CAHAYA PELITA: JURNAL PENDIDIKAN DAN KEBUDAYAAN
Vol. 1, No. 2 (2025): 61-66, EISSN: 2998-0726
Journal Homepage: https://jurnal.cahayapublikasi.com/index.php/cp

Sistem bilangan biner, kunci utama pengkodean sebuah data dalam komputasi digital

Nurhaswinda[1], Yulanda Wulandari[2], Afrina Maiza[3], Rahmi Ramadhani[4], Novi Adelia[5]
[1,2,3,4,5]*Universitas Pahlawan Tuanku Tambusai, Indonesia*

Penulis Korespondensi: Nurhaswinda, **E-mail**: nurhaswinda01@gmail.com

Abstrak
Prinsip kerja komputer erat kaitannya dengan komponen elektronik yang saling berhubungan untuk komunikasi, transmisi, dan penyimpanan data. Dalam menjalankan prosestersebut, digunakan cara kerja pengkodean dengan dua buah simbol bilangan, yakni 0 dan 1atau yang sering disebut dengan bilangan biner. Bilangan biner merupakan dasar dari semuasistem bilangan berbasis digital. Setiap digit penyusunnya dinamakan bit, memiliki bobot kepangkatan 2 n dengan n merupakan bilangan bulat positif dan negatif. Bit digital disusunmenjadi kode seperti ASCII (American Standart Code for Information Intercharge) untuk komputer personal dan EBCDIC (Extended Binary Coded Decimal for Information) untuk komputer mainframe dan minikomputer IBM, dan Kode Boudot untuk teleprint dan teletype.Komputer tidak dapat membaca huruf-huruf seperti yang kita kenal. Oleh karena itu, mesinhanya dapat membaca pengkodean 0 dan 1 sehingga sistem bilangan biner berperan sebagai kunci utama dalam pengkodean sebuah data pada komputasi digital. bstrak memuat tujuan, metode, hasil, dan kesimpulan penelitian.

Kata Kunci
Sistem Bilangan, Biner, Kode, Data, Komputasi Digital

Naskah diterima : Januari 2025 *Naskah disetujui : Januari 2025* *Terbit : Januari 2025*

1. PENDAHULUAN

Prinsip kerja komputer erat kaitannya dengan komponen elektronik yang salingberhubungan untuk komunikasi, transmisi, dan penyimpanan data. Dalam menjalankan prosestersebut, digunakan cara kerja pengkodean dengan dua buah simbol bilangan, yakni 0 dan 1atau yang sering disebut dengan bilangan biner. Bilangan biner merupakan dasar dari semua sistem bilangan berbasis digital [1]. Ketika dua buah simbol dari bilangan biner dikombinasikan,maka akan dapat dimengerti oleh komputer serta menyebabkan komputer dapat berkomunikasidengan manusia dan dapat ditransmisikan. Maka dari itu, sistem bilangan biner atau yang juga dapat disebut dengan istilah bit atau Binary Digit merupakan unit satuan terkecil dalam suatusistem komputasi digital. pada dasarnya, komputer bekerja dengan menggunakan sistem bilangan, yang memungkinkan perangkat keras dan perangkat lunak untuk berinteraksi secara efisien. Sistem bilangan ini mencakup sistem biner (basis 2), yang menjadi dasar dari semua operasi komputasi, di mana angka-angka dan instruksi disandikan dalam bentuk dua status, yaitu 0 dan 1. Prinsip kerja komputer ini melibatkan konversi data ke dalam sistem biner, pemrosesan melalui rangkaian logika digital, dan penyimpanan serta pengambilan data dalam bentuk bilangan yang dapat dipahami oleh mesin. Pemahaman mendalam tentang sistem bilangan ini sangat penting untuk merancang, mengembangkan, dan memahami perangkat keras dan perangkat lunak komputer secara keseluruhan.

2. METODE

Analisis Algoritma Pengkodean:

Metode pertama yang digunakan adalah mempelajari dan menganalisis algoritma pengkodean yang digunakan, seperti Huffman Coding, ASCII, Unicode, atau Base64. Algoritma-algoritma ini menentukan bagaimana data diubah menjadi urutan biner yang dapat disimpan atau dikirim.
Kunci utama dalam konteks ini dapat merujuk pada teknik pengkodean tertentu yang digunakan untuk mengubah data asli menjadi format biner atau mengenkripsi data. Menurut penelitian Putra et al. (2018), optimasi pengkodean Huffman dapat meningkatkan efisiensi transmisi data dalam sistem komunikasi terbatas bandwidth, yang penting untuk meningkatkan performa jaringan dalam aplikasi berbasis cloud atau IoT (Putra, A. H., et al. (2018).

Teori Informasi:

Metode teori informasi membantu dalam menganalisis efisiensi pengkodean. Dengan menggunakan entropi dan kompresi, kita dapat mengevaluasi seberapa baik sebuah pengkodean mengurangi redundansi dan memaksimalkan penggunaan ruang untuk menyimpan data. Sebuah studi oleh Budiarto & Hartanto (2019) menunjukkan bahwa penerapan teori informasi dalam kompresi gambar menggunakan algoritma wavelet memungkinkan pengurangan ukuran file yang lebih efisien, serta meningkatkan kecepatan pengiriman data dalam sistem transmisi gambar melalui jaringan berkecepatan rendah (Budiarto, Y., & Hartanto, S. (2019).

Analisis Keamanan (Kriptografi)

Dalam konteks kriptografi, menganalisis kunci utama pengkodean data melibatkan teknik untuk mengamankan data. Kunci enkripsi (seperti dalam algoritma AES, RSA, atau ECC) digunakan untuk mengonversi data ke bentuk yang tidak dapat dibaca tanpa kunci yang benar.

Serangan Kriptografi (misalnya, serangan brute-force atau analisis frekuensi) sering digunakan untuk menguji kekuatan kunci enkripsi dengan cara mencoba menebak atau memecahkan kunci yang digunakan. Penelitian oleh Haryanto et al. (2020) menyarankan penerapan kriptografi kuantum dalam mengantisipasi kemungkinan serangan di masa depan yang dapat mengeksploitasi kelemahan dari metode enkripsi saat ini (Haryanto, A., et al. (2020).

Pengkodean Error-Correction

Dalam analisis kunci utama pengkodean data, kode koreksi kesalahan (seperti kode Hamming atau kode Reed-Solomon) digunakan untuk mengidentifikasi dan memperbaiki kesalahan yang mungkin terjadi selama pengkodean atau transmisi data. Analisis kunci dalam konteks ini berfokus pada seberapa baik kode dapat mendeteksi dan mengoreksi kesalahan. Pengkodean error-correction adalah aspek penting dalam pengelolaan kualitas data yang dikirim melalui saluran komunikasi yang rentan terhadap gangguan atau noise. Teknik-teknik seperti kode Hamming dan Reed-Solomon telah terbukti efektif dalam mendeteksi dan memperbaiki kesalahan dalam transmisi data.

Menurut Zulfiqar & Putra (2017), penerapan kode Reed-Solomon dalam sistem komunikasi satelit menunjukkan peningkatan signifikan dalam ketahanan terhadap gangguan noise, yang mengarah pada pengiriman data yang lebih handal dan bebas kesalahan (Zulfiqar, M., & Putra, A. H. (2017).

Analisis Kompleksitas Algoritma:

Untuk mengidentifikasi kunci utama dalam pengkodean data, analisis kompleksitas algoritma digunakan untuk mengevaluasi berapa banyak waktu dan sumber daya yang dibutuhkan untuk mengodekan atau mendekodekan data, serta tingkat keamanan yang disediakan oleh metode pengkodean tertentu. Penelitian oleh Suryanto et al. (2020) membahas teknik optimisasi kompleksitas dalam algoritma pengkodean untuk sistem dengan kapasitas komputasi terbatas, seperti perangkat

mobile atau sistem embedded, yang memungkinkan pengkodean dilakukan secara efisien meskipun dalam lingkungan yang penuh keterbatasan (Suryanto, T., et al. (2020).

Fungsi Hash:

Fungsi hash (misalnya, MD5, SHA-256) digunakan untuk menghasilkan nilai hash unik yang dapat bertindak sebagai kunci utama untuk data tertentu. Dalam analisis ini, kita memeriksa bagaimana data diterjemahkan menjadi nilai tetap yang menggambarkan data asli, yang juga digunakan dalam verifikasi integritas data dan pengkodean. penelitian mengemukakan jenis penelitian, alasan sebuah metode digunakan, populasi sampel/subjek, tempat dan waktu, teknik pengumpulan data, dan teknik analisis data. Penelitian kuantitatif perlu mencantumkan teknik pengujian hipotesis yang relevan. Fungsi hash berfungsi untuk menghasilkan representasi unik dari data asli, yang sering digunakan dalam verifikasi integritas data dan keamanan sistem. Hashing yang efektif, seperti dengan algoritma SHA-256, dapat memvalidasi integritas data tanpa mengungkapkan informasi asli, yang penting untuk aplikasi kriptografi dan penyimpanan data.
Menurut Indra & Kurniawan (2021), penerapan SHA-256 dalam sistem verifikasi transaksi digital memungkinkan perlindungan data dari manipulasi, sekaligus menyediakan verifikasi yang efisien dan aman dalam transaksi berbasis blockchain (Indra, S., & Kurniawan, A. (2021).

3. HASIL DAN PEMBAHASAN

Hasil dan pembahasan mengenai metode analisis algoritma pengkodean dalam teori informasi, analisis keamanan pengkodean, error correction, analisis kompleksitas algoritma, dan fungsi hash dalam sistem bilangan biner serta kunci utama pengkodean data dalam komputasi digital dapat dijelaskan sebagai berikut:

Metode Analisis Algoritma Pengkodean dalam Teori Informasi

Pengkodean dalam teori informasi bertujuan untuk menyandikan data atau informasi dalam format yang dapat disimpan, ditransmisikan, dan diproses secara efisien. Salah satu contoh pengkodean adalah pengkodean Huffman yang mengoptimalkan ruang penyimpanan dengan memberikan kode lebih pendek pada simbol yang lebih sering muncul. Dalam analisis algoritma pengkodean, kita menganalisis efisiensi ruang dan waktu dari algoritma pengkodean yang digunakan, serta seberapa baik pengkodean dapat mengurangi redundansi. Metode pengkodean dalam teori informasi semakin relevan seiring dengan meningkatnya kebutuhan penyimpanan dan transmisi data yang efisien. Algoritma pengkodean, seperti pengkodean Huffman, yang meminimalkan redundansi data, juga dapat dikombinasikan dengan algoritma kompresi data lainnya untuk meningkatkan efisiensi lebih lanjut. Penelitian terbaru oleh Sutanto et al. (2021) mengembangkan varian dari pengkodean Huffman yang lebih efisien dalam pengkodean data berbasis tekstual dan multimedia, dengan mengurangi overhead komputasi yang diperlukan dalam pemrosesan data besar (Sutanto, R. A., et al. (2021).

Analisis Keamanan Pengkodean

Keamanan pengkodean mengacu pada proteksi informasi yang dikodekan agar tidak dapat diakses atau dimodifikasi oleh pihak yang tidak berwenang. Algoritma enkripsi seperti AES (Advanced Encryption Standard) dan RSA digunakan dalam pengkodean untuk menjaga kerahasiaan data. Analisis keamanan ini berfokus pada ketahanan algoritma terhadap serangan kriptografi, seperti serangan brute force, serangan analisis statistik, dan serangan man-in-the-middle. Kekuatan kunci enkripsi dan panjang kunci sangat menentukan tingkat keamanan dari sistem pengkodean. Keamanan dalam pengkodean sangat bergantung pada kualitas algoritma enkripsi dan pengelolaan kunci. Dalam beberapa penelitian, kriptografi kuantum mulai dipertimbangkan sebagai alternatif dalam menghadapi potensi ancaman dari komputer kuantum terhadap algoritma kriptografi klasik. Rahman et al. (2017) menyarankan bahwa untuk memastikan keamanan jangka panjang, sistem

enkripsi harus adaptif terhadap kemajuan teknologi seperti kriptografi berbasis matriks dan protokol quantum key distribution (Rahman, S. H., et al. (2017).

Error Correction dalam Pengkodean

Dalam transmisi data atau penyimpanan informasi, kesalahan dapat terjadi karena gangguan sinyal atau kerusakan media. Error correction adalah teknik yang digunakan untuk mendeteksi dan mengoreksi kesalahan tersebut. Contoh teknik error correction termasuk kode Hamming dan kode Reed-Solomon. Kode Hamming memungkinkan deteksi dan koreksi kesalahan bit tunggal, sedangkan Reed-Solomon digunakan untuk koreksi kesalahan pada blok data yang lebih besar, misalnya dalam pengkodean CD/DVD atau komunikasi satelit. Teknik koreksi kesalahan memainkan peranan krusial dalam menjaga integritas data yang ditransmisikan. Dalam situasi yang lebih kompleks, seperti komunikasi satelit atau jaringan nirkabel, penggunaan kode koreksi kesalahan seperti Turbo Codes dan LDPC (Low-Density Parity Check) menunjukkan hasil yang lebih baik dibandingkan dengan kode tradisional dalam memperbaiki kesalahan bit dalam blok data besar. Menurut Wahyudi et al. (2019), penggunaan LDPC memberikan peningkatan signifikan dalam efisiensi koreksi kesalahan dengan mengurangi kesalahan bit di saluran komunikasi yang terdegradasi (Wahyudi, H., et al. (2019).

Analisis Kompleksitas Algoritma

Analisis kompleksitas algoritma bertujuan untuk mengukur efisiensi suatu algoritma dalam hal waktu (time complexity) dan ruang (space complexity). Dalam konteks pengkodean, kita mengukur seberapa cepat algoritma dapat mengkodekan dan mendekodekan data, serta seberapa banyak sumber daya (seperti memori) yang diperlukan. Misalnya, pengkodean Huffman memiliki kompleksitas waktu O(n log n) untuk membangun pohon Huffman, sementara enkripsi RSA dapat memerlukan waktu eksponensial tergantung pada panjang kunci. Analisis kompleksitas algoritma menjadi sangat penting dalam memilih metode pengkodean yang efisien. Dalam penelitian oleh Ibrahim dan Aziz (2020), diperkenalkan teknik optimisasi untuk algoritma pengkodean Huffman yang mengurangi waktu komputasi dengan menggunakan teknik parallel processing, yang dapat mempercepat proses pengkodean dan dekode data secara signifikan dalam sistem dengan sumber daya terbatas (Ibrahim, F., & Aziz, A. (2020).

Fungsi Hash dalam Pengkodean dan Keamanan

Fungsi hash adalah algoritma yang mengubah input data menjadi nilai hash tetap yang unik. Fungsi hash digunakan dalam berbagai aplikasi, seperti dalam integritas data (misalnya, checksum) dan kriptografi (misalnya, dalam penandatanganan digital atau verifikasi pesan). Fungsi hash yang baik harus memenuhi sifat deterministik, cepat dihitung, dan memiliki collision resistance (sulit untuk menemukan dua input yang menghasilkan nilai hash yang sama). Contoh fungsi hash yang sering digunakan adalah MD5, SHA-1, dan SHA-256. Fungsi hash menjadi komponen utama dalam memastikan integritas data dan autentikasi sistem dalam berbagai aplikasi digital. Fungsi hash yang memiliki sifat collision resistance menjadi syarat mutlak dalam kriptografi untuk mencegah potensi penyusupan. Penelitian oleh Fauzi et al. (2018) menunjukkan bahwa fungsi hash berbasis SHA-256 memberikan perlindungan yang lebih baik dibandingkan dengan MD5 atau SHA-1 dalam mengidentifikasi perubahan data yang tidak sah (Fauzi, N., et al. (2018).

Kasus Sistem Bilangan Biner dan Kunci Utama Pengkodean

Dalam komputasi digital, semua data dikodekan dalam sistem bilangan biner, yang hanya menggunakan dua simbol (0 dan 1). Pengkodean dalam sistem biner memanfaatkan bit untuk mewakili data. Kunci utama dalam pengkodean adalah pengelolaan kunci dalam sistem enkripsi untuk memastikan data tetap aman. Kunci simetris dan kunci publik-privat merupakan dua pendekatan utama dalam pengelolaan kunci enkripsi. harus diberi nomor sesuai dengan urutan penyajiannya (mis. Tabel 1. dll.). Tabel hanya berisi garis untuk baris tanpa garis kolom, sumber tabel ditulis di

bawah tabel, sedangkan nomor dan judul tabel ditulis di atas tabel, rata tengah. Sistem bilangan biner adalah dasar dari semua komputasi digital, dan pengelolaan kunci enkripsi memainkan peranan penting dalam memastikan data tetap aman dari potensi penyusupan. Dalam konteks pengkodean data dan manajemen kunci, penelitian oleh Setiawan et al. (2020) menekankan pentingnya menggunakan sistem bilangan biner dalam pengkodean kunci simetris dan publik-privat untuk memastikan efisiensi dan ketahanan terhadap serangan. Selain itu, teknik seperti key exchange protocols, yang digunakan dalam pengelolaan kunci publik-privat, menawarkan solusi tambahan dalam menjaga integritas komunikasi digital (Setiawan, D., et al. (2020).

4. SIMPULAN

Berdasarkan penjelasan di atas, maka dapat disimpulkan bahwa pada system komputasi digital menggunakan operasi bilangan biner yang terdiri atas nilai 0 dan 1. Bilangan biner dipopulerkan oleh John Von Neumann. Setiap digit penyusunnya dinamakan bit, memilikibobot kepangkatan 2n dengan n merupakan bilangan bulat positif dan negatif. Komputer dapatberkomunikasi dengan adanya penggunaan sinyal digital atau bit yang berupa bilangan biner.Bit digital tersebut disusun menjadi kode seperti ASCII (American Standart Code for InformationIntercharge) untuk komputer personal dan EBCDIC (Extended Binary Coded Decimal for Information) untuk komputer mainframe dan minikomputer IBM, dan Kode Boudot untuk teleprint dan teletype. Komputer tidak dapat membaca huruf-huruf seperti yang kita kenal. Oleh karena itu, mesin hanya dapat membaca pengkodean 0 dan 1 sehingga sistem bilangan biner berperan sebagai kunci utama dalam pengkodean sebuah data pada komputasi digital. Analisis algoritma pengkodean, keamanan pengkodean, error correction, dan kompleksitas algoritma sangat penting dalam memastikan integritas, efisiensi, dan keamanan dalam sistem komputasi digital. Fungsi hash dan penggunaan kunci dalam pengkodean membantu menjaga keaslian dan kerahasiaan data dalam berbagai aplikasi, termasuk komunikasi dan penyimpanan data.

Adapun salah satu rekomendasi yang dapat diberikan oleh penulisan untuk penelitian berikutnya adalah pengembangan algoritma pengkodean yang lebih efisien dan aman, serta penerapan teknik kriptografi untuk menjaga kerahasiaan dan integritas data. Selain itu, penelitian mengenai koreksi kesalahan dalam pengkodean juga perlu diperluas, untuk menangani masalah kesalahan dalam komunikasi data yang lebih kompleks, seperti dalam jaringan IoT atau 5G. Penggunaan fungsi hash yang lebih optimal untuk memastikan keaslian data juga menjadi area yang menarik untuk diteliti lebih lanjut. Di sisi lain, penelitian dapat berfokus pada pengembangan algoritma pengkodean yang lebih efisien bagi perangkat dengan sumber daya terbatas, serta analisis kompleksitas algoritma untuk meningkatkan kinerja sistem tanpa mengurangi keamanan. Terakhir, dengan kemajuan teknologi komputasi kuantum, penting untuk menjelajahi pengkodean dan enkripsi yang mampu melindungi data dari ancaman baru yang ditimbulkan oleh komputasi kuantum. Penelitian-penelitian ini dapat membantu menciptakan solusi yang lebih aman, efisien, dan andal di dunia komputasi digital yang terus berkembang.

PUSTAKA ACUAN

A.H., Ghuswari, Augmented Reality Pembelajaran Konversi Bilangan Biner ke Desimal danPerhitungan Subnetting, Bandung: UIN Sunan Gunung Djati; 2021.

Aho, A.V., Lam, M.S., & Sethi, R. (2006). Compilers: Principles, Techniques, and Tools. Addison-Wesley.

Budiarto, Y., & Hartanto, S. (2019). "Data compression based on wavelet transform for efficient image transmission", Jurnal Sistem Informasi.

Cormen, T.H., Leiserson, C.E., Rivest, R.L., & Stein, C. (2009). Introduction to Algorithms (3rd ed.). MIT Press.

Dr. Muchlas, M.T. Buku Ajar Teknik Digital, Yogyakarta: Muchlas, 2020, 10-12.

Fauzi, N., et al. (2018). "Comparative analysis of hash functions for data integrity in digital transactions", Jurnal Teknologi dan Kriptografi.

Haryanto, A., et al. (2020). "Quantum cryptography: A new paradigm for future secure communication systems", Jurnal Keamanan dan Teknologi.

Hennessy, J.L., & Patterson, D.A. (2011). Computer Architecture: A Quantitative Approach (5th ed.). Morgan Kaufmann.

Ibrahim, F., & Aziz, A. (2020). "Optimization of Huffman coding using parallel computing techniques", Jurnal Informatika.

Indra, S., & Kurniawan, A. (2021). "SHA-256 for secure digital transaction verification in blockchain technology", Jurnal Keamanan Informasi.

Knuth, D.E. (1968). The Art of Computer Programming, Volume 1: Fundamental Algorithms. Addison-Wesley.

Lestari, Muji. Pengkodean Data, Jakarta: Universitas Guna Darma; 2020.

Millington T. Alaric.1971.Dictionary of Mathematics. Barners & Noble Books A Division of Harper& Row Publisher

Mills, D. (2000). The Art of Digital Design. Prentice Hall.

Nurdin.Mochamad.Et.All.1996. Matematika 1a dan 1b untuk SLTP Kelas 1 Kurikulum 1994.Bandung: PT Remaja Rosdakarya.

Putra, A. H., et al. (2018). "Optimizing Huffman coding for data transmission efficiency in IoT-based networks", Jurnal Teknologi Informasi.

Rahman, S. H., et al. (2017). "Quantum encryption systems: A new frontier in data security", Jurnal Kriptografi dan Keamanan Sistem.

Scottish Mathematics Group. 1992.Modern Mathematics for School.London:Blackie & Son Ltd.

Setiawan, D., et al. (2020). "Key management in symmetric and asymmetric encryption systems", Jurnal Keamanan dan Komputasi.

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice (7th ed.). Pearson Education.

Suryanto, T., et al. (2020). "Optimizing algorithm complexity for embedded systems in data compression", Jurnal Teknologi Embedded.

Sutanto, R. A., et al. (2021). "Optimizing Huffman coding for large-scale multimedia data transmission", Jurnal Teknologi Informasi.

Tanenbaum, A.S. (2011). Computer Networks (5th ed.). Pearson

Wahyudi, H., et al. (2019). "Improved error correction with LDPC codes for noisy communication channels", Jurnal Telekomunikasi dan Komunikasi Digital.

Zulfiqar, M., & Putra, A. H. (2017). "Reed-Solomon error correction for satellite communication systems", Jurnal Teknologi Komunikasi.