International Journal of Innovative Research and Scientific Studies, 8(4) 2025, pages: 507-515

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Integration of El-Gamal cryptosystem and AI to enhance cyber defence

Zhanerke Temirbekova[1], Rat Berdibayev[2], Sakhybay Tynymbayev[3], Alimzhan Baikenov[4*], Guldiana Yermekova[5]

[1,5]*Al-Farabi Kazakh National University, Almaty, Kazakhstan.*
[2,4]*Almaty University of Power Engineering and Telecommunications named after G. Daukeyev, Almaty, Kazakhstan.*
[3]*Internationat IT University (IITU), Almaty, Kazakhstan.*

Corresponding author: Alimzhan Baikenov (*Email: a.baikenov@aues.kz*)

Abstract

The purpose of this study is to develop a secure biometric data protection system that integrates artificial intelligence and cryptographic techniques to enhance data privacy and integrity. The proposed system employs a convolutional neural network (CNN) to extract features from multimodal biometric inputs, including facial images, retinal scans, and fingerprints. A generative adversarial network (GAN) is then trained on these features to produce synthetic biometric representations that closely mimic real data. To ensure confidentiality and authenticity, the El-Gamal cryptosystem is used to encrypt both the features and the biometric images, while a digital signature mechanism based on the SHA-256 hash function secures the data against tampering. The CNN achieved a classification accuracy above 99.8%, with GAN training stabilizing at a discriminator loss of approximately 0.3 and a generator loss of around 4.0. The encryption and signature verification processes demonstrated consistent success, confirming the robustness of the pipeline. This research concludes that the integrated approach is effective in safeguarding biometric data against forgery and unauthorized access. Practically, it provides a viable solution for secure transmission and storage in biometric authentication systems, with strong potential for deployment in high-security environments.

Keywords: Artificial Intelligence, Biometric data, Cybersecurity, El-Gamal cryptosystem, Machine learning.

DOI: 10.53894/ijirss.v8i4.7878
Funding: This study received no specific financial support.
History: Received: 6 May 2025 / **Revised:** 6 June 2025 / **Accepted:** 10 June 2025 / **Published:** 18 June 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

In today's digital society, information is a strategically vital resource affecting nearly all areas of human activity. The increasing reliance on digital infrastructure has transformed business operations, public services, and interpersonal

communications. Among the most critical aspects of this transformation is the security of biometric data, which includes facial images, fingerprints, and retinal scans. Biometric systems are widely deployed for user authentication and access control due to their convenience and accuracy.

However, the emergence of malware and new attack methods poses significant threats to the security of biometric data. A comprehensive approach to protecting this information includes the use of cryptographic techniques, such as the El-Gamal algorithm, as well as the implementation of artificial intelligence-based solutions for detecting and preventing attacks.

The objective of this study is to design and evaluate a secure biometric data protection system that integrates artificial intelligence (AI) and cryptographic techniques to enhance data privacy and robustness against attacks.

The core problem addressed in this research is the vulnerability of biometric data to spoofing, replay attacks, and unauthorized access, particularly due to the limitations of conventional encryption and static biometric templates.

The research gap lies in the lack of comprehensive solutions that combine advanced machine learning methods (such as CNN and GAN) with asymmetric encryption systems to ensure both the security and adaptability of biometric authentication systems. While prior work has demonstrated the effectiveness of AI and cryptographic approaches separately, few studies have developed integrated frameworks with proven performance across multiple biometric modalities.

This study is guided by the following research questions:

1. Can deep learning techniques (CNNs and GANs) effectively enhance the robustness and adaptability of biometric feature extraction and synthesis?
2. How does the integration of the El-Gamal cryptosystem improve the confidentiality and integrity of biometric data?
3. What are the practical performance metrics (accuracy, encryption reliability, resistance to attacks) of the proposed AI–crypto-based biometric system?

In today's digital environment, there is a rapid increase in various types of cyberattacks, posing significant threats to both individual users and organizations worldwide. Based on the data presented (see Figure 1), it is possible to identify four primary categories of cyber threats: malicious software (malware), social engineering attacks, system hacking, and ransomware attacks.

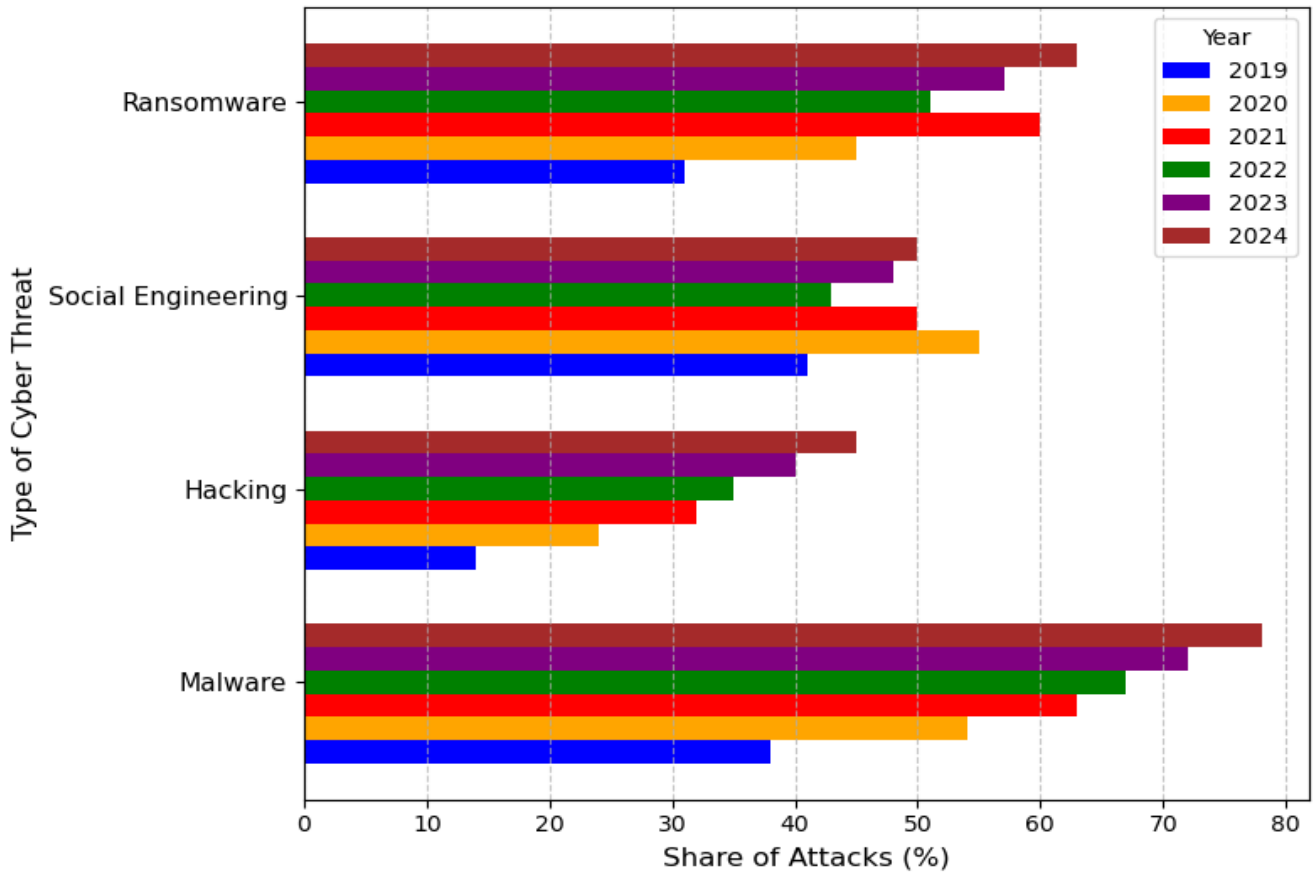

Figure 1.
Share of Different Types of Cyberattacks by Year.

The diagram illustrates the dynamics of the distribution of various types of cyberattacks from 2019 to 2024. Malware consistently holds the largest share among all threats, indicating its high effectiveness and adaptability to modern security systems. This type of attack remains the most prevalent throughout the entire period under consideration.

There is also a significant increase in ransomware attacks, which block access to data and demand a ransom for its recovery. This type of threat is becoming increasingly dangerous, particularly for corporate and governmental organizations. Social engineering methods, including phishing attacks, are also widely used by hackers, as they allow them to circumvent

technical security measures by exploiting the human factor. In addition, there has been an increase in system hacking attacks, indicating the continuous advancement of tools designed to exploit vulnerabilities in software.

Based on this, the analysis of the presented data confirms the need to develop and implement more sophisticated protection mechanisms, including adaptive threat detection methods using artificial intelligence.

To address these questions, the research follows a structured methodology:

- A convolutional neural network (CNN) is implemented to extract key features from facial, fingerprint, and retinal images.
- A generative adversarial network (GAN) is trained to produce synthetic biometric samples.
- The El-Gamal cryptosystem is used for encryption and digital signatures.
- The system is evaluated using publicly available biometric datasets.

This paper is organized as follows: Section 2 provides a literature review on biometric encryption and AI applications in security. Section 3 outlines the proposed methodology. Section 4 presents and discusses the results. Section 5 concludes with implications, limitations, and future directions.

2. Literature Review

Modern security systems increasingly rely on biometric authentication, which uses unique physiological or behavioral traits to verify identity. However, despite the effectiveness of existing biometric systems, they face problems such as spoofing, repeated attacks, and the vulnerability of stored biometric data. In this regard, the relevant direction is the integration of artificial intelligence (AI) with biometric encryption systems to increase their security.

In Zahoor [1], the integration of AI into biometric encryption systems is investigated in order to increase the reliability of authentication. The authors emphasize the need for continuous improvement of authentication mechanisms in the face of the growing complexity of cyber threats and potential vulnerabilities of biometric data. In particular, the application of machine learning algorithms is being considered. Supervised learning using labeled datasets allows AI systems to recognize patterns in biometric data for accurate identification; examples of such algorithms are support vector machines (SVMs), random forests, and neural networks. In cases where the labeled data is limited, unsupervised learning, such as clustering algorithms (such as k-means or hierarchical clustering), can be used to identify similar biometric patterns, which is useful for detecting anomalies and potential threats. In addition, autoencoders can be used to extract features from biometric data before encryption, which compresses the data while preserving essential authentication information.

The study showed that the proposed biometric encryption system with AI demonstrates improvements in accuracy of 15-20%, an increase in data processing speed of 30%, and a decrease in the probability of false positives of 25%. A quantitative assessment of the effectiveness confirms the potential for creating universal authentication systems with a high degree of security.

Another area of research is devoted to the development of new image encryption methods using artificial neural networks (ANN). The article Panigrahy et al. [2] proposes a fast and reliable image encryption method based on ANN with an improved structural similarity index (SSIM). The authors note that the existing data encryption mechanisms have disadvantages, which require further research. The algorithm proposed in this paper is non-recursive, ensuring both forward and reverse secrecy, as well as optimal preservation of image quality after encryption.

Experiments have shown that the proposed method is resistant to statistical and differential attacks, as confirmed by the chi-square (χ^2) test, correlation analysis, and robustness testing against noise-based attacks. The NIST test results for the "Lena" image demonstrated the randomness of the generated sequence. Compared to other encryption methods, the proposed approach achieved an NPCR value of 99.62%, a UACI of 33.45%, a correlation coefficient of 0.001, and an image entropy of 7.999, all of which confirm its strong resistance to various types of attacks.

In Kumari [3], the work explores the combination of the MVK algorithm, the El-Gamal cryptosystem and chaotic systems for image encryption. The MVK algorithm is used to shuffle the pixels of an image in order to reduce the correlation between neighboring pixels. The El-Gamal cryptosystem, which is an asymmetric algorithm, is used directly for encryption. Chaotic Lorenz and Rössler systems are used to generate cryptographic keys and enhance security by increasing the entropy of an encrypted image.

The study demonstrated that the proposed scheme is resistant to statistical, differential, and brute-force attacks. Analysis of entropy, histograms, NPCR, PSNR, and MSE confirmed a high level of data protection. The entropy values reached 7.999, the PSNR was 10.23 dB, and the NPCR was 99.58%. Key sensitivity tests showed that even minimal changes to the keys make decryption impossible, which significantly enhances the security level of the system.

The article Qin and Zhang [4] offers a comprehensive model for encryption and authentication of biometric images while maintaining confidentiality, using the three-dimensional Arnold transform for spatial mixing of pixels and the El-Gamal encryption algorithm for cryptographic protection. El-Gamal's digital signature is used to ensure the integrity and authenticity of biometric data. The authors emphasize the advantages of using a public-key cryptosystem such as El-Gamal for key management and security. The proposed combination of methods aims to solve problems related to the secure transfer, storage, and verification of biometric images, as well as countering attempts at unauthorized access and forgery. The attack resistance analysis showed high GVD values (0.98), which indicate a significant difference between the original and encrypted images, and low PSNR values (9.75 dB) confirm the effectiveness of the method. Experiments with Gaussian noise and "anti-salt and pepper" noise have shown the method's high resistance to attacks.

The study Gumanti et al. [5] explores image super-encryption on Android by combining the BASE64 algorithm with the El-Gamal cryptosystem. BASE64 is used to encode data into ASCII format, while the asymmetric El-Gamal algorithm is applied for subsequent encryption using public and private keys. The proposed scheme aims to enhance image security

through multi-layered encryption. The authors describe the key generation, encryption, and decryption procedures involved in the combined algorithm approach. Although specific results and performance metrics are not provided in the study, the proposed method demonstrates potential for securing images in mobile applications.

Based on the analysis of existing scientific publications, the present study applied machine learning methods in combination with cryptographic algorithms to build a biometric cryptosystem. The El-Gamal scheme integrated with neural network architectures was used as the basic cryptographic mechanism, which provided an increased level of security for biometric data.

As part of the proposed approach, biometric features were extracted using a convolutional neural network, which made it possible to identify key features of the images. To increase resistance to attacks and ensure the uniqueness of patterns, a generative adversarial network was used, which generated variations in the source data. The obtained attributes were encrypted using the El-Gamal algorithm, which ensured confidentiality and resistance to unauthorized access. At the verification stage, the system decrypted the stored data and compared it with the reference biometric characteristics.

The results of the conducted work confirmed that the integration of deep learning methods with asymmetric cryptosystems enables the development of reliable biometric protection that is resistant to various types of attacks and the compromise of biometric templates.

In conclusion, the reviewed studies highlight the growing importance of combining artificial intelligence and cryptography for robust biometric protection. However, most existing works lack an integrated pipeline that covers feature extraction, synthetic data generation, encryption, and authentication. This study addresses these gaps by proposing a comprehensive framework that unifies deep learning and El-Gamal encryption for enhanced cyber defense.

3. Methods

3.1. Research Design

This research adopts an experimental design approach aimed at constructing and evaluating a secure biometric data protection system based on the integration of artificial intelligence and cryptographic methods. The core of the system lies in combining convolutional neural networks (CNNs), generative adversarial networks (GANs), and the El-Gamal cryptosystem. The integration of these technologies allows for the extraction, transformation, encryption, and authentication of biometric data in a privacy-preserving and secure manner. The model was tested using publicly available datasets that cover facial images, fingerprints, and retinal scans.

3.2. Techniques Used

As part of the research, a secure biometric data processing and storage system was developed based on the integration of convolutional neural networks, generative adversarial networks and the El-Gamal cryptosystem.

Convolutional neural networks are widely used in computer vision systems, especially in biometric identification and security tasks. Thanks to their ability to automatically extract and interpret complex features from images, CNNs are used to recognize faces, fingerprints, irises, and other unique biometric characteristics. This is especially important in the context of an increasing number of attacks on authentication systems, where both high accuracy and data processing speed are required.

The main components of CNN are convolutional layers that extract spatial and statistical features, as well as subsampling (pooling) layers that reduce dimensionality and focus on the most significant elements of the image [6].

In biometric systems, convolutional neural networks (CNNs) demonstrate high identification accuracy and robustness to variations in angle, lighting, partial occlusions, and other distortions. These qualities make CNNs particularly well-suited for real-world applications, where the quality of input data may be inconsistent. Depending on the task, architectures may include dozens of convolutional layers, normalization mechanisms, dropout, and residual connections (as in ResNet), allowing for the construction of deep models without compromising training stability.

A comparison of popular neural network architectures in terms of applicability in biometrics is presented in the Table 1.

Table 1.
Comparative analysis of neural network architectures.

Architecture	Network Type	Applicability to Biometrics	Robustness to Distortions	Training Time (Epochs)	Feature Output Vector
CNN (ResNet)	Convolutional	High	High	20–50	128–512
MLP	Fully Connected	Low	Low	10–20	Variable
Autoencoder	Encoding	Medium	Medium	30–50	64–256
Vision Transformer	Transformer	Promising	Very High	100+	512+

One of the key advantages of CNNs is their ability to extract features without the need for manually designed filters. The network learns from examples, automatically discovering optimal convolutional kernels that most effectively capture the visual characteristics of a biometric object. This is critically important when working with biometric images, where the accuracy of the template directly impacts the reliability of authentication.

Generative Adversarial Networks represent one of the most significant breakthroughs in machine learning over the past decade and are widely applied in enhancing the security of biometric systems. Their key feature is the ability to generate synthetic data that is virtually indistinguishable from real data, making them especially valuable in the context of protecting

personal information. When combined with cryptography and convolutional neural networks, GANs open new horizons for building secure and intelligent authentication systems.

Originally proposed by Goodfellow et al. [7], Generative Adversarial Networks are based on the competition between two neural network models a generator and a discriminator [7]. The generator aims to create fake but realistic data, while the discriminator learns to distinguish generated samples from real ones. During the training process, both networks improve: the generator becomes increasingly skilled at mimicking real features, and the discriminator becomes better at identifying them. This dynamic makes the GAN architecture particularly powerful in tasks where the high realism of generated content is essential.

In the context of biometrics, GANs enable the creation of synthetic biometric features that effectively mask real data. These features can be used to substitute original patterns in templates, thereby enhancing the system's resistance to spoofing, reconstruction attacks, and statistical analysis. Importantly, the original biometric vectors are not used directly, which reduces the risk of their compromise. Mixing generated and real templates significantly increases data entropy, expanding the number of possible combinations and making it more difficult for an attacker to access the original information [8]. It is important to emphasize that the use of GANs in biometric systems supports the principles of differential privacy. Synthetic data can be used for training and testing without the risk of exposing real user templates, which is especially relevant when handling personal data under strict information protection regulations (such as GDPR).

Modern cryptographic algorithms play a key role in ensuring cybersecurity, particularly in the context of integration with artificial intelligence technologies and biometric systems. One of the promising solutions is the use of the El-Gamal cryptosystem, which offers strong resistance to cryptographic attacks.

Table 2.
Comparative analysis of cryptosystems.

Cryptosystem	Encryption Type	Processing Speed	Key Size (bits)	Applicability to Biometrics	Authentication Support
El-Gamal	Asymmetric	~10,000 ops/sec (with 1024-bit key on FPGA)	1024–4096	High	Yes
RSA	Symmetric	~3,000 ops/sec (at 1024 bits)	1024–4096	High	Yes
AES	Asymmetric	~50,000–100,000 ops/sec	128, 192, 256	High	No
ECC	Asymmetric	~10,000 ops/sec (with 256-bit key)	160–521	High	No

When selecting a cryptosystem for securing biometric data, it is essential to strike a balance between processing speed and the level of security. The El-Gamal cryptosystem offers strong resistance to attacks due to the complexity of the discrete logarithm problem and provides stochastic encryption, which makes it less vulnerable to ciphertext analysis. Unlike RSA, El-Gamal is better suited for biometric data processing because it avoids deterministic encryption, thereby reducing the risk of template compromise. Compared to AES, El-Gamal offers more secure data transmission without requiring prior key exchange, which is particularly important in distributed biometric systems. While ECC is a strong alternative due to its smaller key sizes and efficiency, its implementation involves more complex mathematical operations and careful configuration. Ultimately, El-Gamal emerges as the optimal choice for biometric systems, offering a combination of reliability, flexibility, and high-level security.

The integration of the El-Gamal cryptosystem with AI and biometric technologies opens new opportunities for advancing cybersecurity. Adaptive key generation based on user behavior analysis enhances resistance to attacks, while asymmetric encryption reduces the risk of biometric data compromise. Interactive biometric authentication, reinforced by machine learning algorithms, improves recognition accuracy, and personalized protection mechanisms make cybersecurity more resilient to hacking and biometric template forgery.

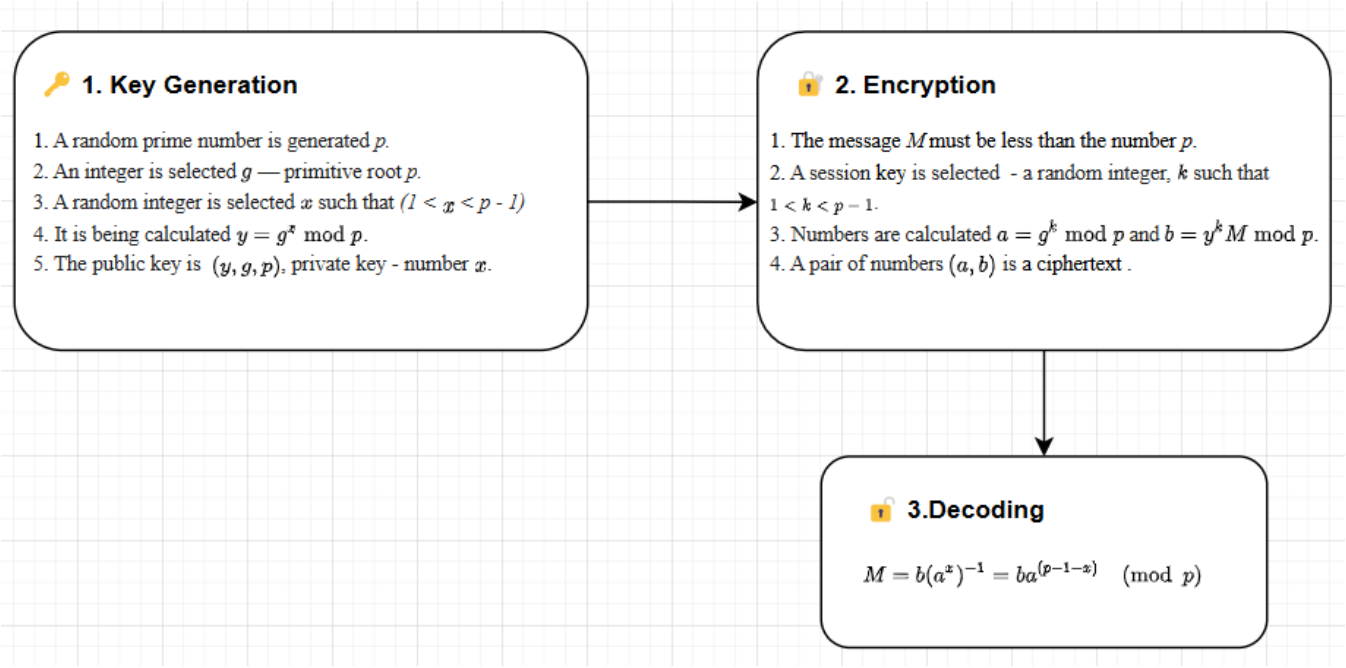

Figure 2.
Flowchart of the El-Gamal cryptosystem.

The mathematical foundation of the algorithm lies in modular arithmetic, finite field theory, and the computational hardness of the discrete logarithm problem, which ensures its cryptographic strength. One of the key advantages of the method is its adaptability it is used for both encryption and digital signatures, enabling the verification of message authenticity.

Overall, the fusion of deep learning techniques with cryptographic protocols enables the creation of an intelligent and secure biometric infrastructure. By embedding CNNs, GANs, and the El-Gamal algorithm into a cohesive workflow, the system not only achieves high recognition accuracy and tamper resistance but also meets the modern requirements of privacy, scalability, and deployment flexibility.

3.3. Participants (Datasets)

The system was evaluated using three publicly available biometric datasets. The facial image dataset used in this study is the CelebA dataset [9], which contains over 202,599 face images of 10,177 individuals. For this experiment, a subset of 10,000 aligned facial images in .jpg format with a resolution of 178 × 218 pixels was selected. The images depict faces in various poses and lighting conditions.

The fingerprint dataset was obtained from the Fingerprint Feature Extraction for Biometrics project [10]. This dataset includes over 5,000 fingerprint images stored in .bmp format with a resolution of 640 × 480 pixels. The fingerprints were collected from multiple individuals using inkless scanners and represent various finger positions.

The retina dataset used in this work is the UBIRIS v2 dataset [11] developed for iris recognition in the visible wavelength spectrum. It consists of 11,000 images collected from 261 subjects, with each image stored in .jpg format at a resolution of 400 × 300 pixels. A total of 10,000 retina images were randomly selected for training and testing purposes.

In total, the combined dataset for this study included over 30,000 images. Experiments were conducted by randomly sampling and balancing the number of images across all three biometric modalities.

3.4. Data Collection Tool and Environment

All experiments were conducted in the Google Colab cloud environment with access to a T4 GPU accelerator, 12.7 GB RAM, and 15 GB GPU memory. The implementation was carried out using Python 3. The machine learning models were built using TensorFlow and Keras libraries, while the cryptographic operations, including encryption and digital signature generation, were implemented using the PyCryptodome library. The CNN model required approximately 25 minutes to train over 10 epochs. GAN training was executed for 10,000 epochs and took around 3–4 hours. The feature extraction, encryption, and signing for a single sample were completed in 1–2 seconds on average.

4. Results and Discussion

The developed biometric protection system was experimentally evaluated using three biometric modalities: facial images, fingerprints, and retinal scans. A convolutional neural network was trained to extract features from these modalities with a classification task. The system demonstrated high performance across all metrics.

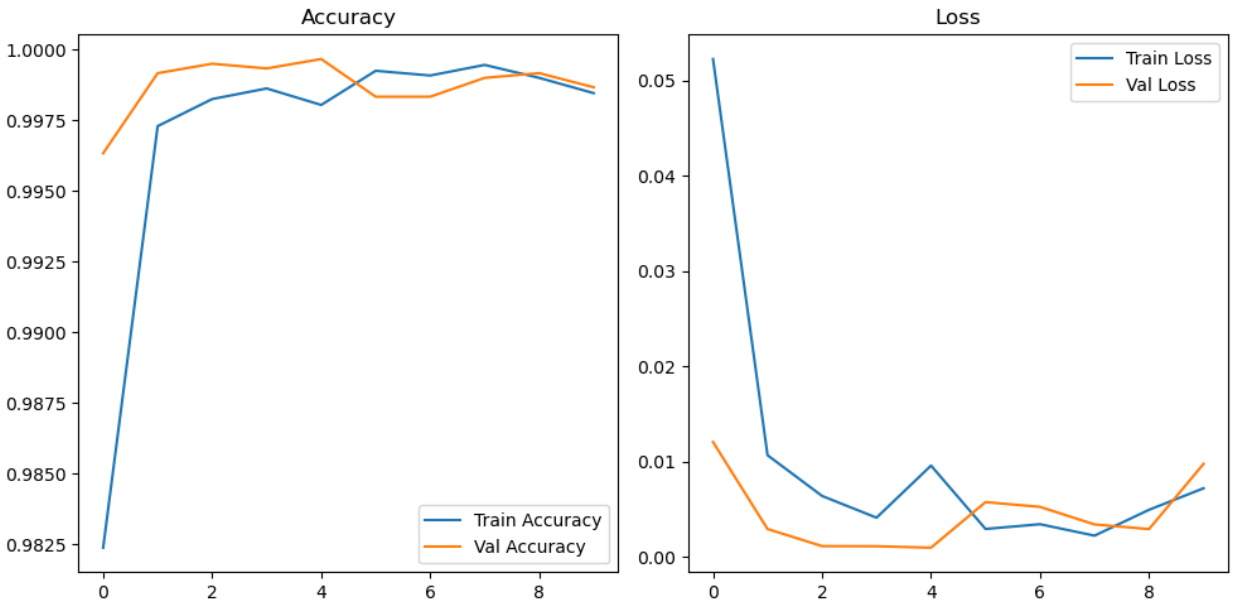

Figure 3.
Accuracy graph.

The CNN model was trained on a classification task involving three types of biometric data. As shown in Figure 3, both training and validation accuracy stabilized above 99.8%, and the loss values quickly dropped to near zero, indicating strong generalization ability and the absence of overfitting. Feature extraction from the images was performed following this training phase.

After feature extraction using the CNN, a generative GAN model was trained with the goal of producing synthetic biometric features that are indistinguishable from real ones. Figure 4 illustrates the training dynamics: the discriminator loss stabilized around 0.3–0.4, while the generator loss gradually increased, reaching approximately 3.8–4.0. Despite this trend, the overall behavior of the graph indicates stable training and a maintained balance between the two models. This confirms the GAN's ability to generate features that are both visually and statistically similar to real biometric data.

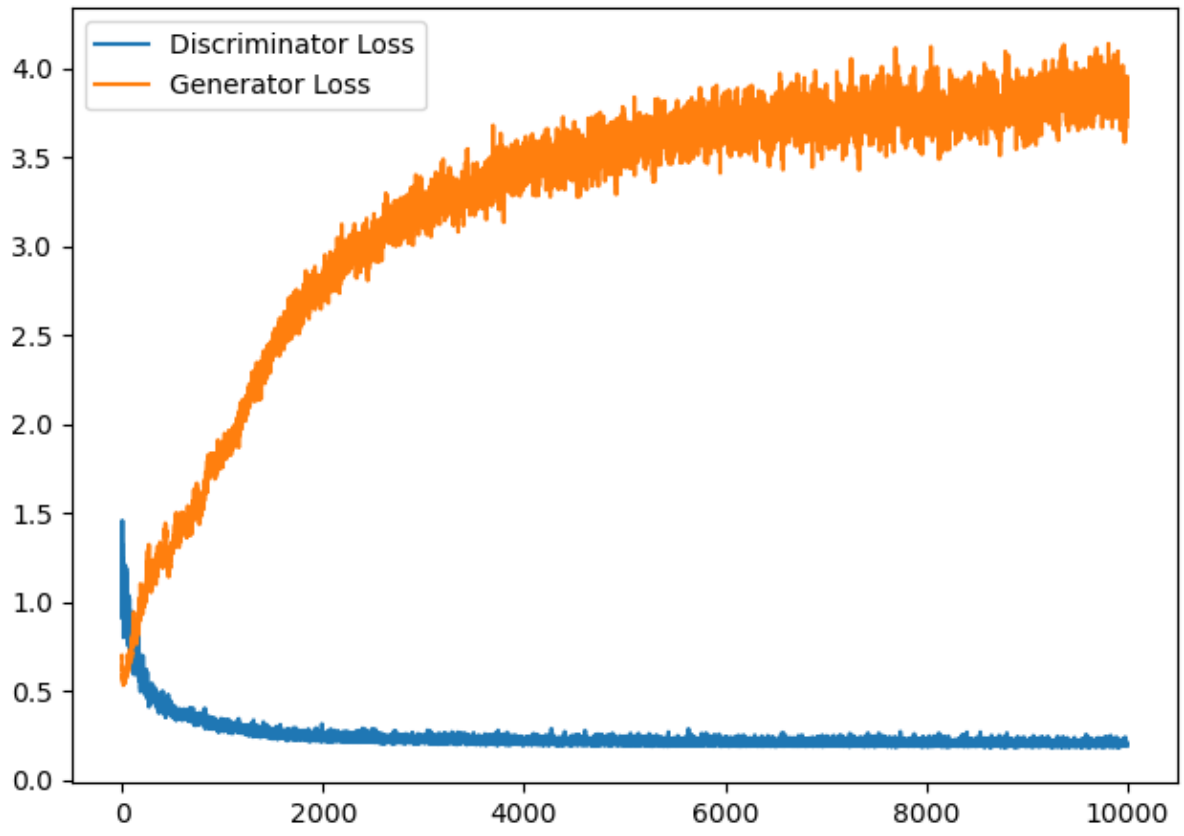

Figure 4.
Loss graph.

The extracted features, both real and synthetic, were encrypted using the El-Gamal algorithm. Additionally, a digital signature was implemented for both the features and the original image using the SHA-256 hash function and the El-Gamal signature scheme. The signature was successfully verified after decryption, confirming the integrity of the data and protection against tampering. The encrypted images, represented as pairs of cryptographic values (C1, C2), were successfully decrypted back to their original byte form without any loss.

Table 3.
The ciphertexts of samples.

Sample	The Ciphertext (C1, C2)
Sample 1	(43913385880269218305279416972400016719995797731907304577811538602468016893994, 133928630464639178340682362508983782399763126423198164863952766885422264461)
Sample 2	(36328161771483275643132981723815703051562231195934373019816669373959407767969, 40477123482026655009995344375658634167837802503915247029077778443111149076148)
Sample 3	(44321936845062758417287382556897344152523124108226826624021287858898695400 17, 30594323019350497196226755777166778581367649689232127554083183356036237215462)
Sample 4	(39864501557730204975096492291395935940803364401041073153979213395747462750445, 40198671800447248401338377660986652700810709119308686270261151002712815961921)
Sample 5	(53098083833962430821143450394195018670457781060256320617516633156577097210604, 29679220955056127635308343640346155997014095552352488631922211439437406227041)

To ensure authenticity, a digital signature was applied to the biometric feature vector (both real and synthetic). The signature was generated using the SHA-256 hash function, followed by the application of the El-Gamal signature scheme to the resulting hash. This approach allowed for the verification of the integrity of the features during the decryption stage and ensured their authenticity.

Table 4.
The digital signature (r,s) of samples.

Sample	The Signature(r,s)
Sample 1	(63330132051287985805491638319882431812819032913051547016015823554388031203480, 34310556382046763369574307717606687657221663981030644898596426912989357847 83)
Sample 2	(55438515603661439257123246618396182557333034320797772931300760832698916820455, 32176628104017793033226340925548849026140520623441327784145710914978729833752)
Sample 3	(80693739419683587189591592722457565018006749881253136045282376862945116166066, 81922902084405002065151931649207593163979036938187039678426259429958644562985)
Sample 4	(93364111402355574783398392093613088122259425783937529849443812084402882619 16, 36849168424852431208908544425753678684637192375211329791067667780109445372617)
Sample 5	(16342761094656517408184669235762109290893208943319548826835160769170480833806, 13088458374301449470619028532471996239763775821638867628578156763172422546774)

The training time for the CNN model was approximately 25 minutes for 10 epochs. Training the GAN model took around 3–4 hours for 10,000 epochs, with the loss function monitored every 1,000 epochs. The processes of feature extraction, encryption, and digital signature generation for a single image were performed in an average of 1–2 seconds.

Compared to previous studies, the proposed system offers several advantages. While Zahoor [1] focused primarily on improving authentication accuracy using AI, they did not address secure transmission or template protection. Panigrahy et al. [2] proposed ANN-based encryption but lacked asymmetric encryption or digital signing mechanisms. Works like Kumari [3] and Qin and Zhang [4] applied El-Gamal to image encryption, but did not utilize synthetic data or end-to-end biometric integration. This study fills those gaps by combining deep learning, data synthesis, and cryptographic protection in a unified and tested framework.

The dual protection offered by both encryption and digital signature mechanisms significantly increases system robustness. The use of synthetic features further enhances privacy by removing the need to store original biometric templates. Importantly, this architecture provides security not only during storage but also during data transmission and identity verification stages, making it highly suitable for deployment in high-assurance systems such as border control, healthcare, and national ID infrastructures.

Thus, the system provides a dual layer of protection: on one hand, through encryption, and on the other, through the ability to verify the authenticity and integrity of the data.

The integration of artificial intelligence and cryptographic methods into a unified secure pipeline proved to be effective: features were extracted, masked, encrypted, and digitally signed in an automated manner. This approach ensures not only a high level of security but also scalability for deployment in real-world biometric systems.

It should be noted that the digital signature significantly enhances the system's reliability, especially in scenarios involving potential substitution of biometric data. However, the use of El-Gamal for both encryption and signing requires substantial computational resources. While this may be critical for real-time systems, such overhead is justified in cloud computing environments. The results obtained demonstrate the practical applicability and high resilience of the proposed method in biometric identification and data protection tasks.

5. Conclusion

Machine learning methods play a crucial role in the protection of biometric data. The use of neural networks (CNN, GAN) enhances identification accuracy, prevents attacks, and enables the secure encryption of biometric information. The integration of artificial intelligence with cryptography, including the El-Gamal cryptosystem and differential privacy, opens up new opportunities in the field of cybersecurity. Further development of this system may focus on incorporating additional biometric characteristics, such as voice or behavioral parameters, as well as adapting it to mobile and distributed computing environments. Moreover, testing the model on larger and more diverse datasets would provide a better assessment of its applicability in real-world scenarios. Thus, the results of this work demonstrate the potential of the developed architecture for use in modern cybersecurity and biometric authentication systems.

5.1. Implications

The proposed approach contributes both technically and practically to the field of cybersecurity and biometric authentication. On a technical level, the study demonstrates that deep learning models can be effectively combined with asymmetric cryptographic systems to protect sensitive biometric information. The use of GANs provides privacy-preserving data synthesis, which reduces the risk of biometric template compromise. On a practical level, the system shows potential for real-world deployment in high-security environments, including border control systems, digital identity management, and secure healthcare authentication frameworks.

5.2. Limitations

While the proposed system achieves promising results, several limitations remain. First, the computational complexity of the El-Gamal encryption and digital signature operations may present challenges for deployment in resource-constrained environments such as mobile devices or embedded systems. Second, the system was evaluated on publicly available datasets that may not fully reflect the variability or quality issues of real-world biometric data in uncontrolled conditions. Third, the focus was limited to image-based biometric modalities, excluding behavioral or multimodal combinations.

5.3. Future Research

Future work will aim to optimize the cryptographic layer for low-power environments through the use of elliptic curve cryptography or lightweight encryption variants. Another direction involves the integration of additional biometric modalities such as voice, gait, or keystroke dynamics to enhance flexibility and accuracy. The system could also benefit from adversarial robustness testing to defend against spoofing attacks specifically targeting deep learning models. Moreover, deployment on edge computing platforms with limited resources would further validate its real-world applicability. Expanding the evaluation to include diverse populations and cross-cultural datasets would provide broader insights into the model's generalizability.

References

[1] E. A. M. S. Zahoor, "Biometric encryption: Integrating artificial intelligence for robust authentication," *Dandao Xuebao/Journal of Ballistics*, vol. 35, no. 3, pp. 25–33, 2023. https://doi.org/10.52783/dxjb.v35.121

[2] A. K. Panigrahy *et al.*, "A faster and robust artificial neural network based image encryption technique with improved SSIM," *IEEE Access*, vol. 12, pp. 10818-10833, 2024. https://doi.org/10.1109/access.2024.3353294

[3] T. M. Kumari, "Image encryption using MVK algorithm, El-Gamal and chaotic systems," *International Journal of Scientific Research in Engineering and Management*, vol. 6, no. 6, pp. 45–51, 2022. https://doi.org/10.55041/ijsrem16112

[4] Y. Qin and B. Zhang, "Privacy-preserving biometrics image encryption and digital signature technique using Arnold and ElGamal," *Applied Sciences*, vol. 13, no. 14, p. 8117, 2023. https://doi.org/10.3390/app13148117

[5] U. Gumanti, A. Pardede, and H. Khair, "Superencryption of BASE 64 algorithm and ELGAMAL algorithm on Android based image security," *Journal of Artificial Intelligence and Engineering Applications*, vol. 2, no. 3, pp. 129-134, 2023. https://doi.org/10.59934/jaiea.v2i3.211

[6] D. Bhatt *et al.*, "CNN variants for computer vision: History, architecture, application, challenges and future scope," *Electronics*, vol. 10, no. 20, p. 2470, 2021. https://doi.org/10.3390/electronics10202470

[7] I. J. Goodfellow *et al., Generative adversarial nets. In Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, & K. Q. Weinberger (Eds.), Advances in Neural Information Processing Systems*. NY, USA: Curran Associates, Inc, 2014.

[8] S. Karthika and M. Durgadevi, "Generative Adversarial Network (GAN): A general review on different variants of GAN and applications," presented at the 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021.

[9] Z. Liu, P. Luo, X. Wang, and X. Tang, "Deep learning face attributes in the wild," in *Proceedings of the IEEE International Conference on Computer Vision*, 2015, pp. 3730-3738.

[10] H. Proença and L. A. Alexandre, "UBIRIS: A noisy iris image database," presented at the International Conference on Image Analysis and Processing, 2005.

[11] S. D. Roy, *Fingerprint feature extraction for biometrics [Code notebook]* Mountain View, CA, USA: Kaggle, 2021.