif dalam meningkatkan efisiensi komunikasi, baik dalam lingkup personal, pendidikan, maupun organisasi. Namun, di balik kemajuan tersebut, muncul tantangan serius terkait aspek keamanan informasi, terutama ketika data yang dikirim bersifat pribadi dan sensitif [2].

Salah satu bentuk komunikasi digital yang semakin populer adalah pesan suara (*voice message*) [3]. Fitur ini banyak digunakan dalam berbagai aplikasi pesan instan karena mampu menyampaikan informasi secara lebih ekspresif melalui intonasi, emosi, dan penekanan suara dibandingkan dengan pesan teks [4]. Penggunaan pesan suara dinilai lebih efektif dalam memperjelas maksud komunikasi serta membangun kedekatan antar pengguna [5]. Meskipun demikian, pengiriman pesan suara melalui jaringan publik memiliki risiko keamanan yang tinggi apabila tidak dilengkapi dengan sistem pengamanan yang memadai [6],[7].

Permasalahan yang sering terjadi di masyarakat adalah penyebarluasan pesan suara yang bersifat privat tanpa izin dari pihak yang bersangkutan [8],[9]. Pesan suara yang seharusnya hanya diterima oleh pihak tertentu justru dapat tersebar luas dan disalahgunakan oleh pihak yang tidak bertanggung jawab. Kondisi ini tidak hanya menimbulkan kerugian secara sosial, tetapi juga berdampak pada aspek psikologis individu yang terlibat [10]. Hal tersebut menunjukkan bahwa pesan suara yang tidak diamankan memiliki potensi besar untuk disadap, dimodifikasi, maupun disebarluaskan secara ilegal. Oleh karena itu, diperlukan suatu mekanisme pengamanan tambahan yang mampu menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan keaslian (*authenticity*) pesan suara dari pengirim hingga ke penerima.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

Salah satu pendekatan yang dapat digunakan untuk mengatasi permasalahan tersebut adalah kriptografi [11]. Kriptografi merupakan teknik pengamanan informasi dengan cara mengubah pesan asli (*plaintext*) menjadi pesan tersandi (*ciphertext*) sehingga tidak dapat dipahami oleh pihak yang tidak berwenang [12]. Dalam konteks pengamanan pesan suara, sinyal audio terlebih dahulu harus direpresentasikan ke dalam bentuk digital [13]. Pada penelitian ini, proses tersebut dilakukan menggunakan metode *Mel-Spectrogram* untuk mengubah sinyal audio menjadi representasi numerik, yang selanjutnya dikonversi ke dalam bentuk biner agar dapat diproses dalam sistem kriptografi berbasis operasi bit [14][15].

Algoritma enkripsi yang digunakan dalam penelitian ini adalah *Vernam Cipher*, yaitu metode enkripsi yang menggunakan operasi XOR antara *plaintext* dan kunci dengan panjang yang sama [16]. Keamanan metode ini sangat bergantung pada kualitas kunci yang digunakan. Jika kunci yang digunakan benar-benar acak dan tidak dapat diprediksi, maka *Vernam Cipher* dapat mencapai tingkat keamanan yang sangat tinggi [17]. Sebaliknya, apabila kunci memiliki pola tertentu atau dapat ditebak, maka sistem enkripsi menjadi rentan terhadap serangan kriptanalisis.

Untuk mengatasi permasalahan tersebut, penelitian ini menggunakan algoritma *Blum Blum Shub* (BBS) sebagai pembangkit bilangan acak semu (*Pseudo Random Number Generator*) [18]. Algoritma ini dikenal memiliki tingkat keamanan yang tinggi karena didasarkan pada permasalahan matematika yang sulit diselesaikan, seperti *integer factorization problem* dan *quadratic residuosity problem*. Dengan dasar tersebut, bilangan acak yang dihasilkan oleh BBS memiliki sifat tidak mudah diprediksi, sehingga sangat sesuai digunakan sebagai pembangkit kunci dalam sistem kriptografi [19] .

Berbeda dengan penelitian sebelumnya yang umumnya hanya menggunakan satu kunci dalam proses enkripsi, penelitian ini mengusulkan penggunaan tiga kunci berbeda yang dihasilkan oleh algoritma BBS untuk meningkatkan kompleksitas sistem keamanan [20],[21]. Penerapan multi-kunci ini diharapkan mampu memperkuat ketahanan sistem terhadap serangan, serta mempersulit pihak lain dalam melakukan analisis pola terhadap *ciphertext* yang dihasilkan.

Berdasarkan uraian tersebut, penelitian mengenai implementasi algoritma *Blum Blum Shub* sebagai pembangkit bilangan acak pada *Vernam Cipher* untuk pengamanan pesan susara menjadi penting untuk dilakukan. Penelitian ini tidak hanya berangkat dari permasalahan nyata terkait kebocoran pesan suara, tetapi juga menawarkan solusi teknis yang inovatif melalui integrasi metode pengolahan sinyal audio dan algoritma kriptografi. Dengan demikian, diharapkan penelitian ini dapat memberikan kontribusi dalam meningkatkan keamanan komunikasi berbasis suara di era digital.

Selain aspek kerahasiaan, pengamanan pesan suara juga harus memperhatikan aspek keutuhan (*integrity*) data. Dalam proses transmisi melalui jaringan, data suara berpotensi mengalami perubahan, baik secara sengaja maupun tidak sengaja. Gangguan jaringan, serangan *man-in-the-middle*, maupun manipulasi data dapat menyebabkan isi pesan berubah dari bentuk aslinya. Oleh karena itu, sistem pengamanan yang dirancang tidak hanya harus mampu menyembunyikan isi pesan, tetapi juga menjamin bahwa pesan yang diterima tetap utuh dan sesuai dengan pesan yang dikirimkan.

Di sisi lain, perkembangan teknik kriptanalisis juga menjadi tantangan tersendiri dalam pengembangan sistem keamanan. Berbagai metode serangan, seperti *brute force attack*, *known-plaintext attack*, dan *ciphertext attack*, terus berkembang seiring dengan meningkatnya kemampuan komputasi. Hal ini menuntut penggunaan algoritma yang tidak hanya kuat secara teoritis, tetapi juga tangguh dalam implementasi praktis. Penggunaan pembangkit bilangan acak yang lemah dapat menjadi celah utama dalam sistem kriptografi, karena kunci yang dihasilkan dapat diprediksi oleh penyerang.

Dalam konteks ini, penggunaan algoritma *Blum Blum Shub* menjadi sangat relevan karena memiliki landasan matematis yang kuat dan telah diakui dalam dunia kriptografi sebagai salah satu pembangkit bilangan acak yang aman. Keunggulan BBS dalam menghasilkan *keystrea*m yang memiliki distribusi acak dan sulit diprediksi menjadikannya pilihan yang tepat untuk mendukung keamanan *Vernam Cipher*. Dengan demikian, kombinasi kedua algoritma ini diharapkan mampu menghasilkan sistem enkripsi yang tidak hanya sederhana dalam konsep, tetapi juga kuat dalam aspek keamanan.

Selain itu, pendekatan yang menggabungkan pengolahan sinyal digital dengan teknik kriptografi memberikan nilai tambah dalam penelitian ini. Penggunaan metode *Mel-Spectrogram* memungkinkan transformasi sinyal suara ke dalam bentuk representasi frekuensi yang lebih informatif, sehingga memudahkan proses konversi ke bentuk biner. Integrasi antara bidang *digital signal processing* dan kriptografi ini menjadi salah satu bentuk inovasi yang relevan dalam menjawab kebutuhan keamanan data multimedia di era modern.

Penting untuk menekankan bahwa keamanan komunikasi tidak hanya menjadi tanggung jawab individu, tetapi juga menjadi bagian dari sistem yang dirancang secara menyeluruh. Penelitian ini berupaya memberikan kontribusi dalam pengembangan sistem keamanan yang lebih baik, khususnya dalam pengamanan pesan suara. Dengan memanfaatkan kombinasi algoritma *Blum Blum Shub* dan *Vernam Cipher*, serta penerapan multi-kunci, diharapkan sistem yang dihasilkan mampu memberikan tingkat perlindungan yang lebih tinggi terhadap ancaman kebocoran dan penyalahgunaan data di era digital yang semakin kompleks.

2. METODOLOGI PENELITIAN

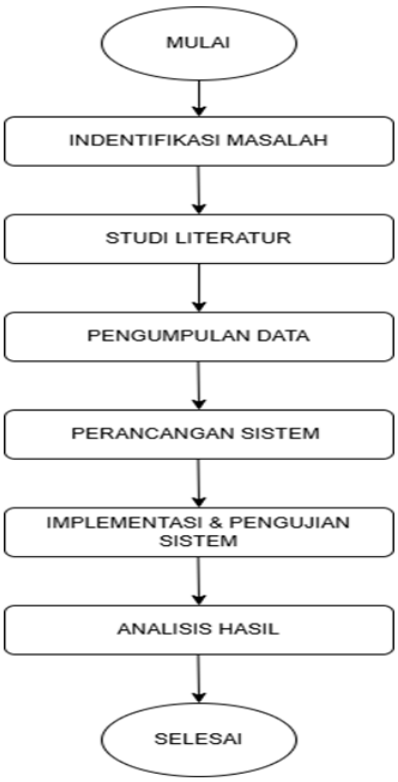
Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

2.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan eksperimental dengan menerapkan algoritma *Blum Blum Shub* (BBS) sebagai metode enkripsi pada pesan suara [22]. Objek penelitian yang digunakan adalah pesan suara (*real time*) yang direkam, kemudian dilakukan enkripsi menggunakan *keystrea*m yang dihasilkan oleh *Blum Blum Shub*.

2.2 Tahapan Penelitian

Penelitian ini dimulai dengan memasukkan data audio atau WAV yang kemudian akan diekstrasi menggunakan *Mel-Spectogram* untuk memperoleh representasi spektrum. Hasil dari spektrum akan diubah menjadi teks melalui proses pengenalan suara, lalu dikonversi ke bentuk biner. Data dari biner tersebut di enkripsi dengan *keystream* dari algoritma *Blum Blum Shub* menggunakan operasi XOR hingga menghasilkan ciphertext. Selanjutnya *ciphertext* dideskripsi kembali dengan cara yang sama untuk mengembalikan pesan ke bentuk aslinya.



Gambar 1. Tahapan Penelitian

Penelitian ini diawali dengan tahap identifikasi masalah, yaitu mengkaji bagaimana meningkatkan keamanan pesan suara agar tidak mudah disadap maupun dimanipulasi oleh pihak yang tidak berwenang. Permasalahan ini menjadi penting mengingat meningkatnya penggunaan pesan suara dalam komunikasi digital yang rentan terhadap berbagai ancaman keamanan. Oleh karena itu, penelitian ini mengusulkan penggunaan pendekatan kriptografi dengan mengombinasikan algoritma *Blum Blum Shub* (BBS) sebagai pembangkit bilangan acak dan *Vernam Cipher* sebagai metode enkripsi, dengan tujuan untuk meningkatkan tingkat keamanan dalam pengiriman pesan suara.

Tahap selanjutnya adalah studi literatur, yang dilakukan dengan mempelajari berbagai teori dan konsep yang relevan dengan penelitian. Peneliti mengkaji kriptografi klasik dan modern, prinsip kerja algoritma *Blum Blum Shub*, mekanisme enkripsi *Vernam Cipher*, serta teknik pengolahan sinyal digital, khususnya metode *Mel-Spectrogram*. Studi literatur ini bertujuan untuk membangun landasan teoritis yang kuat serta memahami metode yang paling tepat untuk diterapkan dalam penelitian.

Pada tahap pengumpulan data, digunakan data berupa pesan suara sederhana yang dijadikan sebagai bahan uji dalam sistem yang dikembangkan. Pesan suara tersebut kemudian dikonversi ke dalam bentuk *Mel-Spectrogram* untuk mengekstraksi karakteristik sinyal audio. Hasil ekstraksi tersebut selanjutnya direpresentasikan ke dalam bentuk biner, sehingga dapat diproses menggunakan algoritma kriptografi berbasis operasi bit.

Tahap perancangan sistem berfokus pada penyusunan alur kerja sistem enkripsi dan dekripsi. Data biner yang dihasilkan dari proses sebelumnya akan diproses menggunakan algoritma *Blum Blum Shub* untuk menghasilkan bilangan acak yang digunakan sebagai kunci dalam *Vernam Cipher*. Selanjutnya, data biner

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

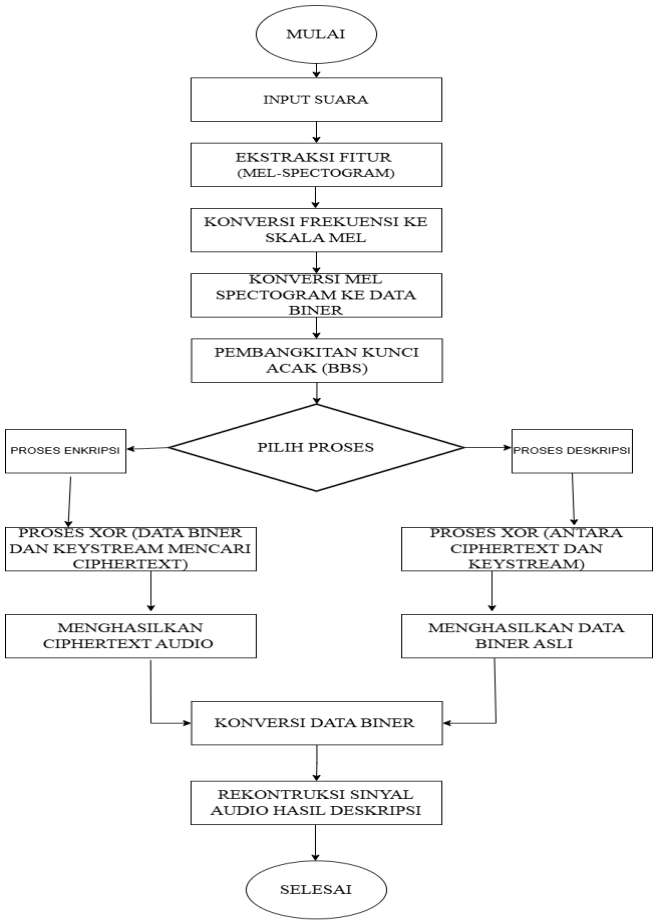
dienkripsi melalui operasi XOR antara *plaintext* dan kunci yang dihasilkan, sehingga menghasilkan *ciphertext* berupa pesan suara yang telah diamankan.

Tahap implementasi dan pengujian sistem dilakukan dengan menggunakan bahasa pemrograman Python. Sistem yang telah dirancang diimplementasikan untuk menguji kemampuan dalam mengenkripsi dan mendekripsi pesan suara. Pengujian dilakukan untuk memastikan bahwa proses enkripsi berjalan dengan baik dan proses dekripsi mampu mengembalikan pesan suara ke bentuk semula tanpa kehilangan informasi.

Tahap terakhir adalah analisis hasil, yang bertujuan untuk mengevaluasi kinerja sistem secara keseluruhan. Analisis dilakukan dengan melihat tingkat efektivitas sistem dalam mengamankan pesan suara, akurasi proses enkripsi dan dekripsi, serta kualitas keacakan bilangan yang dihasilkan oleh algoritma *Blum Blum Shub*. Hasil analisis ini digunakan untuk menilai keberhasilan metode yang diusulkan dalam meningkatkan keamanan komunikasi berbasis pesan suara.

2.3 Diagram Alur Penelitian

Dalam penelitian ini, Diagram Alur Peneletian data menggambarkan rangkaian proses atau tahapan dari sistem menggunakan kombinasi algoritma *Blum Blum Shub* dan *Mel-Spectogram* Berikut merupakan alur kerja sistem dari penelitian ini.



Gambar 2. Diagram Alur Penelitian

Berdasarkan diagram alur penelitian pada Gambar 3, proses pengamanan pesan suara dilakukan melalui beberapa tahapan yang saling berkesinambungan, mulai dari proses *input* sinyal suara, ekstraksi fitur menggunakan *Mel-Spectrogram*, konversi data ke bentuk biner, pembangkitan kunci acak menggunakan algoritma *Blum Blum Shub*, hingga proses enkripsi dan dekripsi menggunakan *Vernam Cipher* serta rekonstruksi kembali sinyal audio.

2.4 Data Penelitian

Data yang digunakan untuk penelitian berupa file audio dengan format WAV dengan frekuensi sampling terntentu (misalnya 16 kHz). Data penelitian ini, teks hasil dari konversi sinyal suara yang dipresentasikan dalam bentuk kode biner menggunakan standart ASCII 8-bit. Karakter pada teks memiliki nilai desimal tertentu yang kemudian akan diubah menjadi representasi biner.

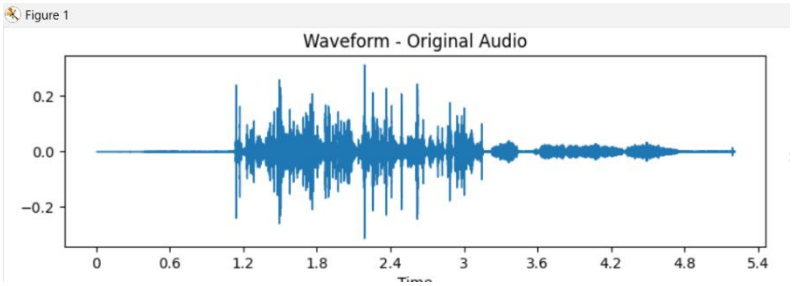
Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

3. HASIL DAN PEMBAHASAN

Sistem yang dirancang memiliki antarmuka utama yang memfasilitasi tiga fungsi utama, yaitu pembuatan kunci menggunakan algoritma pembangkit bilangan acak, proses enkripsi audio untuk mengamankan pesan suara, serta proses dekripsi audio untuk mengembalikan pesan ke bentuk aslinya. Ketiga fungsi tersebut saling terintegrasi dalam satu sistem guna memastikan proses pengamanan dan pemulihan data suara dapat dilakukan secara efektif dan efisien.

3.1 Analisis Pesan Suara ke Representasi Biner Menggunakan *Mel-Spectogram*

Pada Tahap ini dilakukan analisis terhadap sinyal suara asli sebelum melalui proses enkripsi. Analisis dilakukan dalam dua bentuk representasi, yaitu domain waktu (*Wavefrom*) dan domain waktu-frekuensi (*Mel-Spectogram*). Tujuan analisis ini Adalah untuk memahami karakterisitik sinyal suara sebelum melakukan tahap transformasi suara dan pengamanan data. *Wavefrom* merupakan represenatsi sinyal audio dalam domain waktu yang menunjukkan amplitudo dan waktu. Pada Gambar *Wavefrom* audio original yang diperoleh. Sumbu horizontal memperlihatkan representasi waktu (detik), sedangkan sumbu vertical menunjukkan amplitudo sinyal.

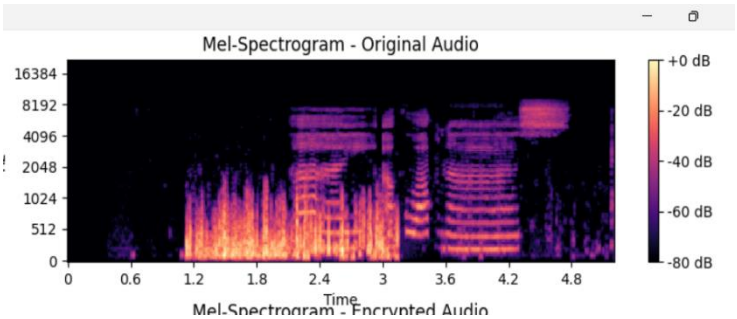


Gambar 3. Hasil *Wavefrom* audio original

Berdasarkan visualisasi tersebut, dapat dilihat bahwa sinyal memiliki fluktuasi amplitudo yang tidak konstan, dengan beberapa bagian menunjukkan amplitudo tinggi yang merepresentasikan energi suara yang kuat, serta bagian lain dengan amplitudo rendah yang menandakan adanya jeda atau intonasi suara yang lebih lemah. Fluktuasi ini merupakan karakteristik alami suara manusia yang dipengaruhi oleh intonasi, tekanan, dan artikulasi saat berbicara. Pola gelombang yang terbentuk menunjukkan struktur yang teratur dan bermakna, sehingga informasi suara dapat dikenali secara temporal dan selanjutnya diproses dalam sistem pengolahan sinyal.

3.2 Analisis Mel-Spectorgam Audio Asli

Dalam memproleh informasi frekuensi yang terkandung dalam sinyal suara, dilakukan transformasi dari domain waktu ke domain waktu-frekunsi menggunakan metode *Short-time Fourier transform*. Transformasi ini menghasilkan spektrum frekuensi untuk setiap potongan waktu (frame) sinyal. Selanjutnya, spektrum tersebut dikonversi ke dalam skala persepsi manusia menggunakan Mel-Scale sehingga diperoleh representasi *Mel-Spectogram*. Dapat dilihat pada gambar hasil dari *Mel-Spectogram*.



Gambar 4. Hasil *Mel-Spectogram* original

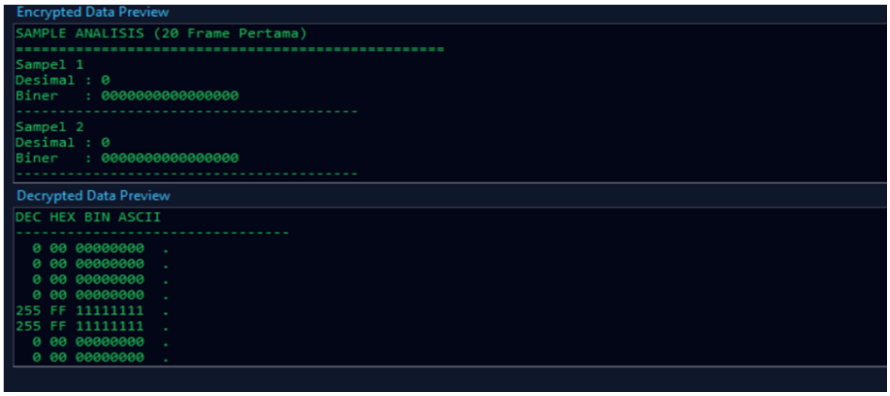
Pada gambar *Mel-Spectrogram* original yang dihasilkan, sumbu horizontal menunjukkan waktu, sumbu vertikal menunjukkan frekuensi dalam satuan Hertz (Hz), sedangkan intensitas warna merepresentasikan besar energi pada frekuensi tertentu, di mana area berwarna terang menunjukkan energi tinggi dan area gelap menunjukkan energi rendah. Terlihat adanya pola horizontal yang cukup jelas yang merepresentasikan formant suara manusia, yaitu resonansi alami saluran vokal saat menghasilkan bunyi tertentu. Berbeda dengan *wavefrom* yang hanya menampilkan amplitudo terhadap waktu, *Mel-Spectrogram* memberikan informasi tambahan

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

mengenai distribusi energi frekuensi, sehingga struktur fonetik suara dapat diamati dengan lebih jelas. Secara umum, pembentukan *Mel-Spectrogram* melibatkan beberapa tahapan, yaitu *frame blocking* (pembagian sinyal menjadi potongan kecil), penerapan *Short-Time Fourier Transform* (STFT), pemetaan frekuensi ke skala Mel, serta perhitungan log energi. Hasil visualisasi *Mel-Spectrogram* original ini menunjukkan bahwa sinyal suara masih memiliki struktur frekuensi yang terorganisir dan belum mengalami proses pengacakan, sehingga masih dapat dikenali sebagai sinyal ucapan.

3.3 Representasi Data Audio dalam Bentuk Biner

Setelah melalui proses ekstrasi fitur dari *Wavefrom* dam *Mel-Spectogram* diperoleh, maka tahap selanjutnya adalah mengkoversi data audio ke dalam bentuk biner. Representasi biner ini digunakkan sebagai masukan pada proses *Vernam Chiper* dengan *keystrea*m yang dibangkitkan dengan *Blum Blum Shub*. Sistem yang dibangun menyediakan fitur lihat proses biner untuk menampilkan hasil konversi tersebut secara langsung.



Gambar 5. Hasil Biner Audio Original

Berdasarkan Gambar, terlihat bahwa data audio telah berhasil direpresentasikan dalam bentuk bilangan biner per sampel. Setiap nilai amplitudo sinyal dikonversi menjadi representasi 8-bit sehingga menghasilkan deretan bit yang akan digunakan pada proses XOR dengan *keystrea*m.

3.4 Pembuatan Kunci

Pembuatan kunci pada sistem ini menggunakan kombanisasi yaitu kunci matematika (BBS) sebagai pembangkit bilangan acak dan kunci aliran (*Vernam*/XOR) sebagai metode enkripsi dan *keystrea*m. Aturan pembuatan kunci kombinasi dengan langkah – langkah sebagai berikut :

a. Pemilihan Bilangan Prima
   Pemilihan ilangan prima menjadi landasan utama dalam pembuatan kunci dimana semakin besar bilangan prima yang digunakan maka akan semakin kuat kunci yang dibuat. Terdapat dua pilihan dalam menentukan bilangan prima yaitu secara manual atau yang dibuat acak oleh sistem.
b. Perhitungan Hasil Kali Bilangan Prima
   Pada Algoritma *Blum Blum Shub*, pemelihan bilangan prima menjadi dasar pembentukan kunci. Dua bilangan prima p dan q harus memenuhi syarat.

$$n = p \times q \tag{1}$$

c. Perhitungan Modulus
   Tahapan ini nilai n sebagai nilai modulus yang dihitung dari perkalian dua bilangan prima p dan q . Nilai n digunakan sebagai dasar operasi modulo pada algoritma BBS dan dihitung dengan:

$$n = 491 \times 547 = 272953$$

   Nilai n sebagai kunci publik internal bagi generator BBS.
d. Penentuaan Seed Awal
   Seed x_0 adalah bilangan awal yang memulai proses pembangkit *keystrea*m. Seed harus relatif prima terhadap n, nilai seed ini yang membuat hasil nilai BBS berbeda walaupun nilai $\boldsymbol{p}$ dan $\boldsymbol{q}$ nya sama, sehingga :

$$\gcd(x_0, n) = 1 \tag{2}$$

   dipilih :

$$x_0 = 12345$$

   Karena :

$$\gcd(12345, 272953) = 1$$

   maka seed tersebut valid.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

e. Pembentukan *Keystrea*m *Blum Blum Shub*
Pada tahap ini bilangan acak dihasilkan dengan rumus sebagai berikut:

$$X_i + 1 = X_i^2 \ mod \ n \tag{10}$$

Karena proses menggunakan operasi modulo n, maka setiap nilai x_i yang dihasilkan akan selalu berada dalam rentang seperti yang ada dalam rumus :

$$0 \leq xi < n \tag{11}$$

Dimana :
Nilai $x_i$tidak pernah negatif
Nilai $x_i$selalu lebih kecil dari n
Jadi semua hasil BBS berada dalam rentang 0 sampai $n-1$
Dengan nilai awal $x_0 = 12345$, diperoleh :

$$x_1 = 12345^2 mod 272953 = 91251$$
$$x_2 = 91251^2 mod 272953 = 40783$$
$$x_3 = 40783^2 \ mod 272953 = 150460$$
$$x_4 = 150460^2 mod 272953 = 35686$$
$$x_5 = 35686^2 mod 272953 = 164851$$
$$x_6 = 164851^2 mod 272953 = 105615$$
$$x_7 = 105615^2 mod 272953 = 30927$$
$$x_8 = 30927^2 mod 272953 = 52017$$

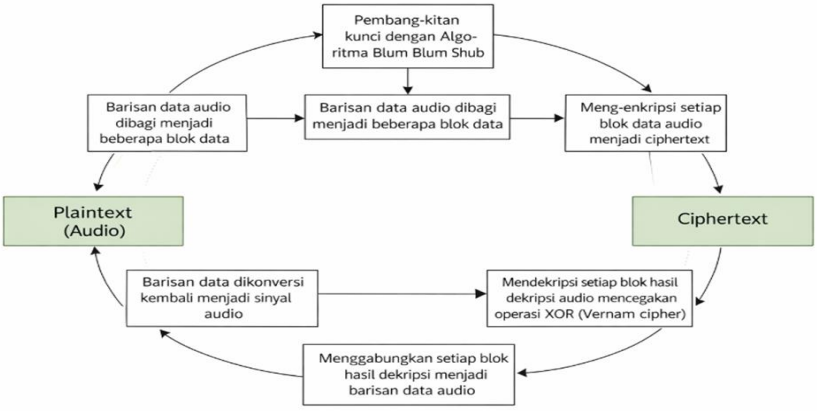
Deret x_i ini membentuk kunci utama BBS. Bit kunci diambil dari bit paling rendah (LSB) adalah :

$$K = 11001111$$

f. Pembentukan Kunci Vernam (XOR Key).
Karena *Vernam Cipher* beroperasi pada data biner 8-bit, maka nilai keluaran BBS rentang dari 0-255 dan operasi modulo 256. Hasil dari data tersebut menjadi kunci XOR untuk digabungkan dengan data audio atau ASCII untuk melakukan tahap enkripsi dan deskripsi untuk kembali ke bentuk semula.
g. Relasi Dua Kunci.
Dalam pembuatan kunci dijelaskan bahwa sistem yang dipakai menggunakan dua lapisan kunci. Kunci BBS pada bagian (p, q, dan x_0) digunakan sebagai pembangkit. Kunci Vernam digunakan sebagai enkripsi (*keystream* hasil BBS). Struktur sistem ini digunakan untuk meningkatkan keamanan karena kunci XOR tidak dapat dibuat langsung, melainkan harus melalui proses kriptografi yang kuat.
h. Keamanan Sistem.
Bagian ini menjelaskan bahwa sistem keamanan ini bergantung pada kesulitan faktorisasi $n = p \times q$, sifat pseudorandom kuat dari BBS (*Blum Blum Shub*). Sifat *Vernam Cipher* yang perfect secrecy jika *keystrea*m tidak diketahui.

3.5 Pembuatan Kunci

Program dapat dimulai dari dua sisi yang berbeda sesuai dengan kebutuhan dari sipengguna. Dimana dapat dimulai dari pengamanan data audio dengan proses enkripsi atau juga dalam pengembalian data audio ke bentuk semula melalui proses dekripsi.



Gambar 6. Diagram Alur Pengamanan Audio

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

3.6 Enkripsi Audio

Proses enkripsi dalam pengamanan audio dapat dilakukan seperti berikut :

a. Konversi Audio
Dalam proses enkripsi hal yang pertama yang dilakukan adalah mengkonversi sinyal audio menjadi bentuk numerik. Audio direkam dan dibaca dalam bentuk sinyal dengan format PCM (*Pulse Code Modulation*).

b. Membagi Blok Teks Angka
Proses enkripsi dilakukan untuk untuk menggunakan algoritma *Vernam Cipher* dengan operasi XOR antara *plaintext* hasil dari kuantisasi *log-mel spectogram* dan *keystream* yang dihasilkan oleh algoritma *Blum Blum Shub*. Data *plaintext* dan *keystream* dibagi menjadi 16-bit ke dalam setiap blok untuk meningkatkan efisiensi dalam proses enkripsi.
Proses enkripsi menggunakan rumus vernam yaitu :

$$C = P \oplus K$$

Dimana :

Nilai P : Hasil dari p dan q dipilih sebagai bilangan prima, yaitu p ≡ 3 (mod 4) dan q ≡ 3 (mod 4). Nilai tersebut kemudian digunakan untuk membentuk modulus n = p × q.
Nilai K : Diperoleh dari iterasi algoritma *Blum Blum Shub*, yaitu hasil xi yang dihitung menggunakan rumus pembentukan *keystream*.

Sebagai enkripsi dapat berupa :
Misalkan :
Bilangan Prima
P = 491
q = 547
Modulus

$$n = 491 \times 547$$
$$n = 272953$$

Nilai hasil dari *keystream Blum Blum Shub* :

$x_1 = 12345^2 \, mod \, 272953 = 91251$
$x_2 = 91251^2 \, mod \, 272953 = 40783$
$x_3 = 40783^2 \, mod \, 272953 = 150460$
$x_4 = 150460^2 \, mod \, 272953 = 35686$
$x_5 = 35686^2 \, mod \, 272953 = 164851$
$x_6 = 164851^2 \, mod \, 272953 = 105615$
$x_7 = 105615^2 \, mod \, 272953 = 30927$
$x_8 = 309272 \, mod \, 272953 = 52017$

Hasil setelah dilakukan perkalian terhadap setiap *keystream* (x_1 mod 256)

$x_1 = 115$ (01110011)
$x_2 = 79$ (01001111)
$x_3 = 188$ (10111100)
$x_4 = 102$ (01100110)
$x_5 = 243$ (11110011)
$x_6 = 143$ (10001111)
$x_7 = 207$ (11001111)
$x_8 = 49$ (00110001)

Pembagian blok per 16-bit dari *keystream* ialah :
x1 dan x2 = 01110011 01001111 = 0111001101001111
x3 dan x4 = 10111100 01100110 = 1011110001100110
x5 dan x6 = 11110011 10001111 = 1111001110001111
x7 dan x8 = 11001111 00110001 = 1100111100110001

Enkripsi dari Blok 1 :
P = 1110001100101101
K = 0111001101001111
XOR = 1001000001100010
Ciphertext blok 1 : 1001000001100010 = 144, 98

Enkripsi Blok 2 :

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

P = 1000000001000000
K = 1011110001100110
XOR = 0011110011100110
Ciphertext blok 2 : 0011110011100110 = 60, 230

Enkripsi Blok 3 :
P = 0110100001101001
K = 1111001110001111
XOR = 1001101111100110
Ciphertext blok 3 : 1001101111100110 = 155, 230

Enkripsi Blok 4 :
P = 0011000100110001
K = 1100111100110001
XOR = 1111111000000000
Ciphertext blok 4 : 1111111000000000 = 254, 0

c. Deskripsi

1. Proses Deskripsi

Proses ini dilakukan untuk mengembalikan *ciphertext* ke bentuk *plaintext* semula. Dekripsi menggunakan *keystream* yang sama untuk melakukan proses enkripsi, yang dihasilkan kembali dari algoritma *Blum Blum Shub* menggunakan parameter dan seed yang identik. Operasi XOR kembali dilakukan antara *ciphertext* dan *keystream* sehingga menghasilkan *plaintext* awal.
Proses dekripsi ini menggunakan rumus :

$$P = C \oplus K$$

Proses dekripsi sebagai berikut :
Blok 1 : *Ciphertext* : 1001000001100010
*Keystrea*m : 0111001101001111
XOR : 1110001100101101
Plaintext Blok 1 : 227, 45 .

Blok 2 : *Ciphertext* : 0011110011100110
*Keystrea*m : 1011110001100110
XOR : 1000000001000000
Plaintext Blok 2 : 128, 128.

Blok 3 : *Ciphertext* : 1001101111100110
*Keystrea*m : 1111001110001111
XOR : 0110100001101001
Plaintext Blok 3 : 104, 105

Blok 4 : *Ciphertext* : 1111111000000000
*Keystrea*m : 1100111100110001
XOR : 0011000100110001
Plaintext Blok 3 : 49, 49

2. Rekontruksi Data Audio

Hasil *Plaintext* dari proses dekripsi kemudian disusun kembali sesuai dengan pembagian blok sebelumnya seperti di awal. Nilai *plaintext* tersebut selanjutnya akan dikonversi kembali dari bentuk bilangan kuantisasi ke representasi *log-mel sepctogram*, dimana akhirnya direkontruksi menjadi sinyal audio. Dengan demikian, audio hasil dekripsi memliki nilai karakteristik yang sama dengan nilai sebelum proses enkripsi dilakukan.

3.7 Hasil Pengujian Pengamanan Data Audio

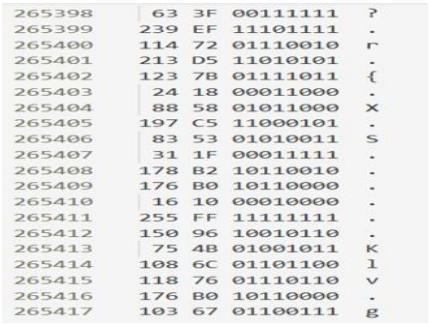
Berdasarkan hasil pengujian, bahwa semakin besar ukuran dan durasi audio, maka waktu yang diperlukan untuk proses enkripsi dan dekripsi yang dibututhkan juga semakin meningkat. Hal ini disebabkan oleh bertambahnya jumlah blok data audio yang harus diproses. Ukuran *ciphertext* relatif tidak mengalami perubahan yang signifikan dibandingkan dengan ukuran audio asli, menunjukkan bahwa proses enkripsi menggunakan algoritma *Blum Blum Shub* dan *Vernam Cipher* yang tidak menyebabkan ekspansi data yang besar.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

Tabel 1. Uji Ukuran

Plaintext (Audio)	Ukuran Audio	Panjang Bit Kunci	Waktu Enkripsi	Jumlah Blok	Ukuran Ciphertext	Waktu dekripsi
AudioPendek.wav	265kb	256 bit	6.8 detik	1.168 blok	2.28kb	8 detik
AudioSedang.wav	562kb	256 bit	11.2 detik	47.850 blok	747kb	12 detik
AudioPanjang.wav	830kb	256bit	13.5detik	849.730 blok	17.102kb	14.1detik

Berdasarkan hasil pengujian, proses pengamanan audio menunjukkan perbedaan yang jelas antara audio asli (pendek, sedang, dan panjang) dengan audio hasil enkripsi. Kecepatan dalam pengamanan juga berbeda terhadap audio dan ukuran yang berbeda. Semakin kecil audio, semakin cepat proses enkripsi dan dekripsi dapat dilakukan.



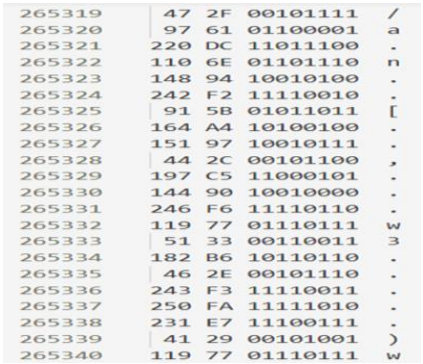
Gambar 7. Hasil Enkripsi

Pengujian ini berfokus pada penggunaan kunci seed yang berbeda pada algoritma *Blum Blum Shub* dalam proses pengamanan data audio. Pengujian yang dilakukan menggunakan data audio, namun dengan nilai seed yang berbeda pada setiap proses enkripsi.

Tabel 2. Uji Kunci

Plaintext (Audio)	Durasi Audio	Nilai Seed	Kecepatan Enkripsi	Jumlah Blok	Ukuran Ciphertext	Kecepatan Deskripsi
Audio.wav	6 Detik	Seed 1	6.8 Detik	849.730	10.68 Mb	7.8 Detik
Audio.wav	4 Detik	Seed 2	5.3 Detik	440.770	8.6 Mb	6 Detik
Audio.wav	9 Detik	Seed 3	7.2 Detik	961.480	12.3 Mb	8.9 Detik

Hasil pengujian menunjukkan perbedaan nilai seed pada algoritma *Blum Blum Shub* menghasilkan jumlah blok dan *ciphertext* yang berbeda dengan menggunakan audio secara real-time pada enkripsi. Hal ini disebabkan oleh perbedaan deret kunci acak yang dibangkitkan dari setiap seed, sehingga meningkatkan keamanan sistem yang digunakan.

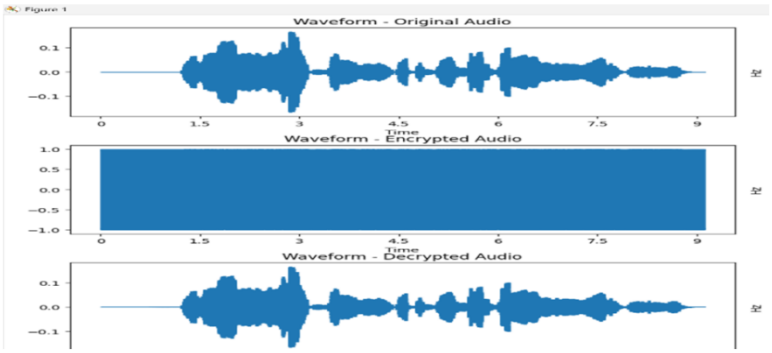


Gambar 8. Hasil Dekripsi

Berdasarkan Gambar, ditampilkan hasil proses enkripsi data audio menggunakan nilai seed 1 pada proses pembangkitan kunci. Data yang dihasilkan menunjukkan perubahan nilai dari data asli menjadi data terenkripsi yang direpresentasikan dalam bentuk nilai desimal, heksadesimal, serta biner. Perubahan nilai

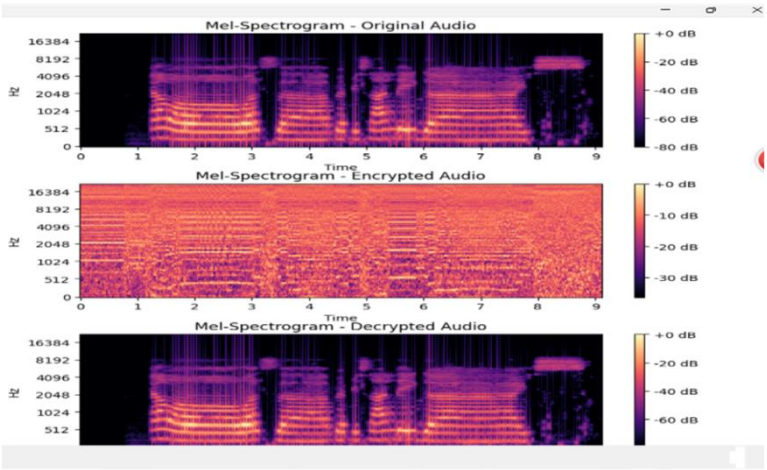
Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

tersebut menunjukkan bahwa informasi asli dari data audio telah berhasil disamarkan sehingga tidak dapat dikenali secara langsung tanpa proses dekripsi.



Gambar 9. Hasil *Wavefrom*

Tahap akhir analisis menampilkan representasi data audio dalam bentuk biner yang dihasilkan oleh sistem. Data biner ini merupakan hasil konversi setiap sampel sinyal dan menjadi dasar utama dalam proses enkripsi berbasis operasi XOR.



Gambar 10. Hasil Hasil Mel Spectogram

4. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa penerapan algoritma *Blum Blum Shub* (BBS) yang dikombinasikan dengan *Vernam Cipher* mampu digunakan secara efektif untuk mengamankan pesan suara. Proses pengamanan dilakukan melalui beberapa tahapan, yaitu perekaman suara, ekstraksi fitur menggunakan Mel-Spectrogram, konversi sinyal ke bentuk biner, pembangkitan keystream menggunakan algoritma BBS, serta proses enkripsi dan dekripsi dengan operasi XOR. Tahapan tersebut menunjukkan bahwa data suara dapat diubah menjadi ciphertext yang sulit dikenali dan tidak dapat dipahami secara langsung oleh pihak yang tidak berwenang. Hasil pengujian menunjukkan bahwa algoritma BBS mampu menghasilkan bilangan acak semu dengan tingkat keacakan yang tinggi, sehingga layak digunakan sebagai pembangkit kunci dalam sistem kriptografi. Penggunaan nilai seed yang berbeda juga menghasilkan ciphertext yang berbeda meskipun data audio yang digunakan sama, sehingga meningkatkan tingkat keamanan sistem. Selain itu, proses dekripsi berhasil mengembalikan pesan suara ke bentuk semula tanpa mengalami perubahan isi maupun kehilangan informasi yang signifikan. Dengan demikian, kombinasi algoritma *Blum Blum Shub* dan *Vernam Cipher* terbukti efektif dalam meningkatkan keamanan pesan suara, khususnya dalam menjaga kerahasiaan data audio dari risiko penyadapan, manipulasi, dan penyalahgunaan. Penelitian ini juga menunjukkan bahwa integrasi pengolahan sinyal digital dan kriptografi dapat menjadi solusi yang relevan untuk mendukung keamanan komunikasi suara di era digital saat ini.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9666

REFERENCES

[1] R. A. Purba, "Application design to help predict market demand using the waterfall method," *Matrix J. Manaj. Teknol. dan Inform.*, vol. 11, no. 3, pp. 140–149, 2021.
[2] S. A. Chic and M. F. Bilqisthi, "Tantangan dan Peluang Blockchain di Era Digital dalam Bidang Keamanan Data dan Transaksi Digital.," *J. Compr. Sci.*, vol. 3, no. 11, 2024.
[3] B. Hongcharu, "The changing roles of mass media amidst the growth of the digital media," *Cogent Soc. Sci.*, vol. 10, no. 1, p. 2297721, 2024.
[4] J. Melzner, A. Bonezzi, and T. Meyvis, "Information disclosure in the era of voice technology," *J. Mark.*, vol. 87, no. 4, pp. 491–509, 2023.
[5] S. Bormane and E. Blaus, "Artificial intelligence in the context of digital marketing communication," *Front. Commun.*, vol. 9, p. 1411226, 2024.
[6] R. Nazir *et al.*, "A review on machine learning techniques for network security," *J. Cyber Secur. Technol.*, vol. 10, no. 1, pp. 1–45, 2026.
[7] R. A. Purba, J. Sembiring, E. H. Sihombing, and S. Sondang, "Edge image detection combines Laplace operation with convolution technique to produce drawing materials for children," in *Journal of Physics: Conference Series*, 2019, vol. 1402, no. 6, doi: 10.1088/1742-6596/1402/6/066097.
[8] D. Mahmoud Boulaares and M. Boulaares, "Intercepting Voices: Voiceprint Recognition, Lawful Interception and Forensic Linguistics in Comparative Perspective," *Int. J. Semiot. Law-Revue Int. Sémiotique Jurid.*, pp. 1–20, 2025.
[9] S. Sakka, V. Liagkou, A. Ferreira, and C. Stylios, "Digital Boundaries and Consent in the Metaverse: A Comparative Review of Privacy Risks," *J. Cybersecurity Priv.*, vol. 6, no. 1, p. 24, 2026.
[10] G. Ilyassova, B. Aitimov, M. Zhumagulov, and S. Zhamburbayeva, "Ensuring Personal Data Security Using Blockchain Technology: Issues and Perspectives for Legislative Improvement," *J. Leg. Aff. Disput. Resolut. Eng. Constr.*, vol. 18, no. 1, p. 4525098, 2026.
[11] M. Alfawair, "A collaborative multi-party encryption for mitigating man-in-the-middle attacks in smart grid and energy IoT systems," *Sci. Rep.*, 2026.
[12] D. Kasimatis, W. J. Buchanan, P. Papadopoulos, and N. Pitropakis, "Secure communication and privacy-preserving techniques in edge intelligence," in *Edge Intelligence*, Elsevier, 2026, pp. 155–178.
[13] A. Martínez-Ballesté, E. Batista, E. Figueroa, K. Nouni, A. Solanas, and F. Casino, "Security and privacy in complex, context-aware systems: a comprehensive framework," *Int. J. Inf. Secur.*, vol. 25, no. 2, p. 57, 2026.
[14] M. Fadhli and R. Kurniawan, "Rancang Bangun Sistem Deteksi Audio Deepfake Menggunakan Mel-Spectrogram dan ConvNext," *J-KBDI J. Kecerdasan Buatan dan Data Sci. Ind.*, vol. 1, no. 1, pp. 12–17, 2026.
[15] M. A. N. Fadhilah, S. Adinugroho, and I. N. Sari, "Analisis Karakteristik Spectrogram dan Mel-Spectrogram dalam Merepresentasikan Fitur Akustik untuk Klasifikasi Emosi Berbasis Suara," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 3, 2026.
[16] S. F. Nabila *et al.*, "Implementasi Algoritma Caesar Cipher untuk Enkripsi dan Dekripsi Pesan," *Polyg. J. Ilmu Komput. dan Ilmu Pengetah. Alam*, vol. 4, no. 1, pp. 32–41, 2026.
[17] M. M. Cynthia, E. P. Cynthia, and D. N. Cynthia, "Perbandingan Algoritma Kriptografi Modern dalam Melindungi Data Transmisi," *J. Ilmu Komput. dan Tek. Inform.*, vol. 2, no. 1, pp. 29–35, 2026.
[18] A. Fauzi, "SUPER ENCRYPTION OF TEXT DATA USING A HYBRID BEAUFORT VIGENERE CIPHER WITH *BLUM BLUM SHUB* PSEUDORANDOM KEYS," *J. Inform. Kaputama*, vol. 10, no. 1, pp. 38–48, 2026.
[19] Y. Huang, "Corrigendum: Network detection and data security transmission based on hash and AES cryptography algorithm (2026 Eng. Res. Express 8 055207)," *Eng. Res. Express*, 2026.
[20] O. Reyad and M. E. Karar, "Secure CT-image encryption for COVID-19 infections using HBBS-based multiple key-streams," *Arab. J. Sci. Eng.*, vol. 46, no. 4, pp. 3581–3593, 2021.
[21] R. A. Purba *et al.*, *Rekayasa Perangkat Lunak Berorientasi Objek: Teori dan Implementasi*. Yayasan Kita Menulis, 2024.
[22] M. Carl, "The lost melody theorem for infinite time Blum-Shub-Smale machines," in *Conference on Computability in Europe*, 2021, pp. 71–81.