Criptografia Bioinspirada para IoT: Um Estudo Comparativo de Algoritmos Baseados em DNA

Mikael M. F. Sales
mikaelmfsales@gmail.com
Universidade Federal do Ceará

J. C. Aguiar Junior
aguiar.research@gmail.com
Universidade Federal do Ceará

A. Wictor Pereira de Sousa
wictorsousa@alu.ufc.br
Universidade Federal do Ceará

João Marcelo Gomes
joaomarcelgomes@alu.ufc.br
Universidade Federal do Ceará

Emerson B. Tomaz
emerson@crateus.ufc.br
Universidade Federal do Ceará

Filipe de Matos
filipe.fernandes@crateus.ufc.br
Universidade Federal do Ceará

ABSTRACT

Data security in Internet of Things (IoT) devices is a critical challenge due to their inherent limitations in memory, energy, and processing capacity. Traditional security mechanisms are often unfeasible, driving the search for lightweight cryptographic algorithms. In this context, DNA-based cryptography stands out as a promising bioinspired approach. This study presents an empirical and direct comparison of four DNA-based cryptographic algorithms, implemented on a real resource-constrained IoT device, the ESP8266. The analysis quantified performance and efficiency in both encryption and decryption modes, using instrumented measurements of energy consumption (mJ), execution time (μs), electric current (mA), and RAM usage (B). The results reveal statistically significant differences among the algorithms, confirmed by Shapiro-Wilk and Wilcoxon tests. Alg_3 demonstrated the highest efficiency in time and energy, being the fastest and with the lowest total energy consumption, although it required the most RAM. The research highlights the potential of bioinspired cryptography and reinforces the importance of considering the constraints of the target environment when selecting a cryptographic scheme.

PALAVRAS-CHAVE

Análise comparativa, Criptografia, DNA, Internet das Coisas, Sistemas Embarcados.

1 INTRODUÇÃO

A Internet das Coisas (IoT) é um paradigma tecnológico que descreve um sistema de dispositivos computacionais, equipados com sensores, atuadores ou ambos, que se conectam entre si e à Internet para coletar, trocar e processar dados de forma autônoma, permitindo a automação e a integração entre os mundos físico e digital [14, 21]. A IoT está transformando setores sociais ao conectar os mais diversos dispositivos à Internet, coletar dados em tempo real e automatizar processos. As principais oportunidades e aplicações estão em cidades inteligentes [37], transporte [24], saúde [39], agricultura [3] e educação [4].

No entanto, apesar desses avanços, há um desafio relevante quanto à segurança dos dados processados e transmitidos nesses sistemas, uma vez que muitos desses dispositivos são projetados com recursos computacionais limitados [15]. Essas limitações de memória, energia e capacidade de processamento dificultam a implementação de mecanismos de segurança tradicionais e impulsionam a necessidade de desenvolver e adotar algoritmos criptográficos leves, compatíveis com os recursos restritos dos dispositivos IoT [10].

Diante desse cenário, torna-se essencial empregar soluções que equilibrem segurança e eficiência operacional. Entre essas soluções, ganha destaque a criptografia baseada em DNA, uma abordagem bioinspirada, que utiliza os princípios do código genético para realizar operações criptográficas [16]. Algoritmos criptográficos baseados em DNA são projetados para exigir menos processamento, memória e energia, tornando-os mais adequados para dispositivos IoT, sem comprometer a segurança dos dados [18]. Tais algoritmos buscam atender aos principais requisitos de segurança em ambientes restritos, como confidencialidade, integridade e autenticidade.

Nos criptossistemas baseados em DNA, os dados digitais são codificados utilizando as bases do DNA: **`Adenina (A)`**, **`Guanina (G)`**, **`Citosina (C)`** e **`Timina (T)`**. Essas bases são empregadas para codificar dados binários, com cada base de DNA correspondendo a uma sequência específica de bits. Essa abordagem permite a conversão de dados binários em cadeias simbólicas inspiradas no DNA, resultando em representações compactas e de alta densidade informacional [17].

Apesar dessas características promissoras, a literatura permanece fragmentada no que se refere à mensuração comparável: estudos em microcontroladores costumam relatar tempo e memória, enquanto o consumo de energia é frequentemente estimado, sem medição instrumentada [38]. Além disso, são raras as comparações diretas entre múltiplos algoritmos de DNA na mesma plataforma de IoT. O mais frequente é encontrar estudos que comparam algoritmos de DNA com cifradores clássicos, como AES e RC4 [1], o que reduz a comparabilidade intrínseca e prejudica a escolha do algoritmo alternativo mais viável para implementação prática em dispositivos reais.

Diante desse cenário, este trabalho tem como objetivo realizar uma comparação direta, em uma mesma plataforma de IoT, entre os principais algoritmos de criptografia baseados em DNA, quantificando tempo de processamento, uso de memória e consumo de energia, a fim de identificar o algoritmo mais eficiente para esse contexto.

A contribuição deste estudo está em oferecer um conjunto de evidências empíricas, obtidas sob condições controladas e reprodutíveis, que auxiliam na avaliação da viabilidade de algoritmos de

In: Proceedings of the Brazilian Symposium on Multimedia and the Web (WebMedia'2025). Rio de Janeiro, Brazil. Porto Alegre: Brazilian Computer Society, 2025.

ISSN 2966-2753

DNA em dispositivos com recursos limitados. Ao avaliar o desempenho dos algoritmos segundo métricas observacionais comumente utilizadas em pesquisas experimentais sobre criptografia para IoT, busca-se diminuir incertezas presentes na literatura e ampliar as condições para aplicação prática desses esquemas em ambientes reais.

2 FUNDAMENTAÇÃO TEÓRICA

Esta seção apresenta os conceitos e técnicas essenciais para a compreensão da pesquisa, com foco em fundamentos diretamente relacionados à criptografia baseada em DNA e ao contexto de sua aplicação em dispositivos IoT.

2.1 Criptografia baseada DNA

A criptografia baseada em DNA oferece um método seguro e eficiente para cifração de grandes mensagens em volume compacto, aumentando a segurança dos dados e a privacidade da comunicação [20]. Inspirada na biologia molecular, essa abordagem utiliza as propriedades das sequências de DNA, compostas pelas bases `A`, `C`, `G` e `T`, como meio de codificação e transformação de dados digitais.

O processo tem início com a binarização dos dados (texto, imagem, vídeo ou sinal), seguida da conversão de pares de bits em bases de DNA, adotando-se `00` para `A`, `01` para `C`, `10` para `G` e `11` para `T` [23]. Em seguida, são aplicadas operações genéticas como remodelação, *crossover* e mutação. A criptografia utiliza uma chave binária ou codificada em base de DNA para executar uma operação `XOR` com os dados. A remodelação organiza as sequências em estruturas semelhantes a cromossomos. O *crossover* realiza trocas entre segmentos dessas estruturas, e a mutação altera bits ou bases para aumentar a imprevisibilidade.

A mutação pode ocorrer de duas maneiras: Mutação de Complemento e Mutação de Substituição [23]. Ambas as mutações estão exemplificadas na Figura 1. Há uma fase Pré-Mutação, que lida com a sequência de bases de DNA resultante do *crossover*, convertendo-a em uma sequência de bits. Após a conclusão da Pré-Mutação, uma das estratégias de mutação é executada. Na Mutação de Complemento, dentro de um intervalo, cada bit é substituído pelo seu complementar. Na Mutação de Substituição, a sequência de bits é convertida em bases de DNA, de forma que, dentro de um intervalo, a cada quatro bits, tais bits são convertidos em duas bases de DNA (seguindo, por exemplo, o mapeamento da Tabela 1). Após a conversão em base de DNA, é aplicado algum mapeamento, por exemplo: `G` para `A`, `A` para `G`, `C` para `T` e `T` para `C`. Em caso de mutação, o processo inverso se dá aplicando em ordem reversa os passos da estratégia de mutação abordada na cifração.

DNA	Bits	DNA	Bits	DNA	Bits	DNA	Bits
TA	0000	GA	0100	CA	1000	AA	1100
TC	0001	GC	0101	CC	1001	AC	1101
TG	0010	GG	0110	CG	1010	AG	1110
TT	0011	GT	0111	CT	1011	AT	1111

Tabela 1: Bases de DNA e Representação de Bits[1]

[1]Adaptado de Mousa (2016)

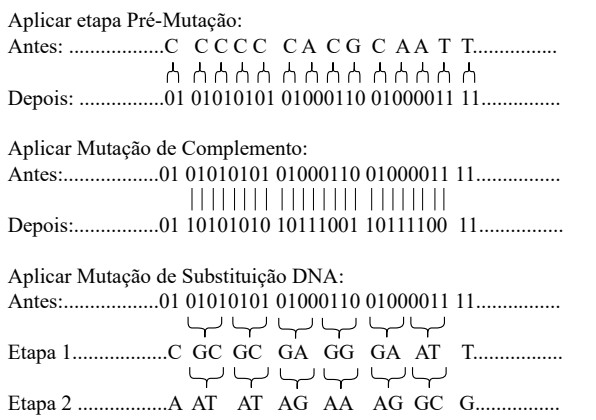

Figura 1: Exemplos de mutação

A complexidade estrutural do DNA e das operações biológicas associadas aumentam a segurança destes criptossistemas, dificultando sua quebra [28, 31]. Além disso, a criptografia baseada em DNA apresenta vantagens como paralelismo computacional intrínseco e baixo consumo de energia [28], o que a torna adequada para aplicações em dispositivos com recursos limitados.

2.2 Algoritmos adotados para a comparação

Para realizar a análise comparativa proposta neste estudo, foram selecionados quatro algoritmos de cifração baseados em DNA descritos na literatura. Os critérios de seleção encontram-se detalhados na Seção 4.1. A seguir, serão descritas as principais características de cada algoritmo, com ênfase nos mecanismos utilizados, complexidade computacional e técnicas de segurança adotadas.

2.2.1 ***A novel cryptosystem based on DNA cryptography, hyperchaotic systems and a randomly generated Moore machine for cyber physical systems.*** Pavithran et al. (2022) apresentaram um modelo de criptossistema desenvolvido para *Cyber-Physical Systems* (CPS). O esquema combina técnicas de criptografia baseadas em DNA e dinâmicas hipercaóticas de uma Máquina de Moore gerada aleatoriamente, com o objetivo de ampliar a aleatoriedade do texto cifrado e otimizar a complexidade computacional.

O funcionamento do esquema se apoia em três fundamentos principais:

- Transformação dos dados em cadeias de DNA, utilizando codificação binária de dois bits por base (`00` para `A`, `01` para `C`, `10` para `G`, `11` para `T`). Nessa etapa, são empregadas regras dinâmicas definidas pelos oito bits iniciais do dado para aumentar a difusão, propriedade pela qual pequenas alterações no texto claro provocam mudanças significativas e distribuídas no texto cifrado, dificultando a identificação de padrões que possam ser explorados em ataques.
- Geração de sequências pseudoaleatórias por meio do sistema hipercaótico de Rössler em quatro dimensões, um modelo matemático sensível às condições iniciais e capaz de produzir

valores numéricos altamente imprevisíveis. Esses valores são normalizados e convertidos em binário, que por sua vez é mapeado para bases de DNA (`A`, `C`, `G`, `T`), formando cadeias de bases que intensificam a difusão.

- Substituições nas cadeias de bases de DNA são realizadas por meio de uma Máquina de Moore, cuja tabela de transições é definida de forma pseudoaleatória. Nesse tipo de autômato finito, cada estado corresponde a uma base de DNA. A ordem de percurso entre os estados, definida pelas regras da tabela de transições, determina as substituições aplicadas. Esse processo cria padrões complexos e não determinísticos que aumentam a confusão e dificultam a dedução da mensagem original sem o conhecimento das regras de substituição. Na criptografia clássica, a técnica de substituição consiste em trocar cada símbolo do texto claro por outro símbolo de acordo com uma regra definida. No método descrito por Pavithran et al. (2022), o princípio é o mesmo: cada base de DNA na cadeia é substituída por outra, segundo as regras definidas na tabela de transições da Máquina de Moore. Assim como nas cifras clássicas, o objetivo é aumentar a confusão e dificultar a dedução da mensagem original sem o conhecimento da chave ou das regras de substituição. A confusão é a propriedade que visa dificultar a identificação da relação entre o texto cifrado e a chave, tornando mais complexa a dedução da chave ou do conteúdo original. No método descrito por Pavithran et al. (2022), esse papel é desempenhado pela tabela de transições da Máquina de Moore, que define as substituições aplicadas às bases de DNA e cuja estrutura deve permanecer desconhecida para garantir a segurança do sistema.

O sistema incorpora também um *Key Pair Generator* (KPG) para distribuição de chaves assimétricas, garantindo a comunicação segura dos parâmetros iniciais do sistema hipercaótico de Rössler e dos demais elementos necessários para que o receptor reproduza o processo para a decifração.

Os testes revelam um espaço de chaves de 2^{195} e efeito avalanche médio de 54,75%, assegurando elevada resistência frente a ataques, incluindo *man-in-the-middle*, *ciphertext-only*, *known-plaintext*, força bruta e criptoanálise diferencial. Destacam-se ainda a complexidade linear ($O(n)$), tempos de processamento reduzidos e distribuição estatística uniforme das bases DNA. O método supera limitações identificadas em abordagens anteriores, como alto custo computacional, uso de cadeias curtas e vulnerabilidades a correlações.

Na implementação, replicaram-se integralmente os procedimentos indicados no artigo, incluindo a geração das variáveis hipercaóticas por meio do sistema Rossler, determinação da Regra de codificação de DNA (DCR) a partir do tempo do sistema e construção da Máquina de Moore de maneira pseudoaleatória.

2.2.2 ***An efficient environmental monitoring data encryption algorithm based on DNA coding and hyperchaotic system***.

Conforme Taamté et al. (2022), o trabalho descreve um esquema de criptografia que integra codificação DNA, sistemas hipercaóticos e uma Máquina de Moore dinâmica, voltado à proteção de informações em sistemas de monitoramento ambiental.

O algoritmo opera aplicando regras dinâmicas de DNA, operações `XOR`, adição, subtração e sequências pseudoaleatórias oriundas de um sistema hipercaótico de quarta ordem. A Máquina de Moore gerada de forma pseudoaleatória, executa substituições sobre cadeias de DNA, reduzindo padrões previsíveis. A implementação foi realizada em Java (*Eclipse IDE*) sob ambiente Ubuntu 20.04, processador Intel i5 e 4GB de RAM, com utilização do *dataset 20 Newsgroups*. Os parâmetros empregados foram $a = 36$, $b = 3$, $c = 28$, $k = -16$ e $\mu = 0.5$, além das variáveis iniciais derivadas da soma dos valores ASCII do texto claro. A construção da Máquina de Moore baseou-se na tabela de transição convertida em binário e, posteriormente, em DNA, obedecendo a uma regra selecionada de forma pseudoaleatória.

O modelo atinge espaço de chaves de 2^{195} e efeito avalanche de 54,75%, mantendo distribuição estatística uniforme e baixíssima correlação. A complexidade é linear ($O(n)$), e os tempos de execução são inferiores aos registrados em esquemas anteriores. Observa-se resistência sólida contra ataques como força bruta, *ciphertext-only*, *known-plaintext*, *man-in-the-middle* e criptoanálise diferencial.

Na aplicação prática, adotaram-se os parâmetros exatos descritos no artigo, incluindo a geração das variáveis iniciais a partir da soma dos valores ASCII, além da construção da Máquina de Moore conforme a metodologia apresentada.

2.2.3 ***DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography***.

No artigo, Singh et al. (2024b) propuseram um esquema criptográfico para segurança de dados em ambientes de nuvem baseados em internet de todas as coisas (*Internet of Everything - IoE*), combinando codificação DNA, dinâmicas hipercaóticas e uma Máquina de Moore de configuração pseudoaleatória. O processo faz uso de regras dinâmicas de DNA, operações `XOR`, adição, subtração e sequências geradas a partir de um sistema hipercaótico de quarta ordem. A Máquina de Moore, construída aleatoriamente para cada operação, executa substituições nas cadeias DNA, eliminando padrões previsíveis.

O sistema é constituído por três agentes: *Key-Pair Generator* (KPG), que gera e distribui chaves públicas e privadas; *Data Owner* (DO), que realiza a cifração; e *Data User* (DU), responsável pela decifração. A comunicação é protegida via SSL. O fluxo de cifração inclui: geração da Máquina de Moore codificada em DNA, produção das sequências caóticas, operações sobre DNA (*scramble*, `XOR`, adição, subtração, nova `XOR`, substituição por Moore e complementação de bases). Dados e parâmetros são cifrados com chaves assimétricas e transmitidos ao receptor.

Na implementação, seguiram-se os parâmetros públicos p e g apresentados no artigo, além da geração dos exponenciais aleatórios segundo o protocolo StS KAP, mantendo a fidelidade aos procedimentos descritos.

2.2.4 ***Image encryption based on 2DNA encoding and chaotic 2D logistic map***.

Alrubaie et al. (2023) em seu estudo apresenta o algoritmo *2DNALM*, que combina codificação dupla em DNA com um mapa logístico bidimensional de comportamento caótico, direcionado à proteção de imagens digitais.

A metodologia contempla três etapas: embaralhamento dos pixels via chave caótica, dupla codificação dos canais RGB em DNA mediante regras distintas e cifração das cadeias DNA com operações `DNA-XOR` e duas sequências caóticas derivadas do mapa logístico 2D, parametrizado com $r = 1.19$, $x_0 = 0.8909$ e $y_0 = 0.3342$. As chaves são aplicadas separadamente sobre linhas pares e ímpares.

A decifração consiste na execução inversa deste processo. Os testes indicam elevada sensibilidade à chave, onde qualquer pequena alteração compromete a decifração. A entropia aproxima-se de 8, comprovando resistência contra análise estatística. Os índices NPCR (acima de 99,5%) e UACI (em torno de 33%) confirmam a robustez contra ataques diferenciais.

As imagens cifradas exibem histogramas com distribuição estatística uniforme. Métricas como MSE elevado e PSNR reduzido refletem alta distorção, característica desejável em esquemas de cifração. Os coeficientes de correlação, originalmente entre 0.90 e 0.95 nas imagens não cifradas, reduzem-se a quase zero nas imagens protegidas. O tempo médio de processamento varia de 6 a 8 segundos para imagens RGB de 256×256, em hardware com processador Core i7 (2.20 GHz) e 8GB de RAM, demonstrando alta eficiência. O algoritmo confirma robustez contra ataques estatísticos, força bruta e criptoanálise diferencial.

Na implementação, foram adotados os parâmetros $r = 1.19$, $x_0 = 0.8909$ e $y_0 = 0.3342$. A codificação DNA seguiu a Regra 1 na primeira etapa e as Regras 3, 5 e 8 para os canais R, G e B, respectivamente, replicando o procedimento estabelecido no artigo.

2.3 Análise de componentes principais

A Análise de Componentes Principais (PCA) é uma técnica de estatística utilizada para reduzir a dimensionalidade de dados multivalorados, preservando a maior quantidade possível de variância. Proposta inicialmente Karl Pearson em 1901, a PCA consiste em encontrar um subespaço de dimensão k que melhor aproxime os dados, minimizando o erro de reconstrução normalmente medido pela norma de Forbrenius mínima ou a norma espectral mínima do erro de aproximação da matriz de dados [34]. Essa abordagem projeta dados em componentes principais ortogonais obtidos via decomposição espectral da matriz de covariância, resultando em uma representação compacta com menor erro quadrático médio [36]. A PCA é amplamente aplicada como etapa pré-processamento em tarefas de aprendizado de máquina, compressão e análise exploratória de dados.

2.4 Teste de classificação sinalizada de Wilcoxon

Segundo Benavoli et al. (2014) , o teste de Wilcoxon com postos sinalizados é um método estatístico não paramétrico utilizado para determinar se há uma diferença significativa entre duas amostras pareadas, especialmente quando a suposição de normalidade não é válida. O teste baseia-se nos sinais e nas magnitudes das diferenças entre observações pareadas. Ao final do processo de validação cruzada, esse teste é aplicado às métricas coletadas em cada partição para comparar o desempenho dos modelos. Para cada par de modelos e cada métrica, calcula-se a estatística de Wilcoxon e seu p-valor utilizando os valores pareados, e os resultados são armazenados em uma tabela indicando se a hipótese nula foi rejeitada. Essa abordagem fornece uma avaliação não paramétrica das diferenças significativas de desempenho.

2.5 Teste de Shapiro-Wilk

De acordo com Mishra et al. (2019), o teste de Shapiro-Wilk é utilizado para verificar se um conjunto de dados segue uma distribuição normal. A estatística calculada, representada por W, considera a associação entre os dados organizados em ordem crescente e os quantis teóricos de uma distribuição normal padrão. Quando o valor de W se aproxima de 1, entende-se que os dados não apresentam desvios significativos da normalidade. Por outro lado, valores mais baixos sugerem a presença de assimetrias ou outros padrões que destoam da distribuição normal.

3 TRABALHOS RELACIONADOS

Os trabalhos correlatos foram selecionados por busca sistemática nas bases IEEE Xplore, ACM Digital Library, SpringerLink e ScienceDirect, utilizando a *string* ("*DNA encryption*" OR "*DNA cryptography*") AND ("*comparison*" OR "*performance analysis*" OR "*benchmarking*") AND ("*embedded systems*" OR "*IoT devices*" OR "*embedded devices*"). A busca retornou 97 artigos, dos quais 7 foram selecionados após filtragem por duplicatas, leitura de títulos, resumos e análise técnica. Os critérios aplicados foram criptografia com base no DNA, aplicações com foco em dispositivos IoT ou dispositivos embarcados, apresentação de resultados quantitativos como consumo de memória e tempo de execução, e sensibilidade a variações de chave.

Qaid and Ebrahim (2023) propuseram um algoritmo leve de criptografia baseado em computação de DNA, utilizando operações de substituição e transposição. Os experimentos realizados envolveram testes de eficiência com arquivos de texto e imagem em dispositivos simulados com restrições de hardware. Os resultados demonstraram que o algoritmo alcança menor tempo de cifração, menor uso de memória e alta resistência contra ataques de análise diferencial. O tempo médio de cifração e decifração foi de 0,067 segundos, o uso de memória foi de 1182 *bytes*, e a entropia dos dados cifrados alcançou 7,9972 *bits/pixel*, indicando forte aleatoriedade. Concluiu-se que a proposta é eficaz para ambientes IoT, combinando segurança e leveza computacional, destacando-se pela simplicidade e baixo custo computacional, embora ainda não tenha sido validada em dispositivos físicos ou redes em larga escala.

Sasikumar and Nagarajan (2024) fizeram uma revisão abrangente de técnicas criptográficas em nuvem, incluindo DNA, criptografia de curvas elípticas (em inglês, Elliptic curve cryptography - ECC), homomórfica e híbrida. Entre os experimentos, foram comparados algoritmos quanto ao uso de energia, tempo de resposta, complexidade algorítmica e resistência a ataques. O estudo destaca que técnicas baseadas em DNA e curvas elípticas oferecem boa escalabilidade e segurança, sendo recomendadas para sistemas em nuvem e IoT. A partir da síntese das técnicas criptográficas e do mapeamento das suas aplicações ideias, os autores concluíram que uma abordagem híbrida é uma solução promissora para equilibrar desempenho e segurança, embora sua complexidade possa dificultar a adoção em dispositivos com recursos muito limitados.

Abdelaal et al. (2025b) propuseram um algoritmo híbrido de criptografia leve baseado em DNA e computação óptica, voltado à cifração de imagens em dispositivos como o Arduino R3. Os experimentos incluíram análise de tempo de execução, uso de memória e resistência a criptoanálise. O algoritmo alcançou um tempo médio de cifração de 3956 μs, com uso de apenas 773 *bytes* de memória, superando AES e XOR em desempenho. Concluiu-se que a abordagem é ideal para aplicações críticas em monitoramento médico e

segurança nuclear, embora dependa de operações ópticas difíceis de integrar a dispositivos comerciais comuns.

Imdad et al. (2024) desenvolveram o algoritmo DNA-PRESENT, que combina o algoritmo PRESENT com técnicas de replicação de DNA. Os experimentos envolveram a análise de difusão, sensibilidade à chave e taxa de erro. Os resultados mostraram aumento da sensibilidade à chave em 73,57%, com média de 50,2% de alteração nos *bits* para pequenas mudanças na entrada. O tempo de execução foi reduzido em 0,2333s, com *throughput* de 176,47 kb/s. Os autores concluíram que a adição do DNA ao PRESENT melhora tanto a segurança quanto o desempenho, com um aumento de custo computacional aceitável (33,5%), embora ainda necessite de validação prática em redes reais de IoT.

Aqeel et al. (2025) propuseram o DNA-LWCS, sistema leve que combina chaves derivadas de sequências DNA públicas com ECC. Os experimentos focaram em eficiência e segurança em dispositivos IoT com baixo poder computacional. A avaliação demonstrou melhor desempenho em tempo e uso de recursos quando comparado com AES, 3DES e ECC puro. O DNA-LWCS apresentou uma correlação $\leq 0{,}05$ em dois dos três conjuntos de teste, tempos de cifração inferior a 1.1s e uma vazão de até 12Bps. Os autores concluem que ele demonstra eficiência e uma forte proteção em cenários com baixo poder computacional, embora tenha sido testado apenas em ambientes simulados e com conjuntos de dados limitados, exigindo validação futura em dispositivos reais.

Verma et al. (2024) apresentaram uma abordagem inovadora que une criptografia baseada em DNA com tenologia *blockchain*, visando comunicações seguras em IoT de consumo. Os experimentos, conduzidos em MATLAB, compararam a proposta com RSA e outros métodos híbridos. O sistema teve menor tempo de cifração e decifração e maior resistência a ataques de interceptação e falsificação. A conclusão foi que a integração entre DNA e *blockchain* fornece transparência, rastreabilidade e segurança, superando métodos tradicionais para IoT, embora os testes tenham sido realizados em ambiente simulado, limitando a validação prática da abordagem.

4 MÉTODO DE PESQUISA

Esta pesquisa adota uma abordagem experimental e descritiva, comparando algoritmos de criptografia em DNA (apresentados na Subseção 2.2), aplicados a dispositivos IoT com recursos limitados. Tais dispositivos apresentam restrições de processamento, RAM e armazenamento e não suportam criptografia que demandam muitos recursos computacionais nem atualizações avançadas, o que dificulta a correção de vulnerabilidades [6, 12]. A Figura 2 apresenta uma visão geral do processo metodológico, estruturado em etapas que serão detalhadas nas próximas seções.

Figura 2: Pipeline metodológico adotado.

4.1 Seleção dos algoritmos

A identificação dos algoritmos de criptografia baseados em DNA foi realizada a partir de uma revisão sistemática da literatura. Para isso, foi definida uma estratégia de busca com base na frequência dos termos em repositórios acadêmicos (ScienceDirect, IEEE Xplore, Scopus e ACM Digital Library) e no risco de retornarem resultados irrelevantes. Foram utilizadas expressões associadas a dois eixos principais, criptografia baseada em DNA e IoT, e suas ocorrências foram quantificadas em cada base, de forma a estimar sua relevância na produção científica. Paralelamente, realizou-se uma triagem qualitativa para avaliar a ambiguidade de cada termo, classificando-os conforme o risco de retornar publicações fora do escopo da pesquisa, utilizando os níveis "Sim", "Não" e "Talvez". Essa triagem revelou, por exemplo, que embora o termo "DNA encoding"seja comum, ele tende a aparecer em contextos biológicos, o que reduz sua utilidade na pesquisa proposta. Por outro lado, expressões como "Internet of Things"e "smart devices"mostraram-se amplamente utilizadas e com baixa taxa de ambiguidade, sendo, portanto, mais apropriadas para compor a expressão de busca.

Como resultado desse processo, definiu-se um conjunto final de termos a seguinte *string* de busca: ("*DNA based encryption*"*OR* "*DNA cryptography*") *AND* ("*Internet of Things*"*OR* "*IoT*"*OR* "*smart devices*"*OR* "*Internet of Everything*"), que possibilitou a recuperação de publicações alinhadas ao tema da criptografia em DNA com aplicações em sistemas embarcados. As obras encontradas passaram por uma filtragem rigorosa, considerando como critério a disponibilidade de código implementado ou pseudocódigo. Artigos cujo foco era apenas a aplicação de técnicas de cifração em nível teórico, sem demonstração prática ou viabilidade de implementação, foram desconsiderados.

Com base nesses critérios, foram selecionados os algoritmos que atendem aos requisitos definidos. Eles constituem as variáveis independentes deste estudo, pois representam os fatores manipulados nos experimentos para avaliar seu impacto nos resultados [33]. Os trabalhos foram listados a seguir, estando devidamente indexados para facilitar a compreensão e a referência nas seções posteriores deste trabalho:

- **Alg_1**: A novel cryptosystem based on DNA cryptography, hyperchaotic systems and a randomly generated Moore machine for cyber physical systems [25].
- **Alg_2**: An efficient environmental monitoring data encryption algorithm based on DNA coding and hyperchaotic system [30].
- **Alg_3**: DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography [29].
- **Alg_4**: Image encryption based on 2DNA encoding and chaotic 2D logistic map [5].

4.2 Definição das variáveis dependentes

A etapa de definição das variáveis dependentes identificam as métricas que representam os resultados ou efeitos do experimento, sendo medidas ou observadas pelo pesquisador para verificar o impacto decorrente da manipulação das variáveis independentes [33].

No presente estudo, as variáveis dependentes consideram limitações típicas de dispositivos IoT, organizadas em três dimensões principais e avaliadas separadamente nos processos de cifração e decifração: Consumo de memória RAM (bytes), Tempo de execução (μs), Consumo energético (mJ) e Corrente (mA).

4.3 Ambiente de testes

Nesta etapa foram definidos os equipamentos, suas configurações e a arquitetura utilizada para a coleta das métricas de consumo. Os experimentos foram conduzidos no ambiente computacional ilustrado na Figura 3. O dispositivo principal (*Computer*) foi um notebook Lenovo LOQ-e 15iax9e, equipado com processador Intel Core i5-12450HX, 16 GB de RAM, SSD de 512 GB, GPU dedicada NVIDIA RTX 3050 com 6 GB DDR6 e Windows 11 Home (versão 24H2). Os dispositivos embarcados e periféricos empregados nos testes foram:

- **NodeMCU 1.0 (ESP8266)**: tensão de entrada entre 7 e 12 V, tensão de operação de 3,3 V, memória flash de 4 MB, SRAM de 64 KB, CPU Tensilica L106 32-bit RISC, clock de 80 MHz e arquitetura single-core [11], utilizado para executar os algoritmos selecionados.
- **Arduino UNO R3**: baseado no microcontrolador ATmega32-8P, com clock de 16 MHz, tensão de entrada entre 7 e 12 V, 2 KB de SRAM, 32 KB de memória flash e 1 KB de EEPROM [8], utilizado para auxiliar na aquisição de dados de consumo energético durante os testes.
- **INA219**: sensor de corrente e tensão com interface I²C compatível com SMBus, tensão de operação de 3,0 V a 5,5 V, consumo típico de 0,7 mA (máximo de 1 mA), modo de economia entre 6 µA e 15 µA, suporte a tensões de barramento de 0 V a 26 V, faixa de tensão diferencial de ±40 mV a ±320 mV (com PGA ajustável entre ÷1 e ÷8) e resolução ADC configurável de 9 a 12 bits. No contexto do experimento, o INA219 foi responsável por medir os parâmetros elétricos, tensão (V), corrente (mA), potência (mW) e queda de tensão no shunt (mV), durante a execução de cada algoritmo, viabilizando a coleta de dados energéticos de forma não invasiva [32].
- **YwRobot MB102 Power Supply**: módulo de alimentação para protoboard, com entrada de 6,5 V a 12 V (via conector DC) ou 5 V (via USB), saídas selecionáveis de 3,3 V ou 5 V (via jumper), fornecendo corrente máxima inferior a 700 mA [13].

Para a execução experimental, utilizou-se *Python 3.13* na coleta de dados do dispositivo principal e C++ (padrão C++20) no desenvolvimento dos algoritmos embarcados. O *NodeMCU 1.0* (ESP8266) executou os algoritmos, sendo alimentado exclusivamente pelo *YwRobot MB102 Power Supply*, configurado para fornecer 5V. O monitoramento do consumo energético foi realizado pelo Arduino UNO R3 em conjunto com o sensor INA219, conectado em série entre a fonte e o ESP8266 para medir a corrente consumida em tempo real. O circuito foi estruturado de forma que uma saída de 5V do YwRobot passasse pelo INA219 antes de alimentar o ESP8266, enquanto o próprio INA219 recebia alimentação de uma segunda saída de 5V do mesmo YwRobot MB102, independente da linha usada para o ESP8266. A conexão com o computador ocorreu apenas para gravação dos algoritmos e coleta de métricas, não fornecendo energia pela porta USB, de modo que a execução foi alimentada exclusivamente pelo YwRobot MB102.

4.4 Experimentos e coleta de dados

Os experimentos visaram avaliar o desempenho de quatro algoritmos de criptografia em DNA, discutidos na Subseção 2.2, no microcontrolador NodeMCU 1.0 (ESP8266). Adotou-se como entrada o binário de uma imagem, dado que o algoritmo proposto no Alg_4 opera especificamente sobre dados imagéticos. A mesma *string* binária foi usada nos demais algoritmos, garantindo condições equivalentes de teste e comparação imparcial.

Devido às limitações do ESP8266, a imagem foi redimensionada para 32×32 pixels e convertida em um vetor de características, cuja dimensionalidade foi reduzida via Análise de Componentes Principais (PCA), ilustrado na Figura 4. O vetor resultante foi transformado em matriz binária e utilizado como texto claro para todos os algoritmos.

O processo de coleta das métricas foi conduzido de maneira sistemática e controlada. Cada algoritmo, em ambos os modos (cifração e decifração), foi executado 100 vezes de forma independente. A execução ocorreu de maneira isolada para cada cenário; por exemplo, no caso do Alg_1 em modo de cifração, o algoritmo foi executado individualmente em 100 iterações consecutivas, com o registro das métricas associado a cada execução. Esse mesmo procedimento foi repetido para todos os algoritmos e para os dois modos de operação (cifração e decifração), visando a uniformidade no processo experimental. As métricas obtidas em cada execução foram transmitidas para o computador principal, no qual o *script* desenvolvido foi responsável por automatizar a aquisição, estruturar os dados e armazená-los em formato CSV.

Na etapa subsequente, os dados brutos foram submetidos ao método estatístico *Interquartile Range* (IQR), empregado para a remoção de valores extremos em cada grupo de observações. Após esse tratamento, foram selecionadas exatamente 59 amostras por grupo, de modo a manter a consistência do tamanho amostral (N) entre todos os algoritmos e modos de execução. A partir desse conjunto refinado, calcularam-se as métricas de desempenho e consumo energético, fundamentadas no método proposto por [19], com base na equação clássica da eletrotécnica:

$$E = V \cdot I \cdot t$$

em que E representa a energia consumida, em miliJoules (mJ); V a tensão de operação, em Volts (V); I a corrente elétrica, em miliamperes (mA); e t o tempo de execução da operação, em segundos (s).

5 RESULTADOS E DISCUSSÕES

A Tabela 2 apresenta as métricas de desempenho, consumo energético e uso de memória dos algoritmos avaliados. A variância do consumo de memória RAM não foi informada, pois o valor é fornecido diretamente pelo dispositivo embarcado nos metadados durante a execução do algoritmo. Como não houve variação nos registros, a variância permaneceu sempre nula. Os dados sintetizam informações essenciais para a análise comparativa, considerando parâmetros diretamente relacionados à eficiência computacional e à viabilidade em ambientes embarcados.

Foi realizada uma análise estatística para investigar diferenças no desempenho dos algoritmos em relação aos dois modos de operação. Foram avaliados dados pareados das coletas realizadas. A partir dos

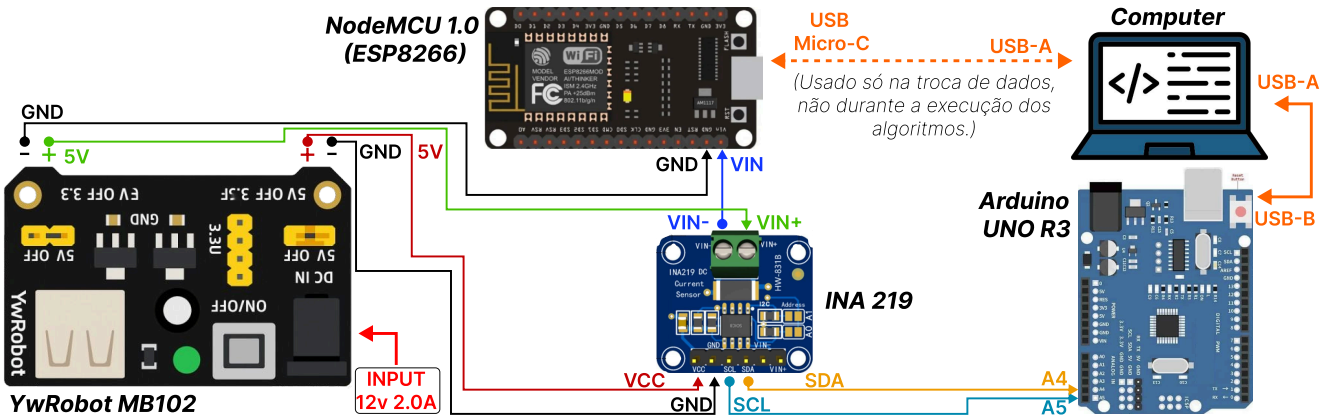

Figura 3: Conexões entre os dispositivos.

Algoritmo	Energia (mJ)	Corrente (mA)	Tempo (μs)	RAM (B)
Alg_1_encrypt	955.3	19.11	19073.88	28856
Alg_1_decrypt	239.4	21.76	2198.49	28412
Alg_2_encrypt	996.1	22.06	18128.10	28564
Alg_2_decrypt	15.7	19.19	164.00	29120
Alg_3_encrypt	298.6	19.22	3107.00	28420
Alg_3_decrypt	260.5	19.11	2727.32	29336
Alg_4_encrypt	1176.6	23.06	10197.88	28652
Alg_4_decrypt	813.4	17.55	9263.88	28440

Tabela 2: Valores médios das métricas avaliadas

testes estatísticos, Shapiro-Wilk e Wilcoxon, aplicados, foi possível avaliar com precisão técnica os algoritmos analisados resumidos na Tabela 3.

Métrica	Melhor	Pior	Observação
Tempo (μs)	Alg_3	Todos os demais	Diferenças significativas entre todos; Alg_3 é o mais rápido
Energia (mJ)	Alg_3	Alg_2	Todos diferem estatisticamente; Alg_3 tem o menor consumo
Corrente (mA)	Alg_2 e Alg_3	Alg_1 e Alg_4	Apenas Alg_2 e Alg_3 são estatisticamente similares; diferenças nos demais
RAM (bytes)	Alg_4	Alg_3	Consumo total: Alg_4 (57092) é o menor; Alg_3 (57756) é o maior

Tabela 3: Comparação dos algoritmos.

Em relação ao tempo de execução, os dados não seguiram distribuição normal, conforme verificado pelo teste de *Shapiro-Wilk*. Por esse motivo, aplicou-se o teste não paramétrico de *Wilcoxon* pareado, em vez de um teste que exige normalidade, como o *t-test* de Student, por exemplo. Os resultados indicaram diferenças estatisticamente significativas entre todos os algoritmos. O Alg_3 apresentou o melhor desempenho, com tempos médios de 3107 μs na cifração e 2727 μs na decifração, além de baixa variação entre as operações, refletindo execução estável e previsível. O Alg_2 mostrou o pior equilíbrio, com forte assimetria entre os modos (18128 μs para cifração contra apenas 164 μs na decifração), revelando uma arquitetura desequilibrada. O Alg_1, embora apresente cifração lenta (19073 μs), compensa com decifração rápida (2198 μs), podendo ser adequado em cenários em que a leitura ocorre com maior frequência que a escrita. Já o Alg_4 apresentou tempos intermediários, porém ainda elevados (10197 μs e 9263 μs), o que compromete sua viabilidade em sistemas com fortes restrições temporais.

No que se refere ao consumo energético, o teste de *Wilcoxon* evidenciou diferenças estatísticas entre todos os algoritmos. O Alg_3 se destacou por apresentar o menor consumo total e baixa variação entre cifração (298,6 mJ) e decifração (260,5 mJ), caracterizando-se como o mais eficiente energeticamente. O Alg_1, embora apresente custo mais elevado na cifração (955,3 mJ), manteve valores consistentes e previsíveis entre as operações. O Alg_2 revelou a maior assimetria (996,1 mJ na cifração contra 15,7 mJ na decifração), sendo estatisticamente inferior aos demais. O Alg_4, por sua vez, apresentou os maiores consumos absolutos (1176,6 mJ e 813,4 mJ), limitando sua adequação em cenários energicamente restritivos.

Quanto à corrente elétrica, as médias variaram entre 17,55 mA e 23,06 mA. Apesar da proximidade dos valores, o teste de *Wilcoxon* indicou diferenças estatisticamente significativas, exceto entre Alg_2 e Alg_3. O Alg_3 apresentou os valores mais equilibrados entre cifração (19,22 mA) e decifração (19,11 mA), reforçando sua estabilidade. O Alg_4 mostrou a maior variação (23,06 mA contra 17,55 mA), indicando maior instabilidade.

No que diz respeito ao uso de memória RAM, o somatório das operações revelou que o Alg_4 foi o mais eficiente (57092 B), seguido de perto pelo Alg_1 (57268 B). O Alg_2 e o Alg_3 apresentaram maiores demandas (57684 B e 57756 B, respectivamente), com o Alg_3 sendo o mais exigente nesse aspecto.

De forma integrada, os resultados apontam que o Alg_3 é o mais vantajoso em tempo e energia, além de apresentar consumo de corrente estável, embora demande mais memória. O Alg_1, por sua vez, oferece bom equilíbrio entre as métricas e menor uso de RAM, o que o torna competitivo em cenários embarcados. O Alg_2 mostrou comportamento assimétrico e ineficiente em energia, enquanto o Alg_4, apesar de eficiente em RAM, compromete-se

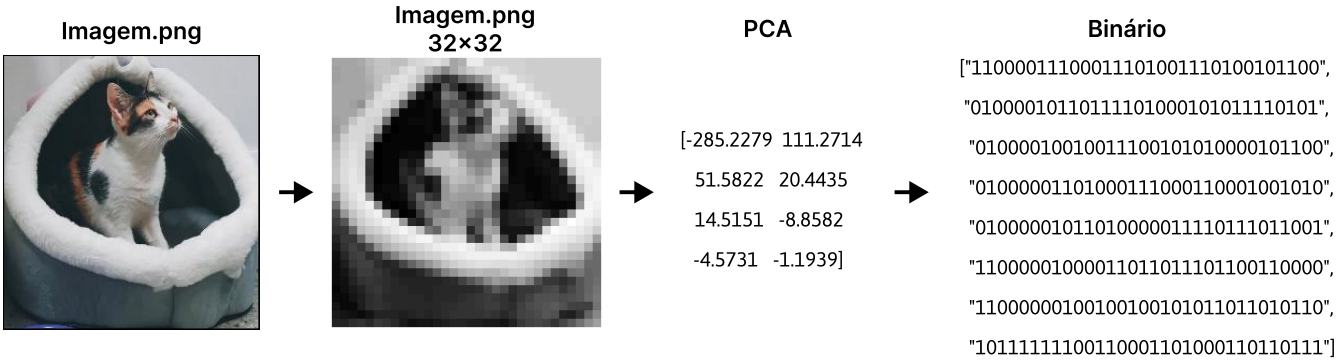

Figura 4: Conversão de imagem em matriz de bits.

em tempo e energia, sendo menos adequado para ambientes com severas restrições de recursos. No caso do Alg_4, esse desempenho decorre do processo de cifração, no qual o embaralhamento e os cálculos caóticos para geração das chaves precisam ser executados para formar o padrão pseudoaleatório inicial. Na decifração, esses padrões apenas são reutilizados para reverter as trocas, resultando em menor consumo de energia e menor carga computacional.

6 CONCLUSÃO

O presente estudo realizou uma análise comparativa de quatro algoritmos de criptografia baseada em DNA, implementados e testados em um microcontrolador ESP8266. Foram avaliadas métricas essenciais para ambientes com restrições computacionais, como tempo de execução, consumo de energia, corrente elétrica e uso de memória RAM, relacionando os resultados ao desenho arquitetural de cada algoritmo. Os dados mostraram que o Alg_3 se destacou como o mais eficiente em termos de tempo e energia, além de apresentar consumo de corrente estável. Contudo, esse algoritmo também foi o mais exigente em termos de memória RAM, o que pode restringir sua aplicação em dispositivos com recursos extremamente limitados. O Alg_1, por sua vez, apresentou bom equilíbrio entre as métricas, com destaque para o baixo uso de RAM e comportamento previsível, configurando-se como uma opção em cenários embarcados. Em contraste, o Alg_4, embora eficiente em RAM, mostrou consumo energético elevado e tempos de execução longos, limitando sua aplicabilidade em sistemas críticos. O Alg_2 demonstrou forte assimetria entre os modos de operação, principalmente no consumo energético, o que o torna menos indicado para aplicações sensíveis a eficiência.

Complementando a análise, os testes estatísticos de normalidade (Shapiro-Wilk) e comparação pareada (Wilcoxon) confirmaram diferenças significativas entre os algoritmos em praticamente todas as métricas. Apenas no caso da corrente elétrica verificou-se proximidade estatística entre Alg_2 e Alg_3, enquanto os demais apresentaram diferenças relevantes. Os achados reforçam que a escolha do algoritmo deve considerar o perfil do sistema-alvo: o Alg_3 é recomendado quando desempenho e eficiência energética são prioridades, ao passo que o Alg_1 representa uma alternativa equilibrada quando há restrição de memória. Nesse contexto, mesmo com baterias melhores, o consumo energético para tarefas como criptografia, comunicação e processamento continua impondo restrições, já que aumentar a capacidade da bateria pode não ser viável por limitações de tamanho, peso ou custo de hardware. Assim, estudos como este contribuem para orientar decisões de projeto em aplicações IoT, promovendo o uso criterioso e eficiente de criptossistemas bioinspirados em ambientes de recursos limitados.

Como trabalho futuro, sugere-se a realização de testes de segurança mais aprofundados, com foco na robustez dos algoritmos frente a ataques práticos. Isso inclui a aplicação de ataques de força bruta para avaliar a resistência ao espaço de chaves, bem como testes de criptoanálise diferencial, estatística e aprendizado de máquina, visando identificar padrões previsíveis nas saídas cifradas. Adicionalmente, análises de entropia, correlação e dispersão podem ser aplicadas para quantificar a aleatoriedade dos dados cifrados, além da investigação da eficiência energética sob diferentes condições operacionais, como variação da frequência do clock e alteração de tensão de alimentação. Também se destaca a necessidade de investigar o impacto do processamento de imagens maiores como forma de avaliar o consumo energético e computacional do dispositivo. Essas abordagens complementariam a análise de desempenho realizada neste estudo e permitiriam uma avaliação mais completa da viabilidade desses algoritmos em cenários reais.

REFERÊNCIAS

[1] Mahmoud A Abdelaal, Abdellatif I Moustafa, H Kasban, H Saleh, Hanaa A Abdallah, and Mohamed Yasin I Afifi. 2025. DNA-Inspired Lightweight Cryptographic Algorithm for Secure and Efficient Image Encryption. *Sensors* 25, 7 (2025), 2322.

[2] Mahmoud A. Abdelaal, Abdellatif I. Moustafa, H. Kasban, H. Saleh, Hanaa A. Abdallah, and Mohamed Yasin I. Afifi. 2025. DNA-Inspired Lightweight Cryptographic Algorithm for Secure and Efficient Image Encryption. *Sensors* 25, 7 (2025). https://doi.org/10.3390/s25072322

[3] R. Abiri, Nastaran Rizan, Siva K. Balasundram, Arash Bayat Shahbazi, and H. Abdul-Hamid. 2023. Application of digital technologies for ensuring agricultural productivity. *Heliyon* 9 (2023). https://doi.org/10.1016/j.heliyon.2023.e22601

[4] Suaad Hadi Hassan Al-Taai, Huda Abbas Kanber, and Waleed Abood Mohammed al Dulaimi. 2023. The Importance of Using the Internet of Things in Education. *International Journal of Emerging Technologies in Learning (iJET)* (2023). https://doi.org/10.3991/ijet.v18i01.35999

[5] Asmaa Hasan Alrubaie, Maisa'a Abid Ali Khodher, and Ahmed Talib Abdulameer. 2023. Image encryption based on 2DNA encoding and chaotic 2D logistic map. *Journal of Engineering and Applied Science* 70, 1 (2023), 60.

[6] Mahmoud Ammar, Giovanni Russello, and Bruno Crispo. 2018. Internet of Things: A survey on the security of IoT frameworks. *Journal of Information Security and Applications* 38 (2018), 8–27. https://doi.org/10.1016/j.jisa.2017.11.002

[7] Sehrish Aqeel, Adnan Shahid Khan, Irshad Ahmed Abbasi, Fahad Algarni, and Daniel Grzonka. 2025. Enhancing IoT security with a DNA-based lightweight cryptography system. *Scientific Reports* 15, 1 (2025), 13367.

[8] Arduino. 2024. *Arduino UNO Rev3 — Tech Specs.* https://docs.arduino.cc/hardware/uno-rev3/#tech-specs Accessed: June 2025.

[9] Alessio Benavoli, Giorgio Corani, Francesca Mangili, Marco Zaffalon, and Fabrizio Ruggeri. 2014. A Bayesian Wilcoxon signed-rank test based on the Dirichlet process. In *International conference on machine learning*. PMLR, 1026–1034.

[10] P. G. Chiara. 2019. Segurança e Privacidade em Dispositivos com Recursos Limitados. 2598 (2019), 1–11.

[11] Espressif Systems. 2023. ESP8266EX Datasheet. https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf Accessed: June 2025.

[12] Jorge Granjal, Edmundo Monteiro, and Jorge Sá Silva. 2015. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Communications Surveys Tutorials* 17, 3 (2015), 1294–1312. https://doi.org/10.1109/COMST.2015.2388550

[13] Handson Technology. 2013. *MB102 Breadboard Power Supply Module Datasheet.* https://www.handsontec.com/dataspecs/mb102-ps.pdf Accessed: June 2025.

[14] Maha Helal. 2025. Current developments, applications, challenges and future trends in internet of things: A survey. *International Journal of Data and Network Science* (2025). https://doi.org/10.5267/j.ijdns.2024.9.008

[15] Han Hu, Qun Wang, R. Hu, and Hongbo Zhu. 2021. Mobility-Aware Offloading and Resource Allocation in a MEC-Enabled IoT Network With Energy Harvesting. *IEEE Internet of Things Journal* 8 (2021), 17541–17556. https://doi.org/10.1109/JIOT.2021.3081983

[16] Maria Imdad, Adnan Fazil, Sofia Najwa Binti Ramli, Jihyoung Ryu, Hairulnizam Bin Mahdin, and Zahid Manzoor. 2024. DNA-PRESENT: An Improved Security and Low-Latency, Lightweight Cryptographic Solution for IoT. *Sensors* 24, 24 (2024), 7900.

[17] Maria Imdad, Sofia Najwa Ramli, and Hairulnizam Mahdin. 2021. Increasing randomization of ciphertext in DNA cryptography. *International Journal of Advanced Computer Science and Applications* 12, 10 (2021).

[18] Tallat Jabeen, Ishrat Jabeen, Humaira Ashraf, NZ Jhanjhi, Abdulsalam Yassine, and M Shamim Hossain. 2023. An intelligent healthcare system using IoT in wireless sensor network. *Sensors* 23, 11 (2023), 5055.

[19] Strahinja P. Janković and Vujo R. Drndarević. 2015. Microcontroller power consumption measurement based on PSoC. In *2015 23rd Telecommunications Forum Telfor (TELFOR)*. 673–676. https://doi.org/10.1109/TELFOR.2015.7377557

[20] Durga Karapurkar, V. Bhaskaran, Shreya Bale, and P. Pednekar. 2018. DNA Based Cryptography. (2018).

[21] Mohammad M. Mansour, Amal Gamal, Ahmed I. Ahmed, L. Said, Abdelmoniem Elbaz, N. Herencsar, and Ahmed Soltan. 2023. Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions. *Energies* (2023). https://doi.org/10.3390/en16083465

[22] Prabhaker Mishra, Chandra M Pandey, Uttam Singh, Anshul Gupta, Chinmoy Sahu, and Amit Keshri. 2019. Descriptive statistics and normality tests for statistical data. *Annals of cardiac anaesthesia* 22, 1 (2019), 67–72.

[23] Hamdy M Mousa. 2016. DNA-genetic encryption technique. *IJ Computer Network and Information Security* 7 (2016), 1–9.

[24] Damilola Oladimeji, Khushi Gupta, Nuri Alperen Kose, Kubra Gundogan, Linqiang Ge, and Fan Liang. 2023. Smart Transportation: An Overview of Technologies and Applications. *Sensors (Basel, Switzerland)* 23 (2023). https://doi.org/10.3390/s23083880

[25] Pramod Pavithran, Sheena Mathew, Suyel Namasudra, and Gautam Srivastava. 2022. A novel cryptosystem based on DNA cryptography, hyperchaotic systems and a randomly generated Moore machine for cyber physical systems. *Computer communications* 188 (2022), 1–12.

[26] Gamil RS Qaid and Nadhem Sultan Ebrahim. 2023. A lightweight cryptographic algorithm based on DNA computing for IoT devices. *Security and Communication Networks* 2023, 1 (2023), 9967129.

[27] K Sasikumar and Sivakumar Nagarajan. 2024. Comprehensive review and analysis of cryptography techniques in cloud computing. *IEEE Access* (2024).

[28] Ashish Singh, Abhinav Kumar, and Suyel Namasudra. 2024. DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography. *Front. Comput. Sci.* 18 (2024), 181801. Issue 1. https://doi.org/10.1007/s11704-022-2193-3

[29] Ashish Singh, Abhinav Kumar, and Suyel Namasudra. 2024. DNACDS: Cloud IoE big data security and accessing scheme based on DNA cryptography. *Frontiers of Computer Science* 18, 1 (2024), 181801.

[30] J Mbarndouka Taamté, VR Folifack Signing, M Kountchou Noube, and BS Bertrand. 2022. An efficient environmental monitoring data encryption algorithm based on DNA coding and hyperchaotic system. *Int J Inf Technol* 14, 3 (2022), 1367–1380.

[31] Jacob Mbarndouka Taamté, Vitrice Ruben Folifack Signing, Michaux Kountchou Noube, Bodo Bertrand, and Saïdou. 2022. An efficient environmental monitoring data encryption algorithm based on DNA coding and hyperchaotic system. *Int. j. inf. tecnol.* 14 (2022), 1367–1380. Issue 3. https://doi.org/10.1007/s41870-022-00887-z

[32] Texas Instruments. 2009. *INA219 High-Side Measurement, Current Shunt and Power Monitor With I2C Interface Datasheet.* https://www.alldatasheet.com/datasheet-pdf/pdf/249609/TI/INA219.html Accessed: June 2025.

[33] William MK Trochim and James P Donnelly. 2001. *Research methods knowledge base*. Vol. 2. Atomic dog publishing Cincinnati, OH.

[34] Namrata Vaswani, Yuejie Chi, and Thierry Bouwmans. 2018. Rethinking PCA for modern data sets: Theory, algorithms, and applications [scanning the issue]. *Proc. IEEE* 106, 8 (2018), 1274–1276.

[35] Ankush Verma, Geetanjali Rathee, and Chaker Abdelaziz Kerrache. 2024. Toward Secure Consumer IoT Communications using DNA Encryption and Blockchain Technology. In *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS)*. IEEE, 1–7.

[36] Sissi Xiaoxiao Wu, Hoi-To Wai, Lin Li, and Anna Scaglione. 2018. A review of distributed algorithms for principal component analysis. *Proc. IEEE* 106, 8 (2018), 1321–1340.

[37] Fan Zeng, Chuang-Chuang Pang, and Huajun Tang. 2024. Sensors on Internet of Things Systems for the Sustainable Development of Smart Cities: A Systematic Literature Review. *Sensors (Basel, Switzerland)* 24 (2024). https://doi.org/10.3390/s24072074

[38] Nabila Zitouni, M. Sedrati, and Amel Behaz. 2023. LightWeight energy-efficient Block Cipher based on DNA cryptography to secure data in internet of medical things devices. *International Journal of Information Technology* (2023), 1–11. https://doi.org/10.1007/s41870-023-01580-5

[39] Hai Ziwei, Dongni Zhang, Zhang Man, Du Yixin, Shuanghui Zheng, Yang Chao, and Chunfeng Cai. 2024. The applications of internet of things in smart healthcare sectors: a bibliometric and deep study. *Heliyon* 10 (2024). https://doi.org/10.1016/j.heliyon.2024.e25392