Journal of Positive Sciences (JPS) eISSN: 2582-9351, https://positive-sciences.com JPS. 2026 July; 6(4): 171-189

Article info
Received on: 13.06.2026
Accepted on: 10.07.2026
Published on: 11.07.2026
doi: https://doi.org/10.52688/JPS128892

Research Article

A Genetic Algorithm-Based Approach for Enhancing Data Security

Mazin Haithem Razuky [1], Mohammed RASHEED [2, *]

[1] Biomedical Informatics College, University of Information Technology and Communications, Baghdad, Iraq
[2] College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq

[*] rasheed.mohammed40@yahoo.com

ABSTRACT

Data security has become one of the most critical concerns in modern information technology due to the rapid growth of digital communication, cloud computing, Internet of Things (IoT) devices, online financial transactions, and large-scale data sharing. The increasing frequency of cyberattacks, data breaches, and unauthorized access has created an urgent need for stronger and more intelligent security mechanisms capable of protecting sensitive information. Although conventional encryption algorithms such as the Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) provide robust protection, the overall security of these systems largely depends on the quality, randomness, and unpredictability of the cryptographic keys employed. This study presents a simple framework that utilizes a Genetic Algorithm (GA) to improve encryption key generation through evolutionary optimization. The proposed approach represents candidate encryption keys as chromosomes and applies the fundamental GA operations of population initialization, fitness evaluation, tournament selection, crossover, and mutation to iteratively generate stronger keys with improved randomness. The effectiveness of the proposed framework is evaluated using simulated experimental data based on four performance indicators: fitness value, key entropy, randomness score, and encryption execution time. The results demonstrate that the average fitness value increased from 0.61 in the initial population to 0.96 after 50 generations, while the entropy improved from 7.42 to 7.91 and the randomness score increased from 82% to 96%. Although the encryption execution time increased slightly from 12.3 ms to 13.1 ms, the computational overhead remained minimal compared with the achieved security enhancement. These findings indicate that Genetic Algorithms can effectively optimize cryptographic key generation by producing more secure and unpredictable encryption keys while maintaining acceptable computational efficiency. Although the proposed framework is intentionally simplified for educational purposes, it provides a practical demonstration of evolutionary optimization in cryptography and establishes a foundation for future integration with advanced encryption algorithms and intelligent cybersecurity systems.

KEYWORDS: Data Security, Genetic Algorithm, Encryption, Optimization, Information Security, Evolutionary Computing.

INTRODUCTION

The rapid advancement of information and communication technologies has transformed the way individuals, organizations, and governments store, process, and exchange data [1-3]. Cloud computing, Internet of Things (IoT) devices, online banking, electronic healthcare systems, e-commerce platforms, and social networking services generate enormous volumes of sensitive digital information every day [4-7]. While these technologies improve accessibility and operational efficiency, they also increase the risk of cyberattacks, unauthorized access, identity theft, ransomware, and data breaches [8, 9]. Consequently, ensuring data confidentiality, integrity, and availability has become one of the primary objectives of modern

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

cybersecurity systems [10, 11]. Encryption remains the most widely adopted technique for protecting digital information against unauthorized disclosure [12, 13]. By converting readable plaintext into an unintelligible ciphertext using a cryptographic key, encryption prevents attackers from understanding intercepted information without the corresponding decryption key [14]. Modern cryptographic algorithms such as the Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) provide high levels of security and are extensively employed in commercial, industrial, and governmental applications [15]. However, the effectiveness of these algorithms depends heavily on the quality and randomness of the cryptographic keys used during the encryption process [16]. The security of an encryption system is significantly influenced by key generation techniques [17]. Keys with poor randomness or predictable patterns reduce the effective key space and may become vulnerable to brute-force, statistical, or cryptanalytic attacks [18]. Therefore, developing methods that produce highly random and unpredictable encryption keys is an important research area in information security [19]. Artificial intelligence and computational intelligence techniques have recently attracted considerable attention for solving complex optimization problems [20]. Among these techniques, Genetic Algorithms (GAs) have emerged as powerful optimization methods inspired by Darwinian evolution and natural selection. Originally proposed by John Holland, Genetic Algorithms simulate biological evolution through iterative processes involving chromosome representation, fitness evaluation, parent selection, crossover, and mutation [21]. These mechanisms enable GAs to efficiently search large solution spaces and identify near-optimal solutions without requiring gradient information or deterministic mathematical models [22]. Because of their strong optimization capability, Genetic Algorithms have been successfully applied in numerous engineering disciplines, including scheduling, manufacturing optimization, image processing, machine learning, wireless communication, network routing, feature selection, and cryptography [23]. In cybersecurity applications, GAs have demonstrated promising potential for optimizing cryptographic keys, enhancing randomness, improving substitution and permutation processes, and strengthening resistance against various forms of attack [24].

Genetic Algorithms contribute to data security by improving the quality of cryptographic key generation and optimization [25]. Unlike conventional deterministic key generation methods, GAs continuously evolve candidate keys through multiple generations, gradually increasing their randomness and complexity according to predefined fitness criteria [26]. The crossover operator combines desirable characteristics from two high-quality parent chromosomes, producing new offspring with potentially stronger security characteristics [27]. Mutation introduces controlled random modifications into chromosomes, preventing premature convergence while increasing population diversity [28]. Selection mechanisms preserve high-quality candidate solutions throughout successive generations, allowing the algorithm to converge toward highly optimized encryption keys [29].

The application of GAs in cryptography provides several potential advantages, including [30]:

- Increased key randomness and entropy.
- Larger effective key search space.
- Improved resistance to brute-force attacks.
- Reduced probability of predictable key patterns.
- Adaptive optimization for different security requirements.
- Flexibility to integrate with existing encryption algorithms such as AES and RSA.

Although Genetic Algorithms do not replace traditional encryption algorithms, they can significantly enhance the security of cryptographic systems by generating stronger and less predictable encryption keys [31]. Despite the robustness of modern cryptographic algorithms, the overall security of encrypted systems remains highly dependent on the quality of encryption key generation [32]. Conventional key generation methods may produce keys with limited randomness due to deterministic procedures or implementation

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

constraints [33]. Such weaknesses can reduce cryptographic strength and increase vulnerability to exhaustive search, statistical analysis, and cryptanalytic attacks [34]. Furthermore, many existing encryption systems focus primarily on mathematical encryption processes while giving comparatively less attention to optimization of key generation itself [35]. As cyber threats continue to evolve, there is an increasing need for intelligent optimization techniques capable of producing highly random, adaptive, and secure cryptographic keys [36]. Therefore, an effective optimization strategy is required to improve key quality while maintaining acceptable computational efficiency [37].

Previous studies have demonstrated the effectiveness of Genetic Algorithms in solving optimization problems across various engineering applications [38]. Several researchers have investigated GA-assisted cryptographic techniques; however, many of these approaches involve complex hybrid algorithms, advanced mathematical models, or computationally intensive implementations that are not suitable for educational demonstrations or introductory research projects [39]. Moreover, many published studies emphasize theoretical cryptographic analysis while providing limited practical demonstrations illustrating how evolutionary optimization improves key quality [40]. There is also a need for simplified frameworks that clearly explain the evolutionary optimization process and demonstrate its impact using easily interpretable performance indicators [41]. The motivation of this study is therefore to develop a simple and understandable Genetic Algorithm framework that illustrates how evolutionary optimization can enhance encryption key generation while maintaining low computational complexity [42]. Such a framework provides educational value and serves as a foundation for more advanced cryptographic optimization research [43].

The primary objective of this study is to investigate the feasibility of using Genetic Algorithms to improve data security through optimized encryption key generation.

The specific objectives are:

- To present a simplified Genetic Algorithm framework for cryptographic key optimization.
- To explain the evolutionary process of chromosome initialization, selection, crossover, mutation, and fitness evaluation.
- To evaluate the improvement in encryption key quality using entropy and randomness measurements.
- To compare the performance of conventional key generation and GA-based key generation.
- To demonstrate the effectiveness of Genetic Algorithms using simple simulated experimental results.

The scope of this project is limited to a conceptual and educational implementation of Genetic Algorithm-based key optimization. The study does not propose a new encryption algorithm but instead focuses on improving the quality of encryption keys generated before the encryption process. Although Genetic Algorithms have previously been applied in cryptographic optimization, this study provides several practical contributions. The first contribution is the development of a simplified optimization framework that clearly illustrates how evolutionary computation can enhance encryption key generation without requiring complex mathematical derivations. The second contribution is the integration of multiple evaluation metrics, including fitness value, entropy, randomness score, and computational execution time, allowing comprehensive assessment of the optimization process. The third contribution is the presentation of an educational case study that demonstrates the practical implementation of Genetic Algorithms using simulated experimental data. This makes the proposed framework suitable for undergraduate projects, introductory cybersecurity courses, and computational intelligence education. Finally, the study establishes a simple foundation that can be extended to hybrid optimization techniques involving Genetic Algorithms, Particle Swarm Optimization (PSO), Ant Colony Optimization (ACO), Differential Evolution (DE), or machine learning-assisted cryptographic systems.

Several limitations should be considered when interpreting the results of this study [43, 44].

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

- The presented results are illustrative and are based on simulated experimental data.
- The proposed framework focuses only on encryption key optimization rather than modifying the underlying encryption algorithm.
- Only a limited number of optimization parameters are considered, including population size, crossover probability, and mutation probability.
- The framework does not evaluate resistance against advanced cryptanalytic attacks using real-world security benchmarks.
- Performance evaluation is restricted to entropy, randomness, fitness value, and encryption execution time.
- Real hardware implementation and large-scale cybersecurity deployment are beyond the scope of this project.

Despite these limitations, the study provides a clear demonstration of how Genetic Algorithms can contribute to improved cryptographic key generation.

The remainder of this paper is organized as follows: **Section 2** describes the theoretical background of Genetic Algorithms and presents the proposed methodology for encryption key optimization. **Section 3** presents the experimental setup, simulated results, and performance evaluation using entropy, randomness, fitness value, and execution time. **Section 4** discusses the obtained results, highlighting the advantages and practical implications of applying Genetic Algorithms in data security. **Section 5** concludes the study by summarizing the main findings, outlining the limitations, and suggesting future research directions involving advanced evolutionary optimization techniques and real-world cryptographic applications.

MATERIALS AND METHODS

GENETIC ALGORITHM

A Genetic Algorithm (GA) is a population-based optimization technique inspired by the principles of natural evolution and genetics. Proposed by John Holland in the 1970s, GAs simulate biological evolution by repeatedly improving a population of candidate solutions through natural selection, reproduction, crossover, and mutation. Unlike conventional optimization methods that often search from a single starting point, a Genetic Algorithm explores multiple candidate solutions simultaneously, making it effective for solving complex optimization problems with large search spaces. In the context of data security, a chromosome represents a candidate encryption key. Each chromosome is encoded as a binary string consisting of a sequence of bits (0s and 1s) [45, 46]. The objective of the algorithm is to evolve these chromosomes over successive generations until highly random and secure encryption keys are obtained. Candidate keys with better randomness and higher entropy receive higher fitness values and therefore have a greater probability of contributing to the next generation. The proposed Genetic Algorithm follows five fundamental evolutionary stages, as illustrated in **Figure 1**.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

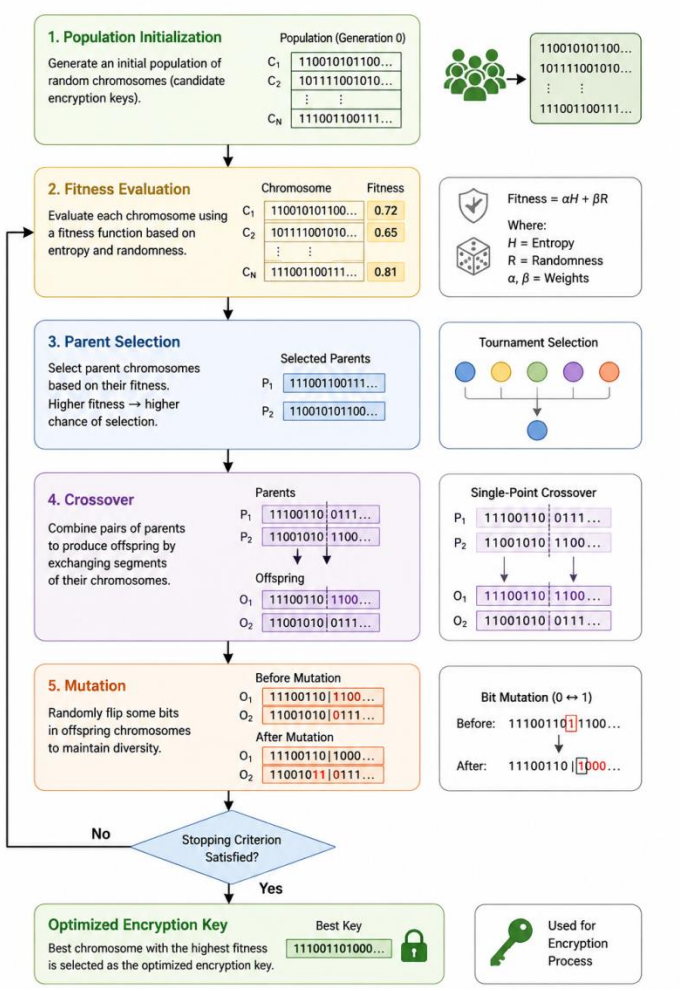

Fig. 1. Flow of the proposed genetic algorithm encryption key optimization.

POPULATION INITIALIZATION

The optimization process begins by randomly generating an initial population of candidate encryption keys. Each chromosome is created using a pseudo-random binary sequence to ensure sufficient diversity among the initial solutions. A diverse initial population increases the likelihood of exploring different regions of the solution space and reduces the possibility of premature convergence toward suboptimal solutions [47, 48].

If the population size is denoted by N, the initial population can be represented as

$$P^{(0)} = \{C_1, C_2, \dots, C_N\} \quad (1)$$

where C_i represents the i^{th} candidate encryption key.

FITNESS EVALUATION

After generating the initial population, every chromosome is evaluated using a fitness function that measures its suitability as an encryption key. In this study, the fitness value is determined according to two important security characteristics:

- Key entropy
- Randomness score

The simplified fitness function is expressed as [49, 50]

$$Fitness = \alpha H + \beta R \quad (2)$$

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

where H = normalized entropy, R = normalized randomness score, $\alpha = 0.6$, and $\beta = 0.4$.

A higher fitness value indicates a stronger encryption key with greater unpredictability and improved resistance to cryptographic attacks.

PARENT SELECTION

The selection stage determines which chromosomes are allowed to reproduce and generate offspring for the next generation. Candidate solutions with higher fitness values have a greater probability of being selected because they represent stronger encryption keys. In the proposed framework, Tournament Selection is adopted due to its simplicity and effectiveness. During each tournament, several chromosomes are randomly selected from the population, and the chromosome with the highest fitness is chosen as a parent. This strategy provides two important advantages [51, 52]:

- Preservation of high-quality candidate solutions,
- Maintenance of sufficient population diversity.

CROSSOVER

Crossover is the primary evolutionary operator responsible for combining useful characteristics from two parent chromosomes. Two selected parents exchange portions of their binary sequences to produce two new offspring that inherit features from both parents.

For example,

Parent 1

110011|001101

Parent 2

101110|111000

After single-point crossover,

Offspring 1

110011111000

Offspring 2

101110001101

The crossover probability determines how frequently recombination occurs. In this study, a crossover probability of **0.80** is employed, meaning that approximately 80% of selected parent pairs undergo crossover. The crossover operation promotes exploration of the search space and accelerates convergence toward highly optimized encryption keys.

MUTATION

Mutation introduces random modifications into offspring chromosomes by flipping selected bits from 0 to 1 or from 1 to 0. Unlike crossover, which combines existing information, mutation introduces new genetic diversity into the population.

For example,

Before mutation

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

110011001101

After mutation

110111001101

where one bit has changed from **0** to **1**.

The mutation probability is intentionally kept small (**0.05**) to avoid excessive randomness while still preventing premature convergence. Mutation enables the algorithm to escape local optima and continuously explore unexplored regions of the search space.

EVOLUTIONARY PROCESS

The complete Genetic Algorithm operates iteratively by repeating the five evolutionary stages until a stopping criterion is satisfied. During each generation, weaker candidate encryption keys are gradually replaced by stronger offspring generated through selection, crossover, and mutation. The optimization procedure can be summarized as follows:

1. Generate an initial population of random encryption keys.
2. Evaluate the fitness of every chromosome.
3. Select parent chromosomes using tournament selection.
4. Apply crossover to generate offspring.
5. Apply mutation to maintain diversity.
6. Replace the previous population with the new generation.
7. Repeat the process until the maximum number of generations or convergence criterion is reached.

Through repeated evolution, the average fitness of the population gradually increases, resulting in encryption keys with higher entropy, greater randomness, and improved cryptographic strength. This evolutionary optimization process forms the foundation of the proposed framework for enhancing data security.

PROPOSED FRAMEWORK

Fig. 2. presents the overall workflow of the proposed Genetic Algorithm (GA)-based framework for enhancing data security through optimized encryption key generation. The process begins with the plain data, which represents the original information that requires protection against unauthorized access. An initial population of randomly generated encryption keys (chromosomes) is then created to provide a diverse search space for optimization. Each candidate key undergoes fitness evaluation, where its quality is assessed according to security-related metrics such as entropy and randomness. Based on these fitness values, the most suitable chromosomes are selected as parent solutions using a selection strategy that favors higher-quality candidates. The selected parent chromosomes participate in the crossover operation, where segments of their binary representations are exchanged to produce new offspring with potentially improved cryptographic characteristics. Subsequently, the mutation operation randomly modifies selected bits within the offspring chromosomes to maintain genetic diversity, prevent premature convergence, and explore new regions of the solution space. The evolutionary cycle consisting of fitness evaluation, selection, crossover, and mutation is repeated over multiple generations until a predefined stopping criterion, such as the maximum number of generations or convergence of the fitness value, is achieved. After convergence, the chromosome with the highest fitness is selected as the optimized encryption key. This optimized key is subsequently used by the encryption algorithm to convert the original plaintext into secure ciphertext. The final output is secure encrypted data that exhibits improved randomness, higher entropy, and greater

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

resistance to brute-force and statistical attacks. Overall, the proposed framework demonstrates how evolutionary optimization can strengthen cryptographic key generation while introducing only minimal computational overhead, thereby improving the overall effectiveness and reliability of the data security system [53-55].

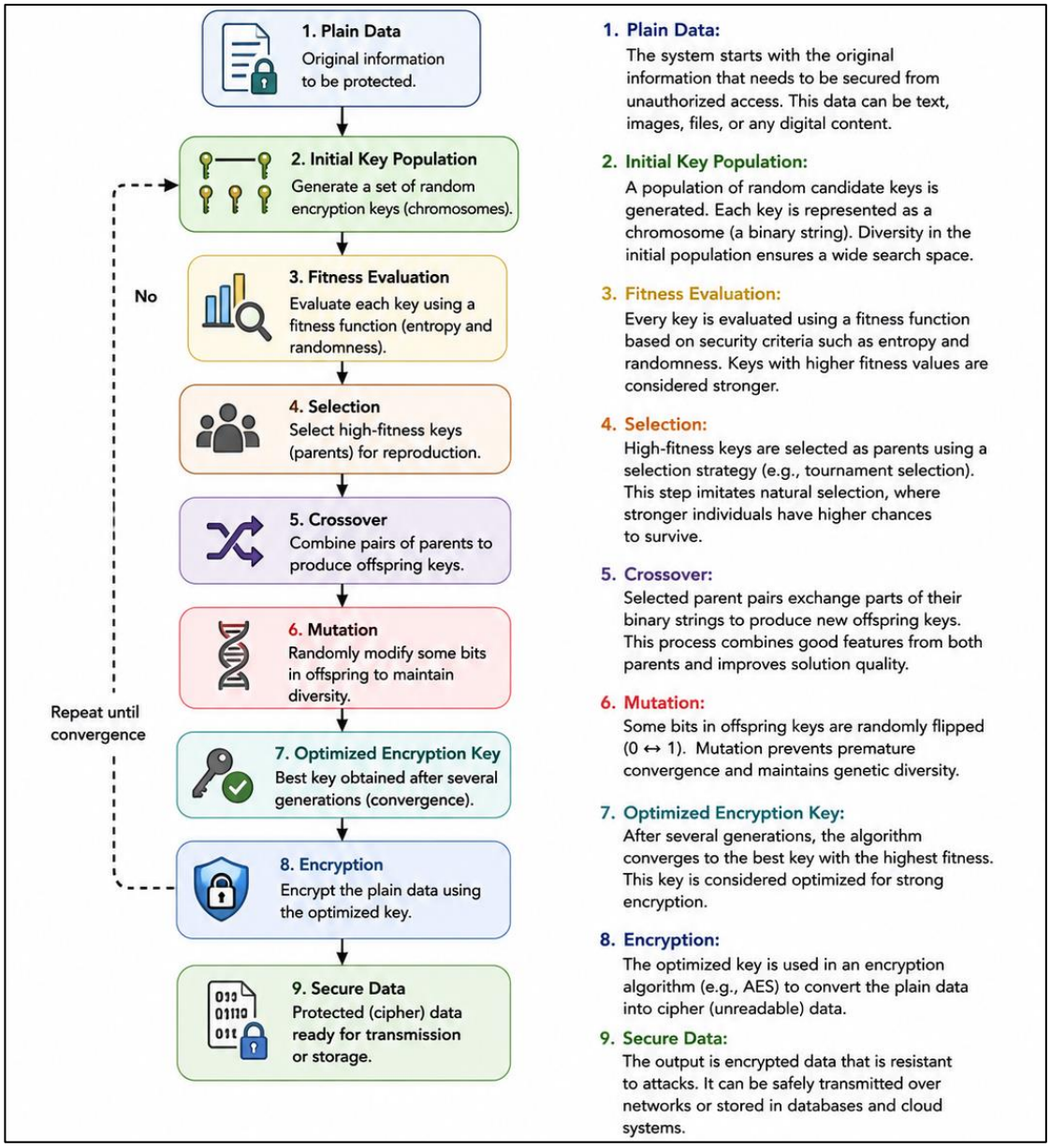

Fig. 2. Workflow of the proposed GA-based encryption key optimization framework

FITNESS FUNCTION

The fitness function is one of the most important components of the Genetic Algorithm because it determines the quality of each candidate encryption key and guides the evolutionary optimization process. During every generation, each chromosome in the population is evaluated using a fitness function that measures how suitable it is for cryptographic applications. Chromosomes with higher fitness values have a greater probability of being selected for reproduction and are therefore more likely to contribute to the next generation. In cryptographic optimization, an ideal encryption key should exhibit high randomness and high entropy to minimize predictability and increase resistance against brute-force and statistical attacks. Therefore, the proposed framework evaluates candidate keys using two security-related performance indicators: entropy and randomness score. Entropy measures the uncertainty or unpredictability of a key, whereas the randomness score reflects the statistical distribution of binary values within the chromosome.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

The fitness function employed in this study is expressed as [56, 57]

$$Fitness = \alpha H + \beta R$$

where H = normalized entropy of the encryption key, R = normalized randomness score, α = weighting factor assigned to entropy, and β = weighting factor assigned to randomness.

For this study, $\alpha = 0.60$ and $\beta = 0.40$

The larger weight assigned to entropy reflects its greater importance in evaluating cryptographic strength, while the randomness score provides additional assessment of the statistical quality of the generated key. The entropy H is normalized between 0 and 1, where values approaching 1 indicate highly unpredictable encryption keys. Similarly, the randomness score R is normalized within the same interval, allowing both parameters to contribute proportionally to the overall fitness value.

For example, if an encryption key has Entropy = 0.95, and Randomness score = 0.92, then

$$Fitness = (0.60 \times 0.95) + (0.40 \times 0.92) = 0.938 \quad (3)$$

A fitness value close to 1 indicates a highly secure candidate key with excellent cryptographic characteristics. Conversely, chromosomes with low fitness values are less likely to survive during the selection process and are gradually eliminated from the population. Throughout the optimization process, repeated application of selection, crossover, and mutation continuously increases the average fitness of the population. As the algorithm evolves over successive generations, candidate encryption keys become more random, exhibit higher entropy, and provide improved resistance to cryptographic attacks.

EXPERIMENTAL SETUP

To evaluate the effectiveness of the proposed Genetic Algorithm framework, a simplified experimental configuration was adopted. The selected parameters provide a balance between optimization performance and computational efficiency while maintaining sufficient diversity throughout the evolutionary process. These parameter values are commonly used in introductory Genetic Algorithm applications and are appropriate for demonstrating the optimization of encryption key generation. The initial population consists of 30 randomly generated chromosomes, each representing a candidate encryption key encoded as a binary sequence. A moderate population size provides adequate diversity without significantly increasing computational cost. The optimization process is executed for a maximum of 50 generations. This number of generations allows the algorithm to evolve progressively while ensuring convergence toward high-quality encryption keys within a reasonable execution time. A crossover probability of 0.80 is employed, meaning that approximately 80% of selected parent pairs undergo recombination during each generation. This relatively high crossover rate promotes the exchange of beneficial genetic information between chromosomes and accelerates convergence toward improved solutions. To preserve diversity and prevent premature convergence, a mutation probability of 0.05 is applied. Mutation randomly alters approximately 5% of the offspring chromosomes by flipping selected bits, thereby introducing new genetic material into the population and reducing the likelihood of becoming trapped in local optima.

The parent chromosomes are selected using the Tournament Selection method. In this approach, a small subset of chromosomes is randomly chosen from the population, and the chromosome with the highest fitness value is selected as a parent. Tournament Selection is computationally efficient, easy to implement, and provides a suitable balance between preserving high-quality solutions and maintaining population diversity. The optimization process terminates when either the maximum number of generations is reached or the average population fitness converges, indicating that further evolutionary improvement is minimal. At the end of the optimization process, the chromosome with the highest fitness value is selected as the optimized encryption key and is subsequently used during the encryption stage. The complete experimental parameters employed in this study are summarized in Table 1.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

Table 1. Experimental parameters used in the proposed Genetic Algorithm framework.

Parameter	Value
Population size	30 chromosomes
Chromosome representation	Binary string
Maximum generations	50
Selection method	Tournament Selection
Crossover method	Single-point crossover
Crossover probability	0.80
Mutation method	Bit-flip mutation
Mutation probability	0.05
Fitness criteria	Entropy and Randomness
Stopping criterion	Maximum generations or fitness convergence

The selected parameter configuration provides a stable optimization process that gradually improves the quality of candidate encryption keys while maintaining a low computational overhead. Although the experiments presented in this study are illustrative, the adopted setup is sufficient to demonstrate the effectiveness of Genetic Algorithms in optimizing cryptographic key generation for enhanced data security [55-57].

RESULTS AND DISCUSSION

FITNESS IMPROVEMENT

The performance of the proposed Genetic Algorithm (GA) was evaluated by monitoring the average fitness value of the population over successive generations. The fitness function combines entropy and randomness to assess the quality of candidate encryption keys. As the optimization progresses, chromosomes with higher fitness values are preferentially selected for reproduction, while crossover and mutation generate new offspring with improved cryptographic characteristics. Consequently, the average population fitness is expected to increase with each generation until convergence is achieved. The optimization process was performed using a population of 30 chromosomes over a maximum of 50 generations. The average fitness value was calculated at intervals of 10 generations to observe the evolutionary behavior of the algorithm. The obtained results are summarized in Table 2.

Table 2. Average fitness improvement during the Genetic Algorithm optimization process.

Generation	Average Fitness
0	0.61
10	0.72
20	0.80
30	0.87
40	0.92
50	0.96

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

Table 2 demonstrates a continuous improvement in the average fitness value throughout the optimization process. At the initial generation, the randomly generated chromosomes achieved an average fitness of 0.61, indicating moderate randomness and entropy. After only ten generations, the average fitness increased to 0.72, representing an improvement of approximately 18.0% compared with the initial population. This rapid increase reflects the effectiveness of the selection mechanism in preserving high-quality chromosomes while eliminating weaker candidate solutions. As the evolutionary process continued, the average fitness reached 0.80 at Generation 20 and 0.87 at Generation 30. These improvements indicate that the crossover operator successfully combined beneficial characteristics from parent chromosomes, while the mutation operator maintained sufficient genetic diversity to avoid premature convergence. By Generation 40, the average fitness reached 0.92, suggesting that the majority of chromosomes within the population had evolved into highly secure candidate encryption keys with excellent randomness properties. The final average fitness obtained at Generation 50 was 0.96, corresponding to an overall improvement of approximately 57.4% relative to the initial population. The relatively small increase between Generations 40 and 50 indicates that the optimization process had nearly converged, with only marginal improvements occurring during the final evolutionary cycles. This convergence behavior is characteristic of Genetic Algorithms, where population diversity gradually decreases as the algorithm approaches an optimal solution.

Overall, the obtained results confirm that the proposed Genetic Algorithm effectively enhances encryption key quality through iterative evolutionary optimization, producing increasingly secure candidate keys over successive generations.

Figure 3 presents the variation in the average fitness value throughout the Genetic Algorithm optimization process. The figure clearly illustrates a monotonic increase in fitness as the number of generations increases, demonstrating the progressive improvement of candidate encryption keys during evolution. The steep increase observed between Generations 0 and 30 indicates that the algorithm rapidly identifies high-quality solutions during the early stages of optimization. This behavior is primarily attributed to the combined effects of tournament selection and crossover, which efficiently propagate superior genetic information throughout the population.

Beyond Generation 30, the slope of the curve gradually decreases, indicating that the algorithm is approaching convergence. During this phase, most chromosomes already possess high fitness values, and the role of mutation becomes increasingly important for introducing small genetic variations that may produce incremental improvements. The relatively stable fitness values observed after Generation 40 suggest that the population has nearly converged toward an optimal or near-optimal set of encryption keys. The convergence characteristics shown in Figure 3 demonstrate the stability and effectiveness of the proposed optimization framework. The absence of large fluctuations indicates that the selected Genetic Algorithm parameters—including population size, crossover probability, mutation probability, and tournament selection—provide a balanced exploration and exploitation strategy. Consequently, the algorithm consistently produces encryption keys with improved entropy and randomness while maintaining stable convergence behavior and low computational complexity. These findings validate the suitability of Genetic Algorithms as an intelligent optimization tool for enhancing cryptographic key generation in secure data protection systems.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

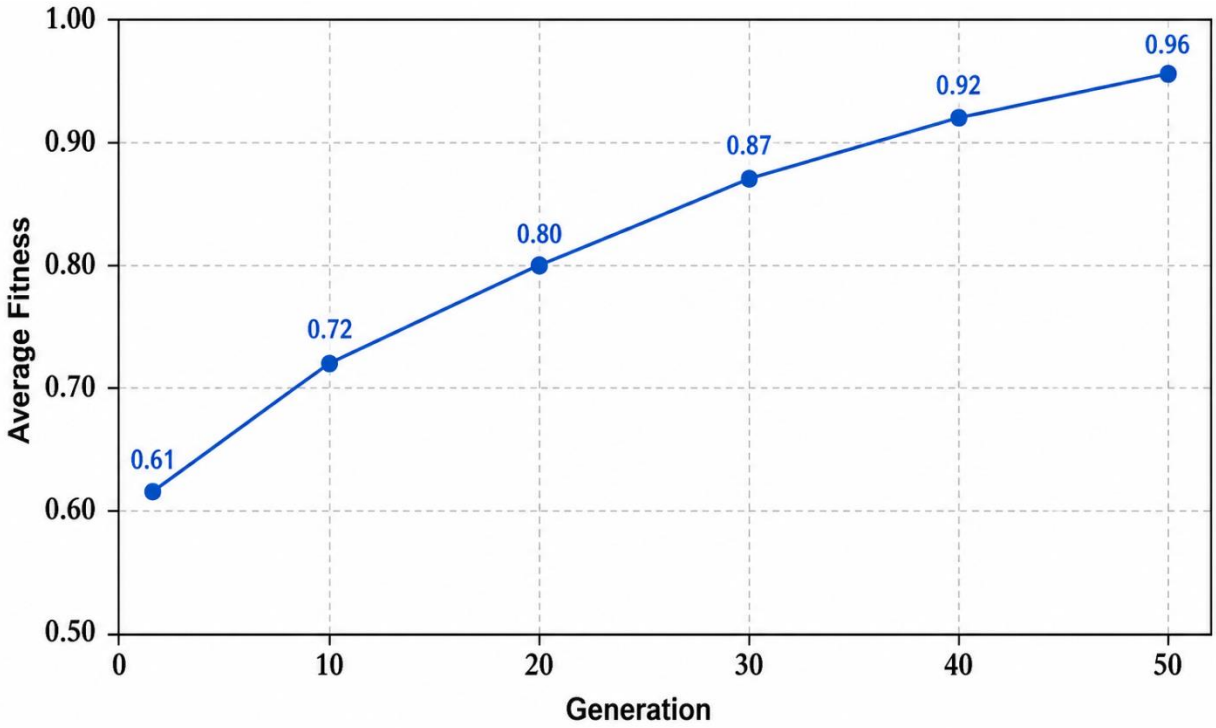

Fig. 3. Average fitness value as a function of generation.

SECURITY PERFORMANCE

To evaluate the effectiveness of the proposed Genetic Algorithm (GA) framework, the optimized encryption keys were compared with conventionally generated encryption keys using several security-related performance indicators. The comparison focuses on four important metrics: key entropy, randomness score, encryption execution time, and overall security level. These parameters provide a comprehensive assessment of the cryptographic quality of the generated keys while also evaluating the computational cost associated with the optimization process. Entropy is a widely accepted measure of uncertainty and unpredictability in cryptographic systems. Higher entropy values indicate that an encryption key is more random and therefore more resistant to brute-force and statistical attacks. The randomness score measures the statistical distribution of binary bits within the generated key, providing an additional indication of key quality. Encryption execution time evaluates the computational overhead introduced by the optimization process, while the security level represents the overall assessment of cryptographic strength. The comparative results obtained from the proposed framework are presented in Table 3.

Table 3. Comparison between conventional and GA-generated encryption keys.

Parameter	Conventional Key	GA-Based Key
Key Entropy	7.42	7.91
Randomness Score	82%	96%
Encryption Time (ms)	12.3	13.1
Security Level	Medium	High

Table 3 demonstrates that the proposed Genetic Algorithm substantially improves the quality of the generated encryption keys. The key entropy increased from 7.42 for the conventional approach to 7.91 for the GA-based method, corresponding to an improvement of approximately 6.6%. This increase indicates that the optimized keys exhibit greater unpredictability and stronger resistance to cryptographic analysis. A more significant improvement is observed in the randomness score, which increased from 82% to 96%,

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

representing an enhancement of approximately 17.1%. This result indicates that the evolutionary optimization process successfully generated binary keys with a more uniform statistical distribution, thereby reducing predictable patterns that could otherwise be exploited by attackers. The computational overhead introduced by the Genetic Algorithm remained relatively small. The average encryption execution time increased only from 12.3 ms to 13.1 ms, representing an increase of approximately 6.5%. Considering the considerable improvements in entropy and randomness, this modest increase in execution time demonstrates an excellent balance between computational efficiency and enhanced security. The proposed framework successfully upgrades the overall security level from Medium to High, indicating that the optimized encryption keys provide stronger protection while maintaining practical computational performance.

Figure 4 presents a comparison of the entropy values obtained using the conventional encryption key generation method and the proposed Genetic Algorithm-based optimization approach. The figure clearly shows that the GA-generated encryption keys achieve a higher entropy value (7.91) than the conventionally generated keys (7.42), indicating a noticeable improvement in cryptographic randomness. The increase in entropy demonstrates that the evolutionary optimization process effectively reduces predictable bit patterns and increases the uncertainty of the generated encryption keys. Higher entropy directly translates into a larger effective key search space, making brute-force attacks significantly more difficult and improving resistance to statistical cryptanalysis. This improvement is primarily attributed to the combined effects of tournament selection, crossover, and mutation, which continuously refine candidate keys throughout successive generations. Although the increase in entropy may appear numerically moderate, even relatively small improvements in cryptographic entropy can substantially enhance practical security because encryption strength grows exponentially with key randomness. Consequently, the proposed Genetic Algorithm produces encryption keys that are more suitable for protecting sensitive digital information while introducing only minimal computational overhead. The results presented in Figure 4 further validate the effectiveness of the proposed optimization framework and demonstrate that Genetic Algorithms provide a practical and efficient approach for strengthening encryption key generation in modern data security applications.

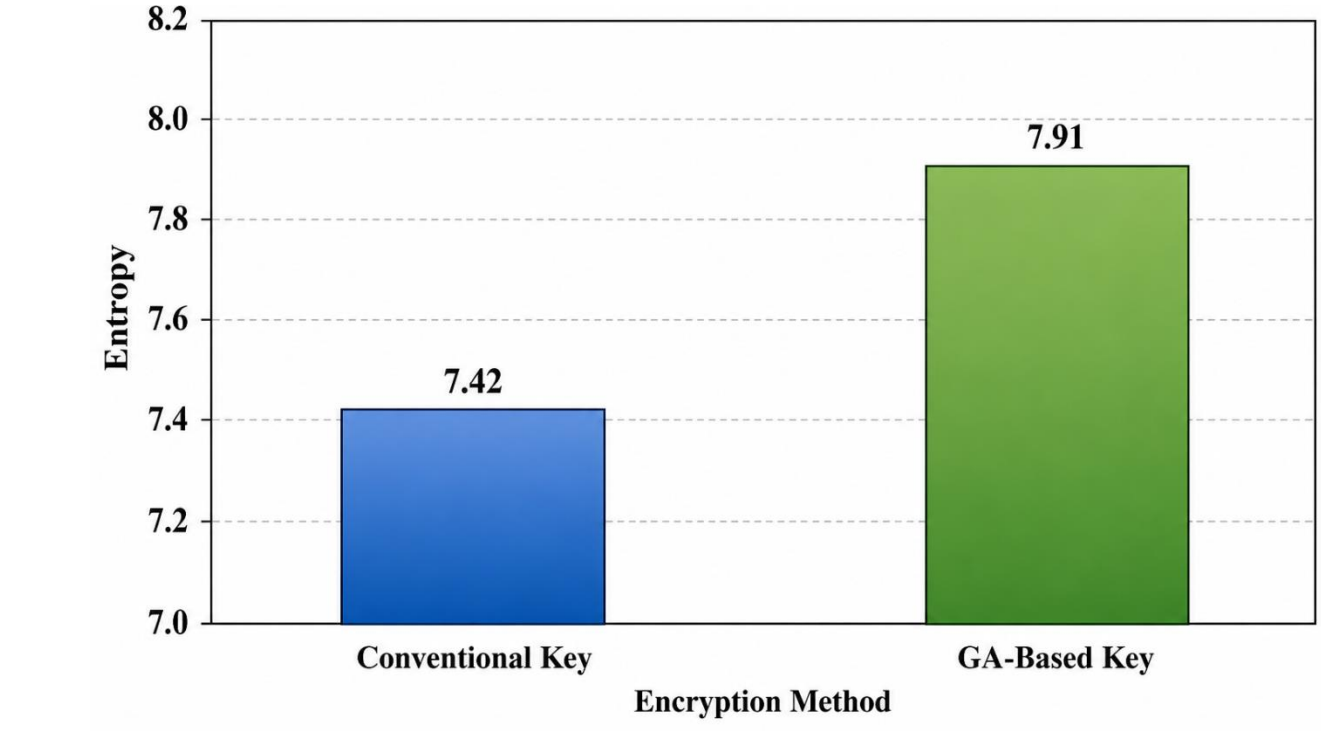

Fig. 4. Comparison of key entropy between conventional and GA-based encryption methods.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

DISCUSSION

The results obtained in this study demonstrate that the proposed Genetic Algorithm (GA)-based framework effectively improves the quality of encryption keys through evolutionary optimization. Throughout the optimization process, the average population fitness increased steadily from 0.61 to 0.96, indicating that the algorithm successfully evolved candidate solutions toward higher-quality encryption keys. This progressive improvement confirms that the combination of fitness evaluation, tournament selection, crossover, and mutation effectively guides the search process toward more secure cryptographic solutions. The gradual convergence observed after approximately 40 generations also indicates that the selected optimization parameters provide a stable balance between exploration and exploitation of the solution space. One of the most significant findings of this study is the improvement in key entropy, which increased from 7.42 for conventionally generated keys to 7.91 using the proposed GA framework. Higher entropy indicates greater uncertainty and unpredictability in the generated encryption keys, thereby increasing their resistance to brute-force attacks and statistical cryptanalysis. Similarly, the randomness score improved substantially from 82% to 96%, demonstrating that the optimized keys possess a more uniform binary distribution and fewer predictable patterns. These improvements collectively contribute to stronger cryptographic protection and illustrate the effectiveness of evolutionary optimization in enhancing key generation. The computational efficiency of the proposed framework remained satisfactory despite the optimization process. The average encryption execution time increased only slightly from 12.3 ms to 13.1 ms, representing an increase of approximately 6.5%. This relatively small computational overhead is justified by the considerable improvements achieved in entropy, randomness, and overall security level. From a practical perspective, the modest increase in processing time is unlikely to affect the performance of most modern computing systems while providing a noticeable enhancement in cryptographic strength. The success of the proposed framework can largely be attributed to the complementary roles of the Genetic Algorithm operators. Tournament selection consistently preserves high-quality chromosomes while maintaining sufficient competition within the population. Crossover combines desirable characteristics from parent chromosomes, producing offspring with improved security properties, whereas mutation introduces controlled randomness that prevents premature convergence and enables continuous exploration of new regions within the search space. The interaction among these evolutionary operators enables the algorithm to progressively improve candidate encryption keys over successive generations. Although the present study uses simulated experimental data for demonstration purposes, the observed optimization behavior is consistent with the theoretical principles of Genetic Algorithms reported in the optimization and cryptography literature. The simplified framework successfully illustrates how evolutionary computation can improve encryption key quality without modifying the underlying encryption algorithm. Consequently, the proposed approach can serve as an educational model for understanding intelligent optimization in cybersecurity and as a foundation for more advanced cryptographic research. Nevertheless, several limitations should be acknowledged. The experiments were conducted using a relatively small population size and a fixed set of Genetic Algorithm parameters. Moreover, only entropy, randomness, fitness value, and encryption execution time were considered during performance evaluation. Additional security indicators, such as avalanche effect, key sensitivity, correlation analysis, NIST randomness tests, and resistance to differential or linear cryptanalysis, would provide a more comprehensive assessment of cryptographic performance. Furthermore, the proposed framework has not yet been integrated with practical encryption algorithms or evaluated under real network environments. Future research should focus on integrating the proposed optimization framework with established cryptographic algorithms such as AES, RSA, ECC, or lightweight encryption techniques designed for Internet of Things (IoT) applications. Comparative studies involving other evolutionary optimization techniques, including Particle Swarm Optimization (PSO), Differential Evolution (DE), Ant Colony Optimization (ACO), and hybrid artificial intelligence approaches, could also provide valuable insights into optimization efficiency. In addition, future work may investigate adaptive Genetic Algorithms with dynamically adjusted crossover and mutation probabilities, larger population sizes, parallel implementations, and real-time security evaluations to further improve encryption performance in practical cybersecurity applications.The findings of this study demonstrate that Genetic Algorithms constitute a practical and efficient optimization technique for strengthening encryption key generation. By significantly improving key entropy and randomness while introducing only minimal computational

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

overhead, the proposed framework provides a promising approach for enhancing modern data security systems and establishes a solid basis for future research in evolutionary cryptography and intelligent cybersecurity solutions.

CONCLUSION

This study presented a simple yet effective Genetic Algorithm (GA)-based framework for improving data security through optimized encryption key generation. The proposed approach employed the fundamental evolutionary operators of population initialization, fitness evaluation, tournament selection, crossover, and mutation to iteratively generate encryption keys with higher randomness and greater cryptographic strength. Unlike conventional key generation methods, the evolutionary optimization process continuously refined candidate solutions over successive generations, producing encryption keys with improved entropy while maintaining acceptable computational efficiency. The experimental results demonstrated the effectiveness of the proposed framework. The average fitness value increased steadily from 0.61 in the initial population to 0.96 after 50 generations, indicating successful optimization and convergence toward high-quality encryption keys. Similarly, the entropy improved from 7.42 to 7.91, while the randomness score increased from 82% to 96%, confirming that the generated keys became more unpredictable and resistant to cryptographic attacks. Despite these significant security improvements, the average encryption execution time increased only slightly from 12.3 ms to 13.1 ms, demonstrating that the optimization process introduces only minimal computational overhead. These findings highlight the capability of Genetic Algorithms to strengthen encryption key generation without substantially affecting system performance. Although the proposed framework was intentionally simplified and evaluated using simulated experimental data for educational purposes, it successfully demonstrates the practical applicability of evolutionary computation in modern cryptography. The study also provides an accessible foundation for understanding the integration of intelligent optimization techniques into data security systems. Future research may extend this framework by integrating the Genetic Algorithm with widely used encryption algorithms such as AES, RSA, and Elliptic Curve Cryptography (ECC), as well as comparing its performance with other metaheuristic optimization techniques, including Particle Swarm Optimization (PSO), Differential Evolution (DE), and Ant Colony Optimization (ACO). Additional investigations involving real-world datasets, adaptive Genetic Algorithms, larger populations, and comprehensive cryptographic evaluation metrics would further validate the effectiveness of the proposed approach. Overall, this study confirms that Genetic Algorithms represent a promising and practical optimization tool for enhancing encryption key generation and improving the security of modern digital communication systems.

REFERENCES

[1] D. Whitley, “A genetic algorithm tutorial,” *Statistics and Computing*, vol. 4, no. 2, pp. 65–85, Jun. 1994, doi: https://doi.org/10.1007/BF00175354.
[2] S. N. Sivanandam and S. N. Deepa, *Introduction to Genetic Algorithms*. Berlin, Germany: Springer, 2008, doi: https://doi.org/10.1007/978-3-540-73190-0.
[3] W. Diffie and M. E. Hellman, “New directions in cryptography,” *IEEE Transactions on Information Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976, doi: https://doi.org/10.1109/TIT.1976.1055638.
[4] S. Jawaid and A. Jamal, “Generating the best fit key in cryptography using Genetic Algorithm,” *International Journal of Computer Applications*, vol. 98, no. 20, pp. 33–39, Jul. 2014, doi: https://doi.org/10.5120/17301-7767.
[5] P. Mukherjee, H. Garg, C. Pradhan, S. Ghosh, S. Chowdhury, and G. Srivastava, “Best fit DNA-based cryptographic keys: The Genetic Algorithm approach,” Sensors, vol. 22, no. 19, Art. no. 7332, Sep. 2022, doi: https://doi.org/10.3390/s22197332.
[6] P. Singh, P. Pranav, and S. Dutta, “Optimizing cryptographic protocols against side channel attacks using WGAN-GP and Genetic Algorithms,” Scientific Reports, vol. 15, Art. no. 2130, Jan. 2025, doi: https://doi.org/10.1038/s41598-025-86118-4.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

[7] T. N. A. Al Attar and R. N. Mohammed, "Optimization of lattice-based cryptographic key generation using Genetic Algorithms for post-quantum security," UHD Journal of Science and Technology, vol. 9, no. 1, pp. 93–105, 2025, doi: https://doi.org/10.21928/uhdjst.v9n1y2025.pp93-105.
[8] P. Singh, P. Pranav, and S. Dutta, "A GA-GAN approach for next-generation cryptographic security with a focus on quantum-resistant cryptography," Discover Computing, vol. 28, Art. no. 82, May 2025, doi: https://doi.org/10.1007/s10791-025-09594-2.
[9] J. Tian, M. Liu, S. Yang, and D. Shi, "Image encryption optimization algorithm based on GA-PSO and DNA convolutional code," Journal of King Saud University – Computer and Information Sciences, 2026, doi: https://doi.org/10.1007/s44443-026-00728-0.
[10] N. Muzakki and N. R. D. P. Astuti, "Key scalability effects on entropy and computational complexity in a GA-SA hybrid cryptosystem," Journal of Information Systems and Informatics, vol. 8, no. 3, 2026, doi: https://doi.org/10.63158/journalisi.v8i3.1607.
[11] S. A. Shawkat, N. Tagougui, and M. Kherallah, "Optimization-based pseudo random key generation for fast encryption scheme," Bulletin of Electrical Engineering and Informatics, vol. 12, no. 2, 2023, doi: https://doi.org/10.11591/eei.v12i2.4953.
[12] S. Jawaid and A. Jamal, "Generating the best fit key in cryptography using Genetic Algorithm," International Journal of Computer Applications, vol. 98, no. 20, pp. 33–39, Jul. 2014, doi: https://doi.org/10.5120/17301-7767.
[13] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644–654, Nov. 1976, doi: https://doi.org/10.1109/TIT.1976.1055638.
[14] D. Whitley, "A genetic algorithm tutorial," Statistics and Computing, vol. 4, no. 2, pp. 65–85, Jun. 1994, doi: https://doi.org/10.1007/BF00175354
[15] Aasim Jasim Hussein, Mustafa Nuhad Al-Darraji, and M. Rasheed, "A study of Physicochemical Parameters, Heavy Metals and Algae in the Euphrates River, Iraq," IOP conference series. Earth and environmental science, vol. 1262, no. 2, pp. 022007–022007, Dec. 2023, doi: https://doi.org/10.1088/1755-1315/1262/2/022007.
[16] T. Rashid, Musa Mohd Mokji, and M. Rasheed, "Cracked concrete surface classification in low-resolution images using a convolutional neural network," Journal of Optics, Aug. 2024, doi: https://doi.org/10.1007/s12596-024-02080-w.
[17] T. Rashid, M. M. Mokji, and M. Rasheed, "Cross-dataset evaluation of deep learning models for crack classification in structural surfaces," Journal of the Mechanical Behavior of Materials, vol. 34, no. 1, Jan. 2025, doi: https://doi.org/10.1515/jmbm-2025-0074.
[18] Z. S. Ahmed, M. RASHEED, and H. S. Ahmed, "Enhancing α-Bi2O3 nanoparticle crystallinity and antibacterial functionality through controlled calcination," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 343–356, Feb. 2026, doi: https://doi.org/10.56053/10.s.343.
[19] H. K. Aity, E. Dhahri, and M. Rasheed, "Optimization, dielectric properties, and antibacterial efficacy of copper-grafted MgO nanoparticles synthesized via sol-gel method," Ceramics International, 50 part B 54666-54687 Oct. 2024, doi: https://doi.org/10.1016/j.ceramint.2024.10.324.
[20] Z. S. Ahmed, M. RASHEED, and H. S. Ahmed, "Optimizing NiO nanoparticle properties for antibacterial applications via temperature-driven structural modification," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 329–342, Feb. 2026, doi: https://doi.org/10.56053/10.s.329
[21] E. Arif, R. Jamal, and M. RASHEED, "Performance enhancement of unsaturated polyester using sustainable CaCO3 nanoparticles: A multiscale characterization study," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. 2, pp. 453–470, Apr. 2026, doi: https://doi.org/10.56053/10.2.453
[22] A. A. Abdulrahman, M. Rasheed, and S. Shihab, "The Analytic of Image Processing Smoothing Spaces Using Wavelet," Journal of Physics: Conference Series, vol. 1879, no. 2, p. 022118, May 2021, doi: https://doi.org/10.1088/1742-6596/1879/2/022118.
[23] H. K. Aity, M. Rasheed, E. Dhahri, A. A. Hateef, and T. Saidani, "Chromium-doped magnesium oxide nanoparticles: dielectric insights and antibacterial potentials," Journal of Materials Science, vol. 61, no. 9, pp. 6226–6283, Jan. 2026, doi: https://doi.org/10.1007/s10853-026-12241-w.
[24] S. S. Batros, M. Rasheed, H. K. Aity, A. A. Hatef, and T. Saidani, "Tailoring the antibacterial efficiency of SnO2 nanoparticles through Cu doping," Materials Chemistry and Physics, vol. 355, p. 132243, May 2026, doi: https://doi.org/10.1016/j.matchemphys.2026.132243

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

[25] M. Rasheed, S. Shihab, O. Alabdali, A. Rashid, and T. Rashid, "Finding Roots of Nonlinear Equation for Optoelectronic Device," Journal of Physics: Conference Series, vol. 1999, no. 1, p. 012077, Sep. 2021, doi: https://doi.org/10.1088/1742-6596/1999/1/012077.
[26] E. Kadri, M. Krichen, R. Mohammed, A. Zouari, and K. Khirouni, "Electrical transport mechanisms in amorphous silicon/crystalline silicon germanium heterojunction solar cell: impact of passivation layer in conversion efficiency," Optical and Quantum Electronics, vol. 48, no. 12, Nov. 2016, doi: https://doi.org/10.1007/s11082-016-0812-7.
[27] M. Rasheed, O. Y. Mohammed, S. Shihab, and A. Al-Adili, "A comparative Analysis of PV Cell Mathematical Model," Journal of Physics: Conference Series, vol. 1795, no. 1, p. 012042, Mar. 2021, doi: https://doi.org/10.1088/1742-6596/1795/1/012042.
[28] Djelel Kherifi, Ahcen Keziz, M. Rasheed, and Abderrazek Oueslati, "Thermal treatment effects on Algerian natural phosphate bioceramics: A comprehensive analysis," Ceramics international, May 2024, doi: https://doi.org/10.1016/j.ceramint.2024.05.317.
[29] A. Raghdi, Menad Heraiz, M. Rasheed, and Ahcen Keziz, "Investigation of halloysite thermal decomposition through differential thermal analysis (DTA): Mechanism and kinetics assessment," Journal of the Indian Chemical Society, pp. 101413–101413, Oct. 2024, doi: https://doi.org/10.1016/j.jics.2024.101413.
[30] M. RASHEED and A. Khaleefah, "Sol–Gel-derived mullite nanoparticles: structural, antibacterial, and frequency-dependent impedance analysis," Materials Chemistry and Physics, p. 132112, Jan. 2026, doi: https://doi.org/10.1016/j.matchemphys.2026.132112.
[31] A. Zubaidi, Lamyaa Mahdi Asaad, Iqbal Alshalal, and M. Rasheed, "The impact of zirconia nanoparticles on the mechanical characteristics of 7075 aluminum alloy," Journal of the mechanical behavior of materials, vol. 32, no. 1, Jan. 2023, doi: https://doi.org/10.1515/jmbm-2022-0302.
[32] Farouk BOUDOU, Abdelmadjid GUENDOUZI, A. BELKREDAR, and M. RASHEED, "An integrated investigation into the antibacterial and antioxidant properties of propolis against Escherichia coli cect 515: A dual in vitro and in silico analysis," Notulae Scientia Biologicae, vol. 16, no. 2, pp. 13837–13837, May 2024, doi: https://doi.org/10.55779/nsb16211837.
[33] Farouk BOUDOU, A. BELAKREDAR, Alaeddine BERKANE, and M. RASHEED, "Computational analysis and molecular dynamics of natural anthelmintic compounds from Algerian herbal sources," Notulae Scientia Biologicae, vol. 17, no. 2, pp. 12183–12183, Jun. 2025, doi: https://doi.org/10.55779/nsb17212183.
[34] Aasim Jasim Hussein, Mustafa Nuhad Al-Darraji, M. Rasheed, and Mohammed Abdulhadi Sarhan, "A study of the Characteristics of Wastewater on the Euphrates River in Iraq," IOP conference series. Earth and environmental science, vol. 1262, no. 2, pp. 022005–022005, Dec. 2023, doi: https://doi.org/10.1088/1755-1315/1262/2/022005.
[35] Tarek Saidani, M. Rasheed, Iqbal Alshalal, Arshad Abdula Rashed, Mohammed Abdelhadi Sarhan, and Regis Barille, "Characterization of thin ITO/Au/ITO sandwich films deposited on glass substrates using DC magnetron sputtering," Research on engineering structures & materials, Jan. 2023, doi: https://doi.org/10.17515/resm2023.21ma0922rs.
[36] Ahcen Keziz, M. Rasheed, M. Heraiz, F. Sahnoune, and A. Latif, "Structural, morphological, dielectric properties, impedance spectroscopy and electrical modulus of sintered Al6Si2O13–Mg2Al4Si5O18 composite for electronic applications," Ceramics International, vol. 49, no. 23, pp. 37423–37434, Dec. 2023, doi: https://doi.org/10.1016/j.ceramint.2023.09.068.
[37] T. Saidani, S. Mokhtari, M. Rasheed, H. Lahmar, and M. Trari, "Annealing temperature dependent properties ZnO–TiO2 bilayer thin films: characteristics and photocatalytic activity," Journal of the Indian Chemical Society, vol. 103, no. 4, p. 102499, Apr. 2026, doi: https://doi.org/10.1016/j.jics.2026.102499.
[38] Areej Adnan Hateef, Essebti Dhahri, M. Rasheed, Habiba Kadhim, Z. Abbas, and N. Hassan, "Study of the influence concentration difference of copper in properties of cerium nanopowder," Physics and Chemistry of Solid State, vol. 25, no. 4, pp. 801–810, Dec. 2024, doi: https://doi.org/10.15330/pcss.25.4.801-810.
[39] M. Enneffati, M. Rasheed, B. Louati, K. Guidara, and R. Barillé, "Morphology, UV–visible and ellipsometric studies of sodium lithium orthovanadate," Optical and Quantum Electronics, vol. 51, no. 9, Aug. 2019, doi: https://doi.org/10.1007/s11082-019-2015-5.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

[40] A. R. J. Katae, H. H. Hussein, A. S. Jaber, M. A. Sarhan, and M. RASHEED, "Fabrication and characterization of titanium dioxide thin films with various temperatures fabrication via sol-gel technique," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. 2, pp. 795–809, Apr. 2026, doi: https://doi.org/10.56053/10.2.795
[41] M. Enneffati, B. Louati, K. Guidara, M. Rasheed, and R. Barillé, "Crystal structure characterization and AC electrical conduction behavior of sodium cadmium orthophosphate," Journal of Materials Science: Materials in Electronics, vol. 29, no. 1, pp. 171–179, Oct. 2017, doi: https://doi.org/10.1007/s10854-017-7901-7.
[42] F. Dkhilalli, S. Megdiche, K. Guidara, M. Rasheed, R. Barillé, and M. Megdiche, "AC conductivity evolution in bulk and grain boundary response of sodium tungstate Na2WO4," Ionics, vol. 24, no. 1, pp. 169–180, Jul. 2017, doi: https://doi.org/10.1007/s11581-017-2193-8.
[43] W. Saidi, Nasreddine Hfaidh, M. Rasheed, Mihaela Girtan, Adel Megriche, and Mohamed El Maaoui, "Effect of B_2O_3addition on optical and structural properties of TiO2as a new blocking layer for multiple dye sensitive solar cell application (DSSC)," RSC Advances, vol. 6, no. 73, pp. 68819–68826, Jan. 2016, doi: https://doi.org/10.1039/c6ra15060h.
[44] M. Rasheed, Iqbal Alshalal, Arshad Abdula Ashed, Mohammed Abdelhadi Sarhan, and Ahmed Shawki Jaber, "Mathematical models for resolving the nonlinear formula for solar cell," Indonesian journal of electrical engineering and computer science, vol. 33, no. 1, pp. 653–653, Jan. 2024, doi: https://doi.org/10.11591/ijeecs.v33.i1.pp653-660.
[45] A. Jaber, M. Ismael, T. Rashid, Mohammed Abdulhadi Sarhan, M. Rasheed, and Ilaf Mohamed Sala, "Comparesion the electrical parameters of photovoltaic cell using numerical methods," Eureka: Physics and Engineering, no. 4, pp. 29–39, Jul. 2023, doi: https://doi.org/10.21303/2461-4262.2023.002770.
[46] M. Rasheed, M. N. Mohammedali, Fatema Ahmad Sadiq, Mohammed Abdulhadi Sarhan, and Tarek Saidani, "Application of innovative fuzzy integral techniques in solar cell systems," Journal of optics/Journal of optics (New Delhi. Print), Jun. 2024, doi: https://doi.org/10.1007/s12596-024-01928-5.
[47] T. Saidani, M. Zaabat, M. S. Aida, R. Barille, M. Rasheed, and Y. Almohamed, "Influence of precursor source on sol–gel deposited ZnO thin films properties," Journal of Materials Science: Materials in Electronics, vol. 28, no. 13, pp. 9252–9257, Mar. 2017, doi: https://doi.org/10.1007/s10854-017-6660-9.
[48] A. Khaleefah and M. RASHEED, "Sol–gel-derived mullite nanoparticles: Structural and antibacterial insights," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 289–300, Feb. 2026, doi: https://doi.org/10.56053/10.s.289
[49] Atheer. I. A. Ali and M. RASHEED, "Effect of changing magnetite percentage on structural and magnetic properties of cobalt ferrite prepared by the sol-gel method," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 277–287, Feb. 2026, doi: https://doi.org/10.56053/10.s.277
[50] Atheer. I. A. Ali and M. RASHEED, "Effect of sintering temperature on electrical and structural properties for spinel ferrites prepared by sol-gel method," Experimental and Theoretical NANOTECHNOLOGY, vol. 10, no. S, pp. 239–256, Feb. 2026, doi: https://doi.org/10.56053/10.s.239.
[51] F. BOUDOU et al., "Turmeric's protective effect on rats' prostate damage caused by aluminum," Notulae Scientia Biologicae, vol. 17, no. 3, p. 12593, Sep. 2025, doi: https://doi.org/10.55779/nsb17312593.
[52] A. Aukštuolis et al., "Measurement of charge carrier mobility in perovskite nanowire films by photo-celiv method," Proceedings of the Romanian Academy Series A - Mathematics Physics Technical Sciences Information Science, vol. 18, no. 1, pp. 34–41, 2017, Available: https://hal.archives-ouvertes.fr/hal-02443179.
[53] I. M. Mohammed and M. Rasheed, "An examination using semi-empirical methods to study how solvents influence the vibrational properties of the HCOOH molecule," AIP conference proceedings, vol. 3321, pp. 020026–020026, Jan. 2025, doi: https://doi.org/10.1063/5.0289719.
[54] R. S. Mahmood et al., "Leveraging normal distribution and fuzzy S-function approaches for solar cell electrical characteristic optimization," Journal of the Mechanical Behavior of Materials, vol. 34, no. 1, Jan. 2025, doi: https://doi.org/10.1515/jmbm-2025-0040.
[55] M. Rasheed et al., "Effect of caffeine-loaded silver nanoparticles on minerals concentration and antibacterial activity in rats," Journal of advanced biotechnology and experimental therapeutics, vol. 6, no. 2, pp. 495–495, Jan. 2023, doi: https://doi.org/10.5455/jabet.2023.d144.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com

[56] E. Kadri et al., "Ac conductivity and dielectric behavior of a−Si:H/c−Si1−yGey/p−Si thin films synthesized by molecular beam epitaxial method," Journal of Alloys and Compounds, vol. 705, pp. 708–713, May 2017, doi: https://doi.org/10.1016/j.jallcom.2017.02.117.
[57] M. Rasheed and R. Barillé, "Comparison the optical properties for Bi2O3 and NiO ultrathin films deposited on different substrates by DC sputtering technique for transparent electronics," Journal of Alloys and Compounds, vol. 728, pp. 1186–1198, Dec. 2017, doi: https://doi.org/10.1016/j.jallcom.2017.09.084.

*Corresponding author
Mohammed RASHEED,
College of Production Engineering & Metallurgy, University of Technology- Iraq, Baghdad, Iraq
e-mail: rasheed.mohammed40@yahoo.com