applied sciences

MDPI

Article

Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal

Ying Qin [1] and Bob Zhang [1,2,*]

[1] PAMI Research Group, Department of Computer and Information Science, University of Macau, Taipa, Macau SAR, China; mc25659@um.edu.mo
[2] Centre for Artificial Intelligence and Robotics, Institute of Collaborative Innovation, University of Macau, Taipa, Macau SAR, China
* Correspondence: bobzhang@um.edu.mo; Tel.: +853-8822-4425

Abstract: The scientific study of privacy-preserving biometrics, represented by the palmprint, face, and iris, has grown tremendously. That being said, there has not been much attention paid to the proper preservation, transmission, and authentication of biometric images used in everyday applications. In this paper, we propose a new complete model for encrypting and decrypting biometric images, including their signing and authentication, using a nested algorithm of 3D Arnold Transform. In addition, the ElGamal Encryption Algorithm for the encryption part and the ElGamal Digital Signature for the signature part are applied. The model is mainly based on the Arnold Transform and Public-Key Cryptosystem, which are convenient for key transfer and fully functional. Here, the model succeeds in encrypting and securing the authentication process for privacy-preserving biometric images. Various tests have been carried out to demonstrate the feasibility and security of the proposed model and have been compared with existing encryption methods to achieve better results. Moreover, the proposed model can also be extended to the storage, transmission, and authentication of biometric data for daily use.

Keywords: privacy-preserving biometrics; cryptography; Arnold transform; ElGamal algorithm; digital signature

Citation: Qin, Y.; Zhang, B. Privacy-Preserving Biometrics Image Encryption and Digital Signature Technique Using Arnold and ElGamal. *Appl. Sci.* **2023**, *13*, 8117. https://doi.org/10.3390/app13148117

Academic Editor: Mostafa Fouda

Received: 12 June 2023
Revised: 11 July 2023
Accepted: 11 July 2023
Published: 12 July 2023

1. Introduction

The status and role of information in society are becoming increasingly important and have become a vital strategic resource for social development. Information technology is changing the way people live and work; the information industry has become a new economic growth point, and the informatization of society has become a trend and a core development around the world today. With the rapid development of multimedia and information technologies, our lives are becoming more and more convenient. At the same time, the security of information has become a social issue of concern around the world. In recent years, network security and cryptography technologies have also been developing rapidly. Advanced science and technology have been developed in various fields, and machine learning has been very successful in the field of biometrics research [1], of which face, palmprint, and iris images (data) are vital parts. The biometric images are extremely private, and if stolen or tampered with by unscrupulous individuals, the privacy and security of the people being attacked would be at great risk, with unthinkable consequences. This is why it is extremely important to ensure the security of biometric data. For image data with general security, only pixel replacement or simple image encryption methods are required, without necessarily using cryptographic theory as the basis for encryption, and verification of integrity is not necessary for every type of data. However, research into how to securely transmit, store, and verify these private images used in applications is only just beginning. We hope to resolve these issues by proposing a complete scheme for encrypting, decrypting, and securely authenticating privacy biometric images.

Currently, there are a number of well-established encryption schemes for image encryption; for example, Guan et al. [2] proposed a Chaos-based encryption algorithm; Wang et al. [3] proposed a fast image encryption algorithm based on parallel computing systems; Liu et al. [4] used optical technology for image encryption; and Li et al. [5] proposed an image encryption algorithm based on Autoblocking and Electrocardiography. However, biometric data, due to its privacy and uniqueness, is compatible with the high security and integrity assurance features of cryptographic algorithms. The need for separate encryption of biometric data during transmission is more in line with the irreversible and random nature of cryptographic algorithms. In recent years, the rapid development of quantum cryptography has given us a new direction, and many advances have been made in the study of quantum cryptography, such as those made by Gu et al. [6] and Bennett et al. [7], which greatly enhanced the security of encryption algorithms and better protected the original data. For example, Yin et al. [8] proposed a model for a complete set of digital signatures and encryption algorithms based on quantum cryptography, opening a new path for many researchers. However, quantum cryptography has more complex hardware requirements, making it difficult to implement. That being said, traditional cryptography is still the mainstream encryption method. Therefore, not all of these schemes are suitable for the storage and transmission of privacy-preserving biometric images, with specific encryption schemes required to securely store this private data. With this in mind, the paper attempts to propose an encryption, decryption, and verification scheme that can solve these problems.

Based on the current research in the security of biometric images, especially face, palmprint, and iris, the paper proposes a novel method for encryption, decryption, and authentication in order to achieve better privacy-preserving biometric images. Firstly, the storage and transmission of the face, palmprint, and iris images require the use of an efficient and convenient cryptographic algorithm that needs to be complex and unbreakable, as well as solve specific issues such as the size of the key space and the suitability of the key for storage and transmission. The generation, distribution, and storage of keys are collectively known as key management. Using a single encryption algorithm for encryption is not secure enough and requires nesting of the algorithms to increase the complexity of the model, thus increasing safety. Here, the more common image encryption algorithms are nested with Public-Key Cryptosystems. Spatial domain encryption [9] is a common method and is divided into spatial domain scrambling and sequence encryption, where Arnold Transform [10] is a widely used image scrambling algorithm. The proposed method performs pixel sequence scrambling of the RGB components of a color image using the Arnold Transform. Next, applying the ElGamal Encryption Algorithm [11] to continue the secondary encryption, a Public Key Cryptographic algorithm based on discrete logarithms is obtained. The Public Key Cryptographic algorithm solves two of the most difficult problems in Single-Key Cryptosystems: the key's distribution and digital signatures. Therefore, the Public-Key Cryptographic algorithm ElGamal is chosen for this work, which is superior in the key distribution and signature authentication parts. Another reason for choosing the ElGamal Encryption Algorithm is that it is based on discrete logarithms. The security of discrete logarithm cryptographic algorithms follows mathematical puzzles, such as the discrete logarithm problem [12] and the elliptic curve discrete logarithm problem [13], that are difficult to break even if the nature of the algorithm is known. Here, the ElGamal algorithm based on the discrete logarithm algorithm is also a very good digital signature authentication algorithm, providing strong support for the purpose of the proposed model dedicated to building a complete authentication process in the storage and transmission of biometric images. Digital signatures include authentication, data integrity, non-repudiation, and anonymity. The proposed model uses the ElGamal algorithm to digitally sign the original biometric image before encrypting it and verifying it after decryption to ensure that its identity and content have not been tampered with.

The main novelty and contribution of this paper are

1. Innovated the common 2D Arnold Transform into its 3D Arnold Transform, allowing various parameters to be used before being nested with the encryption from the ElGamal Encryption Algorithm for enhanced algorithmic security.
2. Proposed a complete encryption, decryption, and authentication process that satisfies both encryption and authentication as the two main security requirements for the application of biometric data preservation.

The rest of the paper is described as follows: Section 2 presents the background. Section 3 elaborates on the methodology and mathematical analysis. Section 4 introduces the process of the experiments. Section 5 introduces and discusses the results. Finally, Section 6 concludes this paper.

2. Background

Image transmission has become commonplace in today's fast-moving technological age, and it is imperative that important images are stored and transmitted securely [14]. The growing study into privacy-preserving biometrics has given rise to many inquiries into the security of storing and transmitting biometric data, such as face, palmprint, and iris images. How to transmit images without damage and at the same time ensure that they are not tampered with or stolen is turning out to be a complex subject worth investigating.

How to securely store and authenticate biometric images requires a great deal of cryptographic knowledge. Cryptographic systems can be divided into two main categories [15] in principle, which are Single-Key Systems and Dual-Key systems. The Dual-Key System was first introduced by Whitfield Diffie and Martin E. Hellman in New Directions in Cryptography [16] in 1976. With the Dual-Key System, each user has a chosen pair of keys, one that can be made public and the other that is secret. The Dual-Key System is therefore also known as a Public-Key Cryptosystem. Public-Key Cryptosystems can be used in public networks to enable secure communications and authenticate users. The cryptographic algorithms used in the proposed model belong to the Public-Key Cryptosystem because the environment and characteristics of the Public-Key Cryptosystem are consistent with the requirements of the application. The Public-Key Cryptosystem has the property that it is computationally infeasible to find the decryption key when the cryptographic algorithm and encryption key are known, which means that the sender and receiver do not need to share a secret key. The public key can be distributed freely, while the private key remains secret.

Existing studies for privacy with biometric images mainly use image encryption algorithms, where image encryption mainly consists of the Arnold transform. Arnold Transform (also known as Arnold's Cat Map) is an image encryption algorithm based on the classical cryptographic system that essentially performs multiple matrix operations on the positions of pixels in an image of equal length and width pixel points, thus changing the position of the pixels in space in order to uniformly distribute the energy of the image [17]. The Arnold Transform is the most commonly used technique for mixing digital images [18]. Chen et al. [19] proposed a new approach to color image encryption based on Arnold Transform (ART) and interference methods. Chen et al. [14] extended the 2D Arnold Transform to a 3D Arnold Transform and a real-time secure symmetric encryption scheme. And Ye et al. [20] proposed an image encryption algorithm based on an improved Arnold transform and a chaotic pulse-coupled neural network. While all of these methods make good use of the Arnold Transform, using the Arnold Transform alone has significant security threats, is vulnerable to brute force enumeration cracking, and has some vulnerabilities. Another approach to encrypting privacy-preserving biometric images is to encrypt them using cryptographic algorithms alone. Choudhury et al. [21] used the AES encryption algorithms to encrypt the biometric images and then convert them to QR Codes. The AES encryption algorithm was a popular symmetric encryption algorithm that used the same key for both encryption and decryption. Compared with AES encryption algorithms, the ElGamal Encryption Algorithm is based on the discrete logarithm problem and uses large primes as moduli, so it is very difficult to crack, and the ElGamal Encryption Algorithm is

a Public-Key Cryptosystem with easier key management. After comparison, among the cryptographic algorithms, the ElGamal Encryption Algorithm is more compatible with the use of image encryption. Nouioua et al. [22], Laiphrakpam et al. [23], and Hashim et al. [24] all proposed modifications to the ElGamal Encryption Algorithms and gave us some new ideas. However, the use of a single cryptographic algorithm to guarantee security creates the problem of an excessive volume of keys, which makes the transmission of keys and ciphertexts difficult, and there are shortcomings in this type of approach.

More cryptographic studies use image encryption algorithms and cryptographic algorithms nested together for encryption, which greatly improve algorithmic security. Soni et al. [18] presented a hybrid technique of image encryption using the Arnold Transform and RSA algorithms. Lone et al. [25] proposed RGB encryption based on symmetric keys while mixing Arnold Transform. From these papers, we came up with the idea that the ElGamal Encryption Algorithm has some advantages over the RSA Encryption Algorithm. Thomas et al. [26] proposed a more secure image encryption framework for sending image information over untrusted channels. Chen et al. [27] proposed a scheme based on an improved elliptic curve cryptosystem and Arnold Transform that was suitable for large image encryption and provided high security while avoiding key exchange and distribution. Luo et al. [28] proposed a novel asymmetric image encryption method that was based on the elliptic curve ElGamal Encryption Algorithm and chaos theory. Parida et al. [29] and Parida et al. [30] upgraded their algorithms based on elliptic curve encryption in combination with other image encryption techniques with good results. In this paper, we propose a new privacy-preserving biometric image encryption method based on these studies by combining an improved 3D Arnold Transform with the ElGamal Encryption Algorithm, which both simplifies the encryption and decryption algorithms and improves the security of the whole algorithm.

Digital signatures are well established nowadays. Jonathan Katz explained the many basic methods of constructing a secure signature scheme in his book *Digital Signatures* [31]. Digital signatures have evolved from public key ciphers and have important applications in network security, including authentication, data integrity, non-repudiation, and anonymity. To ensure that encrypted images are not tampered with or corrupted during transmission, I used digital signature algorithms to sign and verify the encrypted images, ensuring data integrity and non-repudiation. Merkle [32] described a new digital signature based solely on traditional cryptographic functions such as DES, whose security did not depend on the difficulty of decomposition and avoided the high computational cost of modular operations. Schneider et al. [33] proposed a digital signature algorithm for verifying images that allowed some types of image modification (e.g., lossy compression) but prevented other types of manipulation (e.g., tampering) and extended signature-based authentication for images to the authentication of video sequences. Alam et al. [34], Nikolaidis et al. [35], Pan et al. [36], and Chang et al. [37] all proposed innovative digital signature schemes that were modified for traditional signature algorithms. Since the traditional ElGamal Digital Signature algorithm used only one random number and therefore had certain security flaws, in order to improve the security of the algorithm, Li et al. [38] proposed an improved ElGamal Digital Signature Scheme that was based on the hard-to-compute property of discrete logarithms over a finite field. In summary, the ElGamal Digital Signature Scheme has strong superiority in digital signatures. However, since digital signature algorithms are often accompanied by cryptographic algorithms, we need to consider the complexity, completeness, and fit of the whole process in addition to the integrity of the authentication. Although the above literature proposes very clever signature methods, they lack a degree of integration with the authentication of cryptographic algorithms. Therefore, the same ElGamal Digital Signature algorithm as the encryption algorithm is used in this method to sign privacy biometric images, which simplifies the complexity of the algorithm as a whole and solves the problem to a certain extent.

After analyzing the various types of encryption and signature algorithms mentioned above, we found that these algorithms can have some minor drawbacks, such as too

much computation, a small key space, inconvenient storage and transportation, and overly complex algorithms. Based on these problems, and after analyzing and summarizing the existing research, this paper proposes a complete encryption and authentication method using the Arnold Transform and ElGamal Encryption Algorithm for encryption and the ElGamal Digital Signature for authentication. The proposed method is improved by upgrading the Arnold transform from 2D to 3D while combining techniques such as the ElGamal encryption algorithm, which cleverly solves the problem of key space and improves the difficulty of the algorithm, making the whole method more complete and better at sustaining the security of privacy-preserving biometric images. This combination solves the problem of tampering during transmission in common encryption scenarios and solves problems in scenarios where privacy protection is a challenge. For example, in laboratories that use privacy-preserving biometric images for research, the experimental data needs to be protected by encryption to prevent leakage when a single encryption alone could easily be cracked and stolen, and the experiment also needs the authenticity and integrity of the data, which requires a digital signature to be added to the encryption process for verification.

3. Proposed Method and Mathematical Analysis

3.1. Overall Framework

The framwork is divided into two main parts: the digital signature part and the encryption/decryption part. The digital signature part uses the ElGamal Digital Signature algorithm, and the encryption/decryption parts mainly apply the Arnold Translation and ElGamal Algorithm. Refer to Figure 1 for the specific process.

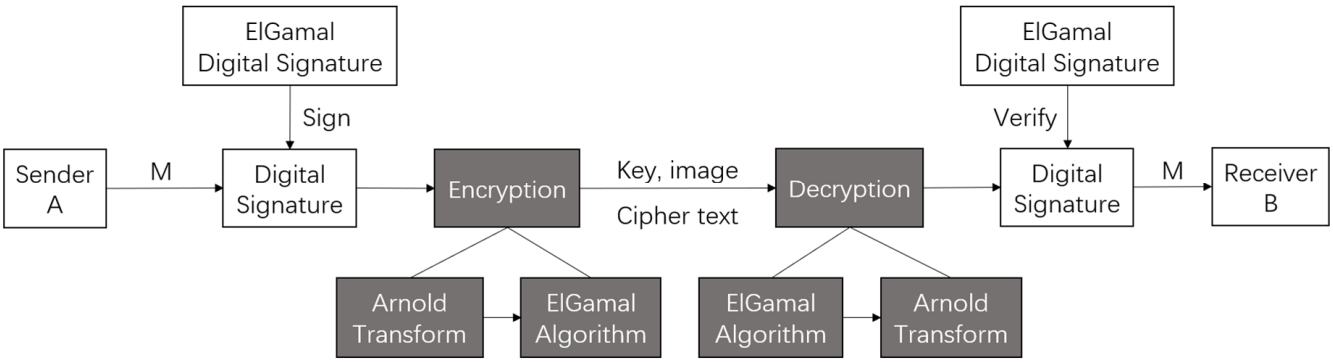

Figure 1. The framework of the proposed method.

Digital signatures are the most effective solution to the growing problem of image tampering. The ElGamal Digital Signature, which is based on the discrete logarithm problem, is a solution to the challenge of image tampering. Arnold Transform uses a 3D transform that scrambles the original image, resulting in better encryption. The Arnold Transform alone has the disadvantage that the key space is too small and vulnerable to exhaustive attacks, while the ElGamal Public-Key encryption, with the same encryption key, repeatedly encrypts different results and provides better security. The combination is a complete cryptographic verification algorithm that is lightweight and easy to use but guarantees the security and authenticity of the biometric data. The digital signature part is mainly used to verify that the biometric data has not been tampered with during transmission to ensure data integrity, and the encryption/decryption part is mainly used to encrypt the image to ensure the security of the image and prevent others from stealing it. The two parts have different divisions of labor and different roles, but both are ensuring that the security of the data is not threatened, and since the biometric data are singular in nature, it is important to ensure that the data have not been stolen. Because of the singular nature of privacy biometric data, it is important to ensure that the data are not tampered with. In order to make the implementation of the algorithm more convenient,

the cryptographic algorithm and the digital signature in this paper are both based on the ElGamal algorithm, which has good randomness and resistance to cracking.

3.2. ElGamal Digital Signature

Digital signature systems based on the discrete logarithm problem are the most common type of digital signature system. The ElGamal Encryption Algorithm can be used to create digital signatures, which provide authentication and non-repudiation of the data. This is achieved by using the private key to sign the data, and the public key to verify the signature. Therefore, the proposed model employs the ElGamal Digital Signature for digital signatures. Following Figure 1, Sender A sends the original message M, first using a digital signature to sign it.

The specific steps for signing are as follows (refer to Figure 2): M is plaintext, E is the encrypted message (as the signed file), D is the decrypted message, SK_A is the private key of Sender A, and PK_A is the public key of Sender A.

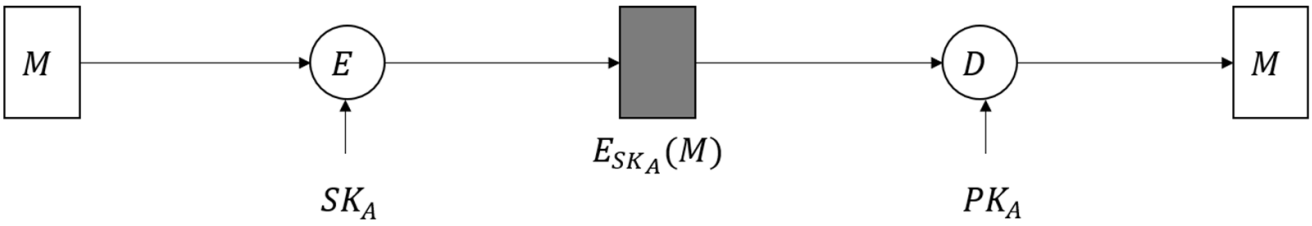

Figure 2. The process of digital signature.

Here, we set a large prime number p, Z_p^*'s generating element g, Sender A's private key $x \leftarrow_R Z_p^*$, and Sender A's public key $y \equiv g^x \ (mod\ p)$.

For the message M to be signed, Sender A performs the following steps:

- Calculate the hash value H(M) of M;
- Select random number k: $k \leftarrow RZ_{p-1}^*$, then calculate $r \equiv g^k \ (mod\ p)$;
- Calculate $s \equiv (H(M) - xr)k^{-1}(mod\ p-1)$;
- Use (r, s) as the resulting digital signature.

Finally, the signature verification process is carried out, where the receiver, upon receiving the message M and the digital signature (r, s), calculates H(M) and verifies it according to Equation (1):

$$Ver(y,(r,s),H(M)) = True \leftrightarrow y^r r^s \equiv g^{H(M)}(mod\ p) \quad (1)$$

Correctness can be proved according to Equation (2):

$$y^r r^s \equiv g^{rx} g^{ks} \equiv g^{rx+H(M)-rx} \equiv g^{H(M)}(mod\ p) \quad (2)$$

Compared to other digital signature algorithms, ElGamal Digital Signature offers a high level of security because it uses asymmetric key cryptography. The private key used for signing is kept secret, while the public key used for verification is available to everyone. ElGamal Digital Signature ensures non-repudiation, which means that the signatory cannot deny having signed the document or message. This feature is crucial in legal and commercial transactions where a signature is required to prove authenticity and intent. In practice, ElGamal Digital Signature can be used to sign any type of document, information, or data. It is not limited to a specific file format or application. Moreover, ElGamal Digital Signature is computationally efficient, can be implemented on a variety of platforms, including mobile and IoT devices, and can be used to sign multiple documents simultaneously. It is also suitable for large-scale applications that require frequent signing and verification. Furthermore, ElGamal Digital Signature is based on a standard encryption algorithm, making it easy to integrate with other systems and applications. It ensures compatibility and interoperability with other digital signature solutions. As a result, ElGamal

Digital Signature makes it easier to authenticate signatures where multiple documents and data are required for privacy-preserving biometric data.

3.3. Encryption and Decryption Methodology

3.3.1. Arnold Transform

There are various methods for encrypting existing images; the Arnold Transform is used in this paper. The traditional Arnold Transform uses 2D transformation, but the 2D transformation of Arnold is easier to crack due to the transformation period and transformation step, and the encryption effect of the 2D transformation is not as secure as the 3D encryption effect. Hence, this paper uses 3D Arnold encryption, where the original image cannot be cracked by brute-force methods alone.

As this paper upgrades the 2D Arnold transformation into a 3D Arnold transformation, the coefficient matrices A and B are also transformed into third-order matrices, and the transform coefficients are increased from two coefficients in the 2D Arnold transformation to six coefficients, both of which are innovations that increase the complexity of the algorithm as well as the security of the final result. The transformation coefficients are also randomly generated by random numbers from (1, 1,000,000,000), and new random numbers are generated for each operation, both of which greatly enhance the security of the algorithm. Following Figure 1, after the Digital Signature operation, the Arnold Transform is used to perform encryption. The first steps of encryption are as follows:

The generalized 3D Arnold Transform is Equation (3):

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = A \begin{pmatrix} x \\ y \\ z \end{pmatrix} mod\ N \tag{3}$$

with the 3D Arnold Transform being Equation (4):

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = B \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} mod\ N \tag{4}$$

Matrix B is the inverse matrix of matrix A in Equation (5).

$$\begin{aligned} A &= \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \\ a_{11} &= 1 + \mathrm{ace} \\ a_{12} &= \mathrm{c} \\ a_{13} &= \mathrm{c} + \mathrm{ac} + \mathrm{abce} \\ a_{21} &= \mathrm{f} + \mathrm{ae} + \mathrm{acef} \\ a_{22} &= \mathrm{cf} + 1 \\ a_{23} &= \mathrm{bf} + \mathrm{abcef} + \mathrm{acf} + \mathrm{abe} + \mathrm{a} \\ a_{31} &= \mathrm{ade} + \mathrm{e} \\ a_{32} &= \mathrm{d} \\ a_{33} &= \mathrm{abde} + \mathrm{ad} + \mathrm{be} + 1 \end{aligned} \tag{5}$$

After the above equations, it is clear that the transformation coefficients a, b, c, d, e, and f in the Arnold Transform are important for encryption and decryption, and that obtaining the above data will lead to a complete conclusion. Therefore, it is extremely important to encrypt the above data.

The encryption process used in 3D Arnold-encrypted images ensures that the image cannot be easily hacked or manipulated, making it ideal for use in applications where security is a top priority.

3.3.2. ElGamal Encryption Algorithm

As Arnold is cyclic and the key space is too small and vulnerable to perform exhaustive attacks, it is not possible to use Arnold alone. Therefore, the ElGamal algorithm is relied upon to expand the key space of Arnold and improve the overall security of the algorithm.

This paper uses traditional cryptographic methods with Arnold superimposed on the encryption method used to enhance the security of the algorithm by employing the discrete logarithm-based ElGamal Encryption Algorithm on top of Arnold encryption for secondary encryption and better preserving the privacy of biometric images. Following Figure 1, Encryption and Decryption sections, we use the ElGamal Encryption Algorithm to encrypt the result of the Arnold Transform.

The ElGamal algorithm is a Public-Key Cryptosystem based on the discrete logarithm problem over a finite field, proposed by ElGamal [11] in 1985. It is a secure encryption method that ensures the confidentiality and integrity of the data. Based on the difficulty of computing discrete logarithms, the method is resistant to brute-force attacks. Public-Key Cryptosystems have certain advantages over Private-Key Cryptosystems (e.g., DES, AES, etc.) in that they can separate encryption from decryption, such that messages encrypted by multiple users can only be interpreted by one user, or messages encrypted by one user can be interpreted by multiple users. The Public-Key Cryptosystem is therefore suitable not only for encryption but also for signature authentication. This model contains a signature authentication component that makes it more appropriate to choose a Public Key cryptographic algorithm. Figure 3 is a block diagram of the public key system encryption applied in this paper.

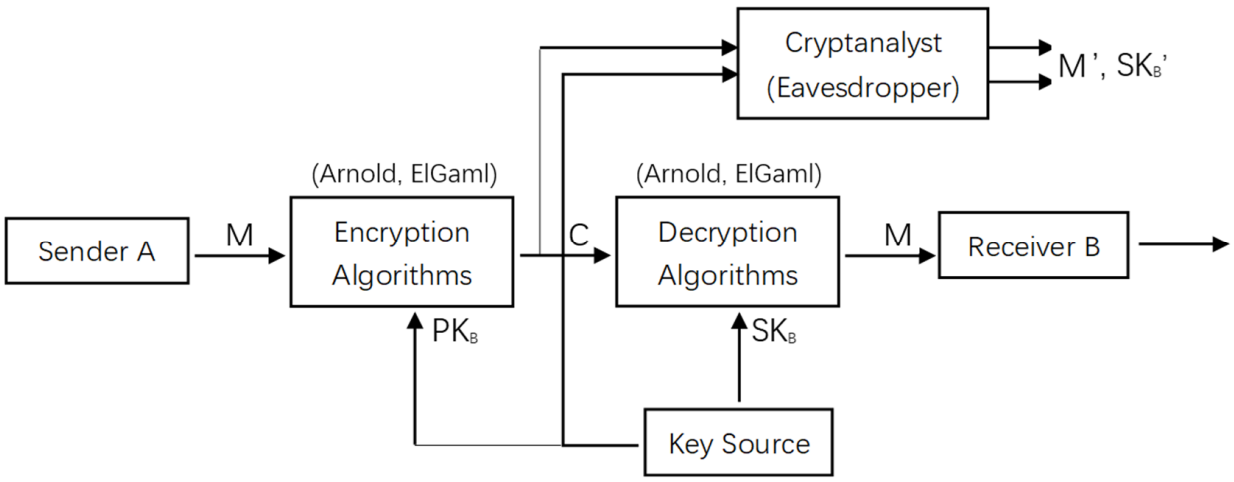

Figure 3. A block diagram of the public key encryption system.

The ElGamal Encryption Algorithm has a unique key generation process; it first chooses a prime number p and two random numbers g and x that are less than p. Next, compute Equation (6). Use (y, g, p) as the public key and x as the secret key.

$$y \equiv g^x mod\ p \tag{6}$$

The encryption process is as follows: Suppose you want to encrypt a plaintext message, M. Randomly select an integer k that is prime to $p - 1$, then calculate Equations (7) and (8).

$$C_1 \equiv g^k mod\ p \tag{7}$$

$$C_2 \equiv\ y^k M\ mod\ p \tag{8}$$

Finally, the ciphertext is Equation (9).

$$C = (C_1, C_2) \tag{9}$$

The decryption process follows Equation (10).

$$M = \frac{C_2}{C_1^x} \ mod \ p \tag{10}$$

The reason for the calculation of Equation (10) is Equation (11).

$$\frac{C_2}{C_1^x} mod \ p = \frac{y^k M}{g^{kx}} mod \ p = \frac{y^k M}{y^k} mod \ p = M \ mod \ p \tag{11}$$

After Equation (10), we employed the Arnold Transform to conduct the final decryption, ultimately using the Digital Signature to verify that the ciphertext had not been tampered with. At the end of all processes, M is sent to Receiver B (refer to Figure 1).

The ElGamal Encryption Algorithm is scalable, which means that it can be used to encrypt large amounts of data efficiently. This is achieved by breaking the data into smaller blocks and encrypting each block separately. At the same time, this algorithm has the advantages of high computational complexity and low space consumption compared with the now more common public key encryption algorithm, RSA. Its security is also higher; it is known to attack discrete logarithmic problems over finite fields using an exponential integration method with an operational complexity of $O\left(exp\sqrt[3]{(\log p)(\log\log p)^2}\right)$.

4. Experiments

4.1. Experimental Settings

The experiments follow the sequence in Figure 4 and are presented in this paper in the same order. Firstly, the image to be encrypted is signed using the ElGamal Digital Signature algorithm. Then, the 3D Arnold transform is performed. Next, the key parameters of Arnold are encrypted using the ElGamal Encryption Algorithm. After that, the encrypted image is sent to the recipient with the public key, who first decrypts the cipher text using the key to obtain the Arnold parameters. Afterwards, it decrypts the image using the parameters and finally uses the ElGamal Digital Signature algorithm to verify that the image has not been tampered with and that it has been restored to the original image after decryption. As shown below, M is plaintext, E is the signed file, D is ciphertext, SK_A is the private key of Sender A, PK_A is the public key of Sender A, SK_B is the private key of Receiver B, and PK_B is the public key of Receiver B.

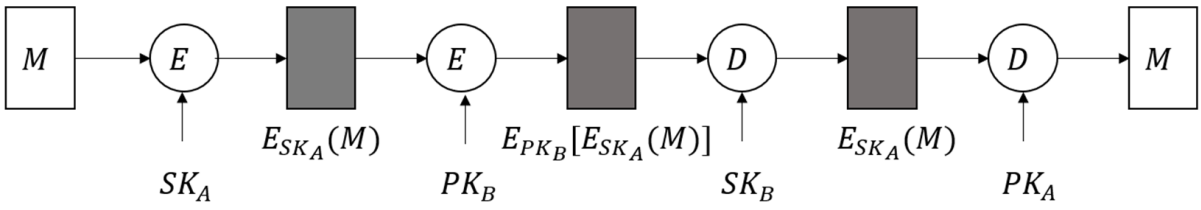

Figure 4. Public key encryption with confidentiality, authentication, and signature.

The proposed algorithm is implemented using Python 3.10.9 by PyCharm 2022.2.3 on the Windows 11 platform using a personal computer with an 11th Gen IntelI CITM) i7-1195G7 @ 2.90GHz and 2.92 GHz Processor. To verify the performance of the proposed framework, we tested it on three distinct modalities coming from three biometric datasets. The face dataset is the FEI (Fundação Educacional Inaciana) dataset [39]. There are 2800 images in this database with 200 subjects, and the images are colored on a homogeneous white background. The face images are in JPG (*.jpg) format, where the size of each face image is 640 * 480 pixels. The palmprint dataset is the IIT Delhi Palmprint Image Database version 1.0 [40]. The database consists of hand images collected from students and staff at IIT Delhi, New Delhi, India. The database was collected from 230 users, with all images in bitmap (*.bmp) format. The resolution of these images is 800 * 600 pixels, and all

of these images are available in bitmap format. The dataset contains 5202 images. The iris dataset is from IIT Delhi Iris Database version1.0 [41]. This dataset mainly consists of the iris images collected from students and staff at IIT Delhi, New Delhi, India. The available database is from 224 users, and all the images are in bitmap (*.bmp) format. The resolution of these Images is 320 * 240 pixels and contains a total of 1120 images. The experiments selected three images randomly from each database. Figure 5 illustrates the original images regarding the biometric data, where samples 1 to 3 are face images, samples 4 to 6 are palmprint images, and samples 7 to 9 are iris images.

Figure 5. Samples of privacy-preserving biometric images that require encryption.

4.2. ElGamal Digital Signature

The original image was first digitally signed by ElGamal Digital Signature; the details are in Table 1. Afterwards, we use Equation (1) to verify the result.

Table 1. The digital signature (r, s) of all samples.

Sample	The Signature (r, s)
Sample 1	(49403562386972889101239812641985822426261568600929413555373108317189108566302658182904229360129949456643308318348548341680203213984974337427422125011695385415969039985638625877946204652788472222754991791639135468475613905777408393254427228818611627255606179146594809249070764944574244956620299141804364454722)
Sample 2	(61001817069789903834733532799590115645066963165036129235083962521897558133265020005042140403856630849184326379561282504819727116569265888384423692910714293920960075631645675970373440968561770676670833763982104027959626991710723503367478791351675817794334667622453078601762339675549694439881156063780318669776)
Sample 3	(83345755023986145287656082248492284463108343079487467735995468215457225650193052730976368350996863409887911575670888607696826327925873579603568157370839551167338802073835158865358549159392555393478170961318628418068994264777594463208938798278839018278166115807923305101675122919996603656200981411845363721 8)
Sample 4	(32770927389331039688022294832445079946003767854742672100976183865179359893047631045241429231475954642673069715296770005380574566960147385390808713462551194, 74317841604665719134560759843286184428988155806608214817669013907179593430212196539625919272193398853848414694097456916233879272922057870323358866643491 63)
Sample 5	(27578652117404991113459163718274825738043277214393148198437662989945229197277066959839502656689013352925824270332348847587097539131050747438050569635859 44, 11325892940740625846349859317307101277883682299089533597056761274924849722036969802956260725697913915194604413511598154787331314714254326095217505710546 37)
Sample 6	(25612173890034996243941155180559197217428638497892432771341656992282011218157428679217979948781260441056992561024889531461698026902559077836620456859113 67, 28375376951879664169089787776744000323863020354495906428186190609525483905059095110396867295480342781658853003582661888319226582295181322129033221329586 47)

Table 1. *Cont.*

Sample	The Signature (r, s)
Sample 7	(54398059576020356857809512618182773599266889824472811267197302864439883175735568642809635255126258348952404924563360871206003565085116468061611918335 5935, 97192750256352128958901024589517901285331945133285248198455237780863066041292735747789319851070286166165811340614511276992401434144326178597706286478888216)
Sample 8	(74102162293030303970936099354904815578385715161969636375804832367015488193883707488965175531722438958331774798202211838942891361716537555008908384185697716, 74862843438716775414638330451199173523483193135260105790801731406859385662888607709776854167213771791970289773875680679936542750641773166886782557114497931)
Sample 9	(32940431999256486348204174476156929124306796643813422836590281167205827332040071527066830246774119672373781267518407561894394518615043159865533681372165 70, 12302137110044656761454391455554356582140667670281753276186673574482105601357613580084190848041515471053319273443253598555793298725175232698358884875541871)

In this process, the signature part is completed, such that this model has a complete authentication, encryption, and decryption process, which is the innovation point of this method.

4.3. Three-dimensional Arnold Transform

The Three-dimensional Arnold Transform is generated via six random numbers (a, b, c, d, e, and f); the specific values for this experiment are listed in Table 2.

Table 2. The parameters of all samples.

Sample	a	B	c	d	e	f
Sample 1	232709439	837958984	5622636709	4889491484	8039179046	8010888566
Sample 2	3332339114	8193641194	3507863116	7924306438	3043082504	8368036383
Sample 3	3202028823	8223356666	8257665806	501329413	497167895	2290551472
Sample 4	1086004930	2458801845	5646181635	4975192797	340014358	785196447
Sample 5	8596903353	3002961029	2021559227	8480832950	3805056567	872322169
Sample 6	589635510	6546165257	3669836237	1031634060	3199039412	5240423885
Sample 7	6740553346	4264195198	161858830	8426007426	1228860491	7087122474
Sample 8	4874003878	3523561682	8052441761	1659046523	3575780783	5109015130
Sample 9	8587831492	393289385	6711451445	2308213150	3577919509	2997423679

Three-dimensional Arnold Transform requires more parameters than two-dimensional Arnold Transform, with periodicity becoming longer, the algorithm becoming more complex, and the encryption being better, which is the advantage of this model.

4.4. ElGamal Encryption and Decryption Algorithm

Next, we used the ElGamal Encryption Algorithm to encrypt the parameters generated in the previous round. The ElGamal Encryption Algorithm has the powerful complexity of discrete computation, making the encryption better and more secure. The public keys are shown in Table 3, and (y, g, p) are calculated by Equation (6).

Table 3. The public key (y, g, p) of all samples.

Sample	The Public Key (y, g, p)
Sample 1	(11847580859627495311720948186104291409177210971433079758835646919242306765 52387430340910681716747612875280525932025613289379060029084639060863093632 7, 11177500151106740177420968835730057510316860424001269569960900361339163135 55774823235631141201792723845767061078204139546725045299055772232684033399 64, 35879479980118957922029633235292776224761472463916452871285889241123343008 85028629717106856204572895091605959486856314348591710221556965097526867379 63)
Sample 2	(16160233489855003456619323487804265696418296748153197092530240368568579576 49176903807263744351325404034159148773668356614842609344255276370192557821 56, 89114762904046931878729571591620945031262154887991301701808844299380561440 72885727270496779662465822554090863117707647181433919005458023318354084400, 38360276179642616923622848794377677993182699651081280201714575800937627647 55428163918402449311345464569404557859879382498043247640641008155818987541 39)
Sample 3	(18250146995062933991396693782979016579984834913597982319006938664901586678 78623895516303416910983819143472487135014445895730282001338079288941519447 80, 15395752785000911259183024492239877895963607279873991856252809745215686964 13352869668459642830190247588336772950116664255016915904896218590237463018 48, 27070600335449959908734153835001799833731689497603999844148273366110505582 88149325979289986168539662096813935803518866387525098707452722227097236028 79)
Sample 4	(47159147661340683752317331693419390055288774913617050809781286801228545160 09466790067740264522635953206686160300840590599688506945710222573100183805 54, 13434772304548847912271626947812354522091991276251614952151665514341468271 03597316653921821965665831342311667295842865083926092815755518367569227892 11, 57638301822541954348220582548451170180538436477063387105698122199450290143 11082864964510154122961228005312105566183158381263639579053441332551267478 87)
Sample 5	(51422361997094442131060300849385490270087762052468605224099276467776339984 85777567498008027698393168686582430936625773093192282570784383300585710231 7, 16344232400749958811031258870678853817327323421664383410651518147434101129 02003505338826637034793383528621941514266251259192589944301095878836124300 23, 44708184732844965581725424922218599260938270392426007695657843061042099075 90932400900289642532385358963633200088460757522073863790880057761346290268 07)
Sample 6	(58667733412023491090337484732002181026870280324486453814644033403654645839 39433507922860303935098188210070447993754027274363812000624060733299661512 27, 16427279722883807601936941119228286634637300537367794951814343401349166261 71457839549106155519776681567978364780267223909625233684748443132042468471 21, 75141849372359559643076798415906103257172694522005243630503374696094889065 93791677021962360518631819922283929995759541455187496917133063467910106177 83)
Sample 7	(49137282503637218628449719444888476123937226172741857584751990940384492922 88341524733747954472445419525832257761708088034239948602230105026298957917 3, 41407815746111675539128298086233018507310188562842083851115516315259112261 20350082588039926850363016101012261041516239942872018835657052354029909921 75, 87375347137831941259747433146765448237163948233924648255021625874119970620 55375886945885893825690208761263900417372458974713451559623270789299657058 67)
Sample 8	(22588446872991414603569287613896269398203125068394045993668834996721166763 68961848294903956637380203048331210738011113212810700240671431739213457264 20, 35506920737271601330785925670305336551180251066380736606277323756681869322 79936213168965273686081256938219304488246764498564916312222758639648047732 30, 56048123077437606721025902816735961995213858363689662120791635845764961053 49811903139526643715162276601721347594806485882041790456784754776988762192 87)
Sample 9	(74210179158883859917607103927058113580295739908631561724785961300549552647 59152553773401360182712100604772234235651909720180425356972359577010973228 4, 34472993974858008989717557966969274522354815690426212808699659687256041130 59194110144906552836656677705234951760256717053446804663741562270044342796 02, 35648129035532251113206969215709223721296674232939371518791252365566482635 64904739815665738983718925401742321401228209111580275582112507570290466185 99)

The ciphertexts are in Table 4, and (C1, C2) are calculated by Equations (7)–(9).

Table 4. The ciphertexts of all samples.

Sample	The Ciphertext (C1, C2)
Sample 1	(291929961547886893926403132104433477760478326053179011873397473708990354494 563413358252500405205189069429895468677759444048706154681226801677094583537, 463809309473788947874032969367302718760344456768292995858334763948046725164 373629174238247088564395263964348112615717176403897958097716468463949799 89)
Sample 2	(332786795704650261032764608278330298122894667055059907021371952075074585057 938821582408083402658494445202878125826999278652742614834842485161153613069, 134198389609432517353819200362500558183127521388116295149512434215553472406 181131542370437537813465659547686350582711809225599462738371954078555022074)
Sample 3	(170642680154235657957340844918765346119457423654962269525415987693823948562 317080824818096878027809533760204829933170648646219943566855270137752005880, 258102357561081418320628083633885425759877781154685032482850017783154575609 461841196875776694776500569953662684030652663310080591492866100569814396174)
Sample 4	(690295461815019074885279200368917978633041123050606236101149131487318579915 293440326000169827977286444901293694449474587837680966170826843128911520 22, 367731812477155060847315787691169200678706699411330086879063503682719315279 233116399296390656124693911156157903661034989925910121130261482159644037 07)
Sample 5	(109471869882438297208400018361196059243557623965971637299193531631742417186 330252691405175324234697871050774841172423437409477732881473436167737641604, 746456687895922323594634922758765774720078336004411600606433290589489515892 627260086164444104563956693256824801262535876922575877312971524817883245 38)
Sample 6	(742141920951522047640232536149164915953866289019728211501311732816006793266 930640383197371071450695074024589782520821544333767702196473361174708424293, 365215727665735652701052871626790010930034419282526341420694749104038410635 378645571767185870493564414016937206361629844889895223327446247008922266 23)
Sample 7	(832122037875872145862608500211229138979542155051329730350016091376647234784 921058822807843722398432351891927695953540800848844479051491930805003002988, 326663441888663885342624179203002352601479714363700347517211743357080501040 565166846106958140742085741283829069360505540627458397760120623202158460077)
Sample 8	(853992243519074644232775358670533483263986519700846988080671917978384282502 906333144860816183987264097220971697828042314569385829496054116509916493 3, 468755558937945162492838668398490588217831578121991222976401679832876707259 138343506929504289978818830328787423352436082760636561814808138736288616590)
Sample 9	(116740776631631619200288268127897330968003414103482271784134881772893388330 853736428512994673326006194589819845583998612325674579004119794118790965943, 346322268112453346222779420604577758061568801950743871956704045841535364498 8272471673872421773322104069312362739144393849743980751650460555179870087 00)

5. Results and Discussion

5.1. Results

The ElGamal decryption result is shown in Table 5.

The process of images with Arnold Transform and ElGamal encryption and decryption is shown in Figure 6.

After decrypting the images, we applied the public key of the ElGamal Digital Signature to verify the integrity and non-repudiation of the image by identifying that it had not been tampered with or corrupted during transmission. Finally, the decrypted image was verified using some functions from OpenCV [42] to compare whether it was exactly the same as the image before encryption. Here, we can report that the result was the same, meaning the signature is valid.

Table 5. The result of the ElGamal Decryption Algorithm.

Sample	a	b	c	D	e	f
Sample 1	232709439	837958984	5622636709	4889491484	8039179046	8010888566
Sample 2	3332339114	8193641194	3507863116	7924306438	3043082504	8368036383
Sample 3	3202028823	8223356666	8257665806	501329413	497167895	2290551472
Sample 4	1086004930	2458801845	5646181635	4975192797	340014358	785196447
Sample 5	8596903353	3002961029	2021559227	8480832950	3805056567	872322169
Sample 6	589635510	6546165257	3669836237	1031634060	3199039412	5240423885
Sample 7	6740553346	4264195198	161858830	8426007426	1228860491	7087122474
Sample 8	4874003878	3523561682	8052441761	1659046523	3575780783	5109015130
Sample 9	8587831492	393289385	6711451445	2308213150	3577919509	2997423679

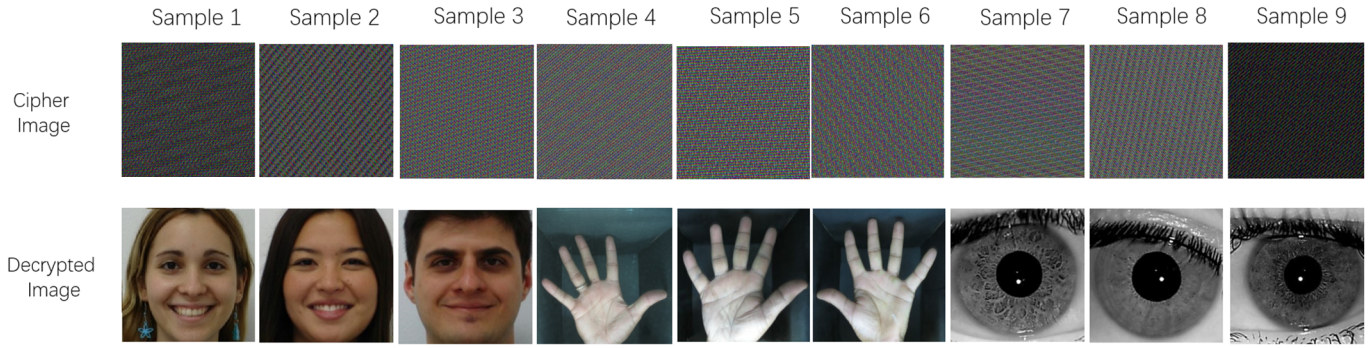

Figure 6. Privacy-preserving biometric images with digital signatures for encryption and decryption.

5.2. Resistance against Existing Attacks

A practical image encryption method should be able to resist existing attacks such as statistical attacks, cropping attacks, known-plaintext attacks, potential attacks, differential attacks, and so on. In this subsection, the paper focused on four test attacks that were more typical and popular than others, with the analytical results presented for security analysis. Here, one image from each dataset was randomly selected for experimental analysis and compared with some recently popular security algorithms, including methods such as Ye et al. [20], Choudhury et al. [21], Lone et al. [25], Parida et al. [29], Parida et al. [30], and Erkan et al. [43]. A comparison between the algorithms being compared and the model algorithm proposed in this paper is shown in Table 6. From this table, it can be observed that only the proposed method uses a digital signature scheme, while others do not. In addition to this, other security analysis methods have been chosen to analyze the proposed model.

Table 6. Comparison between the algorithms being compared and the model algorithm proposed in this paper.

Difference	Proposed Model	[20]	[21]	[25]	[29]	[30]	[43]
Digital Signature	ElGaml Digital Signature	NULL	NULL	NULL	NULL	NULL	NULL
Encryption Method	Three-dimensional Arnold Transform and ElGaml Encryption	Arnold Transform and chaotic pulse-coupled neural network	AES and QRCode	Arnold Transform, 3D logistic chaotic map with XOR operation, and affine hill cipher technique	Elliptic Curve Diffie-Hellman (ECDH)	Henon map, Hopfield chaotic neural network and ElGamal Algorithm	Chaotic log-map, deep convolution neural network (CNN) model, and bit reversion operation for the manipulation process

5.2.1. Randomness Test

The Grayscale Difference (GVD) is a statistical measure of randomness comparing the original image with the encrypted image and can be defined by the following Equation (12):

$$GN(x,y) = \frac{\sum[G(x,y) - G(x',y')]^2}{4}, (x',y') = \begin{cases} (x-1,y) \\ (x+1,y) \\ (x,y+1) \\ (x,y-1) \end{cases} \quad (12)$$

G(x,y) symbolizes the gray score at position(x,y) [44]. The average neighborhood Gray difference of the whole image can be calculated by the following Equations (13) and (14).

$$GVD = \frac{AN'[GN(x,y)] - AN[GN(x,y)]}{AN'[GN(x,y)] + AN[GN(x,y)]} \quad (13)$$

$$AN[GN(x,y)] = \frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1} GN(x,y)}{(M-2)(N-2)} \quad (14)$$

AN and AN′ represent images with the same mean neighborhood gray; however, the former is represented before encryption and later used for post-encryption representation. The final result of the above equation is called the GVD score, which is 0 if the two images are identical and 1 otherwise. The following table (refer to Table 7) shows the GVD scores of the three examples encrypted against the original image. The GVD score for each channel is close to 1, which indicates that the original and encrypted versions are quite different. Furthermore, we compared the randomness test scores via Ye et al. [20], Choudhury et al. [21], Lone et al. [25], Parida et al. [29], Parida et al. [30], and Erkan et al. [43].

Table 7. GVD scores compared with [20,21,25,29,30,43].

Sample	Red	Green	Blue
Sample 3	**0.9853**	**0.986**	**0.9858**
[20] Sample 3	0.9614	0.9683	0.9599
[21] Sample 3	0.8201	0.8015	0.8291
[25] Sample 3	0.9798	0.9802	0.9766
[29] Sample 3	0.9561	0.9731	0.9683
[30] Sample 3	0.9526	0.9423	0.9753
[43] Sample 3	0.8963	0.8964	0.8963
Sample 4	**0.9815**	**0.9861**	**0.9878**
[20] Sample 4	0.9512	0.9491	0.95
[21] Sample 4	0.8712	0.8601	0.8788
[25] Sample 4	0.9211	0.9036	0.9071
[29] Sample 4	0.8779	0.8453	0.8805
[30] Sample 4	0.9457	0.9715	0.9702
[43] Sample 4	0.8637	0.8691	0.8677
Sample 8		**0.9837**	
[20] Sample 8		0.9509	
[21] Sample 8		0.9787	
[25] Sample 8		0.9523	
[29] Sample 8		0.8838	
[30] Sample 8		0.8538	
[43] Sample 8		0.8497	

From Table 7, it can be concluded that the three experimental examples (from the three biometric modalities) generated using the proposed method have the highest GVD scores (bold), which are close to 1. Sample 8 is a grayscale image and does not have a result for the red and blue channels. Compared with recent and popular image encryption algorithms that are based on similar mathematical foundations as the proposed model

(Ye et al. [20], Choudhury et al. [21], Lone et al. [25], Parida et al. [29], Parida et al. [30], and Erkan et al. [43]), all of our scores are higher and obtain a better preservation result.

5.2.2. Robustness against Noise

When communicating over the Internet, parts of an image may be cropped or even lost, so the proposed ciphertext must be able to handle the encryption of a lossy image in an appropriate way. We call it a cropping attack. In the experiments, a portion of the ciphertext image (e.g., the area representing 1%, 5%, and 10% of the total area) is set to pixel values of 0 and then decrypted with the correct key. In image processing, the quality of the reconstructed image can be judged by analyzing the peak signal-to-noise ratio (PSNR) between the ciphertext image and the plaintext image. The peak signal-to-noise ratio (PSNR) [45] looks at the error between the corresponding pixel points. Given an encrypted image X of size M × N and an original image Y, the Mean Square Error (MSE) is defined as follows in Equation (15):

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (X(i,j) - Y(i,j))^2 \quad (15)$$

The peak signal-to-noise ratio (PSNR) can be calculated using the following Equation (16) [23], and Max is the maximum supported pixel value.

$$PSNR = 20 \times log_{10} \frac{Max}{\sqrt{MSE}} \quad (16)$$

where M and N denote the width and height of the image, respectively, and n is the number of pixel bits; a smaller PSNR value represents larger distortion, and the larger the difference between the two images, the better the encryption effect.

From Table 8, we can conclude that the PSNR scores (bold) of the three biometric data are relatively small. Since PSNR is judged on the basis that the larger the PSNR value, the smaller the difference between the two images, the less effective the encryption algorithm. The greater the difference between the original and encrypted images would require a lower PSNR value, representing a better result. Sample 4 has the lowest mean score, the best result, and better encryption quality. When comparing the PSNR data with Ye et al. [20], Choudhury et al. [21], Lone et al. [25], Parida et al. [29], Parida et al. [30], and Erkan et al. [43], all their scores are higher, so our method has a better preservation result.

Table 8. PSNR scores compared with [20,21,25,29,30,43].

Sample	Red	Green	Blue
Sample 3	**9.922517915621553**	**10.584477208324234**	**10.022887303777159**
[20] Sample 3	10.672468476727392	10.983477273647372	10.687648737235655
[21] Sample 3	13.897384092871782	12.938284782936152	12.892837656273718
[25] Sample 3	11.925317254374218	11.782653471625539	10.98346762368122
[29] Sample 3	13.029837646152451	12.652413263262534	11.923167352367181
[30] Sample 3	10.989362534126732	12.763562837928375	10.612453628823641
[43] Sample 3	12.299868378599205	12.299842955330815	12.299868378599205
Sample 4	**6.235614983911999**	**7.39169508965318**	**7.840108667138846**
[20] Sample 4	9.9478993478753784	10.912787376283764	10.176437692387467
[21] Sample 4	11.256354856650981	11.23354354561097	11.326573768720991
[25] Sample 4	10.8257569258420361	11.998795886752346	11.265523458688736
[29] Sample 4	14.00123355411	13.243956091238112	11.998153426462193
[30] Sample 4	10.9418273991324012	9.210472648652581	10.902437719984356
[43] Sample 4	10.987180491083743	10.987586953706003	10.987180491083743
Sample 8		**7.857589179486729**	
[20] Sample 8		10.584746726354853	
[21] Sample 8		12.170754930500951	
[25] Sample 8		11.908392041332121	
[29] Sample 8		12.19436838811037	
[30] Sample 8		11.996559203172371	
[43] Sample 8		10.955354934003573	

5.2.3. Noise Attack

Image encryption algorithms must be robust enough to resist noise attacks in real-world scenarios. Experiments are first performed by adding varying levels of Gaussian or Anti-Salt and Pepper noise to the ciphertext image, then decrypting the noisy encrypted image and comparing the decryption results. Noise immunity is an important metric for testing the performance of an encryption scheme. Gaussian noise with a mean of zero and a variance of 0.0005 as well as 5% check noise were added to the encrypted samples 1 to 9, respectively. Following this, they were decrypted with the following results: Figure 7 is the Gaussian noise attack result, and Figure 8 is the Anti-Salt and Pepper noise attack result.

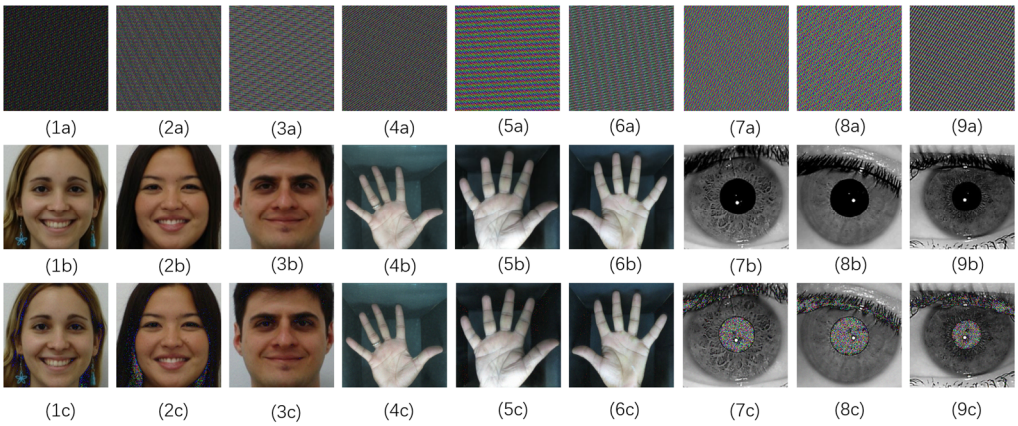

Figure 7. The ciphertext image with Gaussian noise. (**1a**–**9a**) are the encrypted images with Gaussian noise; (**1b**–**9b**) are the plain-text images; (**1c**–**9c**) are the decrypted images.

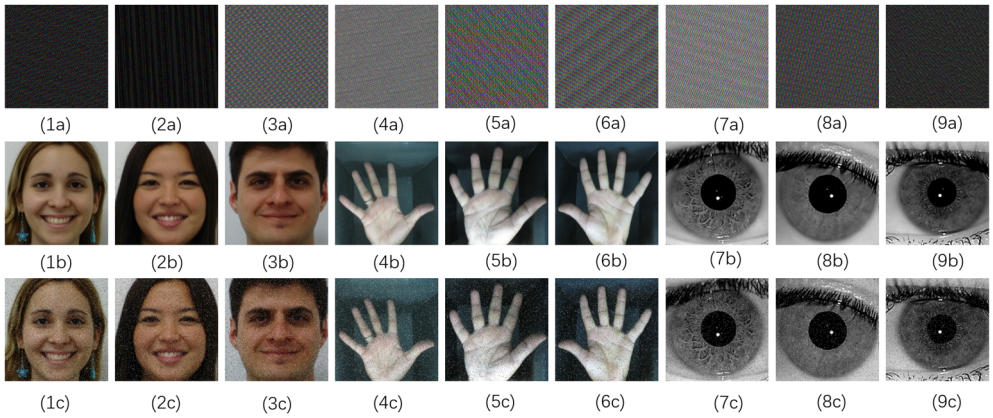

Figure 8. The ciphertext image with Anti-Salt and Pepper noise. (**1a**–**9a**) are the encrypted images with Anti-Salt and Pepper noise; (**1b**–**9b**) are the plain-text images; (**1c**–**9c**) are the decrypted images.

5.2.4. Potential Attack

Potential attacks can be divided into pure ciphertext attacks, known as plaintext attacks, and selected plaintext attacks. A pure ciphertext attack is an attack to decrypt ciphertext when only the ciphertext itself is available and the attacker tries to recover the corresponding plaintext or encryption key. It is known that a plaintext attack is an attacker's attempt to recover the key in possession of the ciphertext and related plaintext fragments. A selected plaintext attack is when the attacker uses the selected plaintext attack to destroy the encryption algorithm.

Because the ElGamal algorithm used in the proposed model is random, the key and ciphertext of the same original file are different each time, and the characteristics of a discrete logarithm make it impossible for attackers to attack it reversely. That is, they cannot get the key even if they have all the plaintext. Therefore, neither a pure ciphertext attack nor a known plaintext attack or a selected plaintext attack can be cracked. The digital

signature selected by the model using the same ElGamal cryptographic algorithm can resist these types of attacks.

5.3. Discussion

Although the experimental design is complete and the results are satisfactory, there are a few shortcomings in this model, and some other areas need to be optimized, such as the model's vulnerability to brute force cracking. That being said, the model increases the range of random numbers, leading to higher cracking costs, and the sheer volume of work involved in encrypting and signing each image for authentication can further mitigate these attacks. However, with the development of quantum cryptography, traditional cryptographic applications are also threatened to some extent. We will continue to improve the proposed model by placing quantum cryptography as a major research direction in future studies.

The model proposed In this paper can be used to encrypt all 2D privacy-preserving biometric data directly without any modification. However, the model proposed in this paper is not applicable to 1D data, such as voice. Having said that, with the development of technology, more and more applications will not choose voice as the carrier for private information transmission and will usually select more secure 2D data for privacy-preserving biometrics. Moreover, voice is easy to compress and lose during transmission, and the data obtained by the receiver may be different from the original voice even if it is not attacked.

6. Conclusions

In this paper, a new image encryption-digital signature method is proposed for privacy-preserving biometric images. The original biometric image is first encrypted using the 3D Arnold Transform, with the ElGamal Encryption Algorithm performing a secondary encryption of the Arnold's parameters, after which the encrypted image and ciphertext are sent to the receiver, and the original biometric image is signed and authenticated using the ElGamal Digital Signature algorithm. For this process, the commonly used ordinary 2D Arnold Transform is replaced with a 3D Arnold Transform to better avoid the possibility of brute force cracking. Here, the ElGamal Encryption Algorithm is more random than other public key regime algorithms based on discrete logarithms, and even if certain parameters of the process are stolen, the plaintext cannot be deduced in reverse. The nesting of these two encryption algorithms better enhances the security of the whole model. Except for the encryption algorithms, the model is verified using a digital signature to avoid the risk of biometric image tampering. ElGamal Digital Signatures offer the advantages of randomness, provable security, revocability, and scalability over other digital signature algorithms. The security of the model has been tested through several security tests, such as randomness tests, robustness against noise, noise attacks, and potential attacks, with the encryption working well. In addition to the use of encryption algorithms, the model also uses digital signature algorithms, a nested security model that better protects the integrity and protection of the data from tampering during transmission and makes it easier to verify the authenticity of the images.

As part of our future work, we will take quantum cryptography as the main research direction and continue to improve the algorithm.

Author Contributions: Y.Q.: Methodology, Software, Validation, Formal analysis, Investigation, Writing—original draft, Visualization. B.Z.: Conceptualization, Validation, Formal analysis, Resources, Writing—review and editing, Supervision, Project administration, Funding acquisition. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Natural Science Foundation of China under Grant 61602540.

Institutional Review Board Statement: For this study not involving humans or animals.

Informed Consent Statement: Not applicable.

Data Availability Statement: Portions of the work tested on the Artificial Intelligence Laboratory of FEI in São Bernardo do Campo, São Paulo, Brazil, IITD Touchless Palmprint Database version 1.0, and IITD Iris Database version 1.0.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Dhiman, A.; Gupta, K.; Sharma, D.K. Chapter 1—An introduction to deep learning applications in biometric recognition. In *Trends in Deep Learning Methodologies*; Piuri, V., Raj, S., Genovese, A., Srivastava, R., Eds.; Academic Press: Cambridge, MA, USA, 2021; pp. 1–36. [CrossRef]
2. Guan, Z.-H.; Huang, F.; Guan, W. Chaos-based image encryption algorithm. *Phys. Lett. A* **2005**, *346*, 153–157. [CrossRef]
3. Wang, X.; Feng, L.; Zhao, H. Fast image encryption algorithm based on parallel computing system. *Inf. Sci.* **2019**, *486*, 340–358. [CrossRef]
4. Liu, S.; Guo, C.; Sheridan, J.T. A review of optical image encryption techniques. *Opt. Laser Technol.* **2014**, *57*, 327–342. [CrossRef]
5. Li, C.; Lin, D.; Lü, J.; Hao, F. Cryptanalyzing an Image Encryption Algorithm Based on Autoblocking and Electrocardiography. *IEEE MultiMedia* **2018**, *25*, 46–56. [CrossRef]
6. Gu, J.; Cao, X.-Y.; Fu, Y.; He, Z.-W.; Yin, Z.-J.; Yin, H.-L.; Chen, Z.-B. Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources. *Sci. Bull.* **2022**, *67*, 2167–2175. [CrossRef]
7. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *Theor. Comput. Sci.* **2014**, *560*, 7–11. [CrossRef]
8. Yin, H.-L.; Fu, Y.; Li, C.-L.; Weng, C.-X.; Li, B.-H.; Gu, J.; Lu, Y.-S.; Huang, S.; Chen, Z.-B. Experimental quantum secure network with digital signatures and encryption. *Natl. Sci. Rev.* **2022**, *10*, nwac228. [CrossRef]
9. Wang, K.; Wu, X.; Wang, H.; Kan, H.; Kurths, J. New color image cryptosystem via SHA-512 and hybrid domain. *Multimed. Tools Appl.* **2021**, *80*, 18875–18899. [CrossRef]
10. Hu, W.-W.; Zhou, R.-G.; Luo, J.; Jiang, S.-X.; Luo, G.-F. Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms. *Quantum Inf. Process.* **2020**, *19*, 82. [CrossRef]
11. Elgamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Trans. Inf. Theory* **1985**, *31*, 469–472. [CrossRef]
12. Gordon, D. Discrete Logarithm Problem. In *Encyclopedia of Cryptography and Security*; van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Boston, MA, USA, 2011; pp. 352–353. [CrossRef]
13. Hankerson, D.; Menezes, A. Elliptic Curve Discrete Logarithm Problem. In *Encyclopedia of Cryptography and Security*; van Tilborg, H.C.A., Jajodia, S., Eds.; Springer: Boston, MA, USA, 2011; pp. 397–400. [CrossRef]
14. Chen, G.; Mao, Y.; Chui, C.K. A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos Solitons Fractals* **2004**, *21*, 749–761. [CrossRef]
15. Vollala, S.; Ramasubramanian, N.; Tiwari, U. Cryptographic Techniques. In *Energy-Efficient Modular Exponential Techniques for Public-Key Cryptography: Efficient Modular Exponential Techniques*; Vollala, S., Ramasubramanian, N., Tiwari, U., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 3–30. [CrossRef]
16. Diffie, W.; Hellman, M. New directions in cryptography. *IEEE Trans. Inf. Theory* **1976**, *22*, 644–654. [CrossRef]
17. Guo, Q.; Liu, Z.; Liu, S. Color image encryption by using Arnold and discrete fractional random transforms in IHS space. *Opt. Lasers Eng.* **2010**, *48*, 1174–1181. [CrossRef]
18. Soni, G.K.; Arora, H.; Jain, B. *A Novel Image Encryption Technique Using Arnold Transform and Asymmetric RSA Algorithm*; Springer: Singapore, 2020; pp. 83–90.
19. Chen, W.; Quan, C.; Tay, C.J. Optical color image encryption based on Arnold transform and interference method. *Opt. Commun.* **2009**, *282*, 3680–3685. [CrossRef]
20. Ye, J.; Deng, X.; Zhang, A.; Yu, H. A Novel Image Encryption Algorithm Based on Improved Arnold Transform and Chaotic Pulse-Coupled Neural Network. *Entropy* **2022**, *24*, 1103. [CrossRef]
21. Choudhury, Z.H.; Munir Ahamed Rabbani, M. *Biometric Passport Security by Applying Encrypted Biometric Data Embedded in the QR Code*; Springer: Singapore, 2020; pp. 41–52.
22. Nouioua, N.; Seddiki, A.; Ghaz, A. Medical Image Watermarking Scheme in Transform Domain Based on Asymmetric Crypto-System and Arnold Chaotic Map. In Proceedings of the 2021 44th International Conference on Telecommunications and Signal Processing (TSP), Brno, Czech Republic, 26–28 July 2021.
23. Laiphrakpam, D.S.; Khumanthem, M.S. Medical image encryption based on improved ElGamal encryption technique. *Optik* **2017**, *147*, 88–102. [CrossRef]
24. Hashim, H.R.; Neamaa, I.A. Image Encryption and Decryption in A Modification of ElGamal Cryptosystem in MATLAB. *arXiv* **2014**, arXiv:1412.8490.
25. Lone, M.A.; Qureshi, S. RGB image encryption based on symmetric keys using Arnold transform, 3D chaotic map and affine hill cipher. *Optik* **2022**, *260*, 168880. [CrossRef]
26. Thomas, S.; Krishna, A.V.N. Securing grayscale image using improved Arnold transform and ElGamal encryption. *J. Electron. Imaging* **2022**, *31*, 063012. [CrossRef]

27. Chen, L.; Shen, A.D. A Novel Public Key Image Cryptosystem Based on Elliptic Curve and Arnold Cat Map. *Adv. Mater. Res.* **2014**, *989–994*, 4183–4186. [CrossRef]
28. Luo, Y.; Ouyang, X.; Liu, J.; Cao, L. An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems. *IEEE Access* **2019**, *7*, 38507–38522. [CrossRef]
29. Parida, P.; Pradhan, C.; Gao, X.Z.; Roy, D.S.; Barik, R.K. Image Encryption and Authentication with Elliptic Curve Cryptography and Multidimensional Chaotic Maps. *IEEE Access* **2021**, *9*, 76191–76204. [CrossRef]
30. Parida, P.; Pradhan, C.; Alzubi, J.A.; Javadpour, A.; Gheisari, M.; Liu, Y.; Lee, C.-C. Elliptic curve cryptographic image encryption using Henon map and Hopfield chaotic neural network. *Multimed. Tools Appl.* **2023**. [CrossRef]
31. Katz, J.G. *Digital Signatures*, 1st ed.; Springer Science + Business Media: New York, NY, USA, 2010. [CrossRef]
32. Merkle, R.C. *A Digital Signature Based on a Conventional Encryption Function*; Springer: Berlin/Heidelberg, Germany, 1988; pp. 369–378.
33. Schneider, M.; Shih-Fu, C. A robust content based digital signature for image authentication. In Proceedings of the 3rd IEEE International Conference on Image Processing, Lausanne, Switzerland, 19 September 1996; Volume 3, pp. 227–230. [CrossRef]
34. Alam, S.; Jamil, A.; Saldhi, A.; Ahmad, M. Digital image authentication and encryption using digital signature. In Proceedings of the 2015 International Conference on Advances in Computer Engineering and Applications, Ghaziabad, India, 19–20 March 2015; pp. 332–336. [CrossRef]
35. Nikolaidis, N.; Pitas, I. Copyright protection of images using robust digital signatures. In Proceedings of the 1996 IEEE International Conference on Acoustics, Speech, and Signal Processing Conference Proceedings, Atlanta, GA, USA, 9 May 1996; Volume 4, pp. 2168–2171.
36. Pan, W.; Coatrieux, G.; Cuppens-Boulahia, N.; Cuppens, F.; Roux, C. *Medical Image Integrity Control Combining Digital Signature and Lossless Watermarking*; Springer: Berlin/Heidelberg, Germany, 2010; pp. 153–162.
37. Chang, Y.-S.; Wu, T.-C.; Huang, S.-C. ElGamal-like digital signature and multisignature schemes using self-certified public keys. *J. Syst. Softw.* **2000**, *50*, 99–105. [CrossRef]
38. Li, X.; Shen, X.; Chen, H. ElGamal Digital Signature Algorithm of Adding a Random Number. *J. Netw.* **2011**, *6*, 774. [CrossRef]
39. Thomaz, C.E. FEI Face Database. 2012. Available online: https://fei.edu.br/~cet/facedatabase.html (accessed on 11 June 2023).
40. Kumar, A. *IIT Delhi Touchless Palmprint Database (Version 1.0)*; IIT Delhi: New Delhi, India, 2014.
41. Kumar, A. *IIT Delhi Iris Database (Version 1.0)*; IIT Delhi: New Delhi, India, 2008.
42. Bradski, G. The Opencv Library. *Dr. Dobb's J. Softw. Tools* **2000**, *25*, 122–125.
43. Erkan, U.; Toktas, A.; Enginoğlu, S.; Akbacak, E.; Thanh, D.N.H. An image encryption scheme based on chaotic logarithmic map and key generation using deep CNN. *Multimed. Tools Appl.* **2022**, *81*, 7365–7391. [CrossRef]
44. Rehman, A.U.; Liao, X.; Ashraf, R.; Ullah, S.; Wang, H. A color image encryption technique using exclusive-OR with DNA complementary rules based on chaos theory and SHA-2. *Optik* **2018**, *159*, 348–367. [CrossRef]
45. Wu, X.; Kan, H.; Kurths, J. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps. *Appl. Soft Comput.* **2015**, *37*, 24–39. [CrossRef]