inventions

MDPI

Article

A Comparative Assessment of Homomorphic Encryption Algorithms Applied to Biometric Information

Georgiana Crihan , Marian Crăciun and Luminița Dumitriu *

Faculty of Automation, Computer Sciences, Electronics and Electrical Engineering, "Dunărea de Jos" University, Științei Street No. 2, 800210 Galați, Romania; georgian.crihan@ugal.ro (G.C.); marian.craciun@ugal.ro (M.C.)
* Correspondence: luminita.dumitriu@ugal.ro

Abstract: This paper provides preliminary research regarding the implementation and evaluation of a hybrid mechanism of authentication based on fingerprint recognition interconnected with RFID technology, using Arduino modules, that can be deployed in different scenarios, including secret classified networks. To improve security, increase efficiency, and enhance convenience in the process of authentication, we perform a comparative assessment between two homomorphic encryption algorithms, the Paillier partial homomorphic algorithm and the Brakerski–Gentry–Vaikuntanathan fully homomorphic encryption scheme, applied to biometric templates extracted from the device mentioned above, by analyzing factors such as a histogram analysis, mean squared error (MSE), peak signal-to-noise ratio (PSNR), the structural similarity index measure (SSIM), the number of pixel change rate (NPCR), the unified average changing intensity (UACI), the correlation coefficient, and average encryption time and dimension. From security and privacy perspectives, the present findings suggest that the designed mechanism represents a reliable and low-cost authentication alternative that can facilitate secure access to computer systems and networks and minimize the risk of unauthorized access.

Keywords: security; Paillier algorithm; BGV algorithm; Arduino modules; encryption assessment

check for updates

Citation: Crihan, G.; Crăciun, M.; Dumitriu, L. A Comparative Assessment of Homomorphic Encryption Algorithms Applied to Biometric Information. *Inventions* **2023**, *8*, 102. https://doi.org/10.3390/inventions8040102

Academic Editor: Braghin Francesco

Received: 28 June 2023
Revised: 19 July 2023
Accepted: 8 August 2023
Published: 11 August 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The proliferation of attack vectors in the whole network infrastructure has a considerable impact on the entire spectrum of information security because it offers adversaries the opportunity to exploit device vulnerabilities and weaknesses for various purposes, including accessing, modifying, deleting, or releasing sensitive information; changing system configurations; installing malicious code; or denying system access to authorized users. Exploitation of software or hardware devices' shortcomings determines the degradation of system resources and capabilities and also provides a great opportunity to compromise the confidentiality, integrity, and availability of an information system. These unfavorable circumstances determined the emergent need to develop and implement physical protective measures in order to improve authentication capabilities and avoid unauthorized release or disclosure of confidential information and potential escalation of user privileges.

To achieve the goal of strengthening authentication systems, a hybrid mechanism of authentication is designed and proposed, based on the complementary application of three main authentication factors, namely, the biometric component ("something you are"), the RFID, and the cryptographic component ("something you have") [1]. Systems that incorporate multi-factor authentication are considered to be more powerful and robust compared to those that use only one factor and have the role of increasing the degree of data security in the process of verifying the identity of an authorized user who tries to access a computer system. According to [2], biometric factors and cryptographic algorithms are among the strongest factors of authentication that could ensure the highest level of protection for information and could be implemented and adopted in a wide variety of domains with strict requirements for maintaining user confidentiality, especially in military network architectures, as presented in Figure 1.

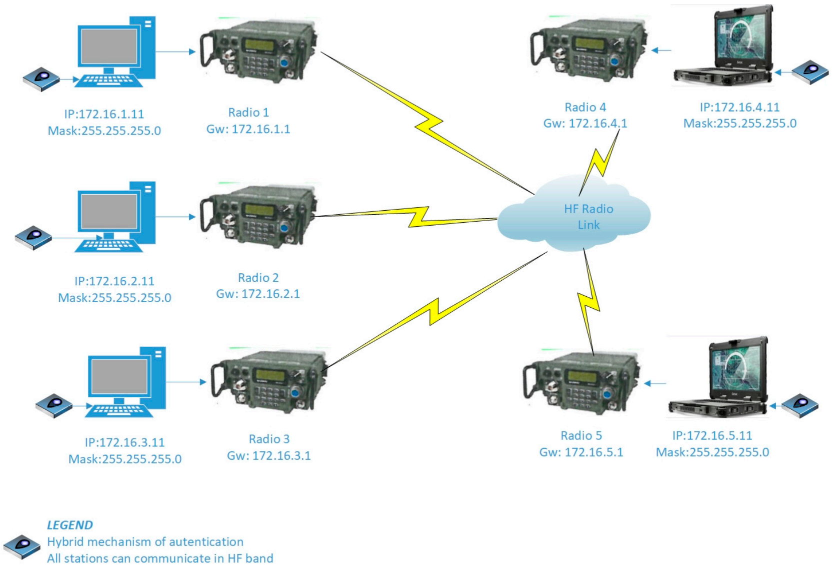


Figure 1. Implementation of the hybrid mechanism of authentication in the architecture of a radio network.

The main objective of this research is to develop a comparative analysis between two homomorphic encryption algorithms, the Paillier partially homomorphic encryption algorithm and the BGV (Brakerski–Gentry–Vaikuntanathan) fully homomorphic encryption scheme, to identify the most efficient algorithm of encryption that can be tested on biometric templates extracted from the hybrid mechanism of authentication. More specifically, this tool intends to provide secure and reliable authentication in computer systems and network devices in order to counteract the limitations and vulnerabilities of the mentioned elements and also to prevent emerging computer attacks.

Homomorphic encryption is a special cryptographic construction, a niche structure of modern cryptography that builds on the concept of homomorphism and allows a third party (cloud, service provider) to execute certain operations over the encrypted data while maintaining function characteristics and encrypted data formats. The applicability of homomorphic encryption was demonstrated in several data privacy applications, such as healthcare systems, financial domains, surveillance systems, cloud-encrypted email storage, online retail, border control systems, e-voting systems, and privacy-preserving advertising systems. Depending on the type and number of operations that can be performed on them, homomorphic encryption schemes are classified into the following types: partially homomorphic encryption (PHE), somewhat homomorphic encryption (SHE), or fully homomorphic encryption (FHE) [3].

Researchers developed early security assessments of the homomorphic encryption algorithms applied in biometric authentication, such as the PHE Paillier, ElGamal [4–7], and FHE [8–10], to maintain the security and privacy of the biometric templates and to improve the performance of parameters like speed, security, dimension, and accuracy. Several representative techniques will be described using the examples above.

The authors of [11] designed and launched a novel, effective, lightweight homomorphic cryptographic technique that contains two layers of encryption. The first layer uses a symmetric key algorithm and substitution/permutation structural approaches inspired by Feistel mixed with Shannon's theory of diffusion/confusion by the participation of logical operations (such as XOR, XNOR, shifting, sapping), and the second layer uses a multiplicative homomorphic R.S.A. algorithm considered for improving information security in cloud computing.

The authors of [12] suggested a method for the high-security level of information in cloud computing by using deployed data on the public cloud platform "Contabo" and testing it on real-world aviation data using a single keyword searchable encryption (SKSE) scheme, which is implemented using the Paillier encryption algorithm.

According to [13], an optimized privacy-preserving bimodal authentication system is proposed, using the Brakerski/Fan–Vercauteren (BFV) HE scheme over the fused template generated by the combination of fingerprint and iris images of the user, to overcome the drawbacks of biometric cryptosystems and cancelable biometrics.

Some improvements and efficient achievements were submitted in [14], where in-depth experimental examinations were carried out using bloom filters and fully homomorphic encryption to design hybrid biometric template protection schemes based on iris recognition that aim to obtain high recognition accuracy and to protect sensitive biometric information during storage.

A novel approach to FHE implementation was presented in [15], which devised an Automated Speech Recognition (ASR) system based on voice feature verification and the Cheon–Kim–Kim–Song (CKKS) fully homomorphic encryption scheme to obtain a real-time and non-interactive solution that processes encrypted speech data suitable for real-time speaker verification systems.

Despite these various studies regarding the implementations of different homomorphic encryption techniques for securing behavioral or physiological biometrics that provide similar functionality with our approach based on PHE and FHE, we present a new perspective and a different technical solution for enhancing user security in the authentication process in order to maintain confidentiality, integrity, and availability of information, and also we propose newer scenarios for deployment.

In contrast to the biometric and cryptographic methods presented above, the main contributions of this present research are as follows:

1. Develop, install, and configure an authentic hybrid mechanism of authentication, three-structural-layered for standalone system and network devices, that is created by interconnecting several Arduino modules and designed specifically for fingerprint biometrics.
2. Enhance the storage security of user biometric information by encrypting the data using the Paillier homomorphic encryption algorithm or BGV fully homomorphic encryption algorithm.
3. Perform a comparative analysis between the selected homomorphic encryption algorithms using several statistical parameters, specific to the image processing field, in order to identify and evaluate the most efficient and convenient algorithm that can provide strong security while achieving good recognition performance.

Even if intense development and simulations have been carried out in these research areas, the originality of this work derives from the implementation level, because we have conducted an extensive analysis of the homomorphic encryption algorithms on a dedicated mechanism of authentication, specially designed for improving authentication capabilities.

The present study is organized as follows: in the Introduction, a brief description and state-of-the-art review of existing homomorphic cryptographic algorithms used to secure biometric information in the literature are provided; Section 2 describes the structure of the homomorphic algorithms and the design of the hybrid authentication mechanism based on a biometric element combined with RFID technology; Section 3 presents the experimental results and the research findings in detail, comparing and evaluating the performance of the proposed cryptographic algorithms, and is followed by the conclusion in Section 4.

2. Materials and Methods

For the practical implementation of this work, a hybrid authentication system that has the smart capacity to perform biometric and RFID enrollment, verification, and identification with security guarantees, low cost, high performance, and a template protection warranty; to store data; and to transmit it over insecure channels is designed, as presented in Figure 2.

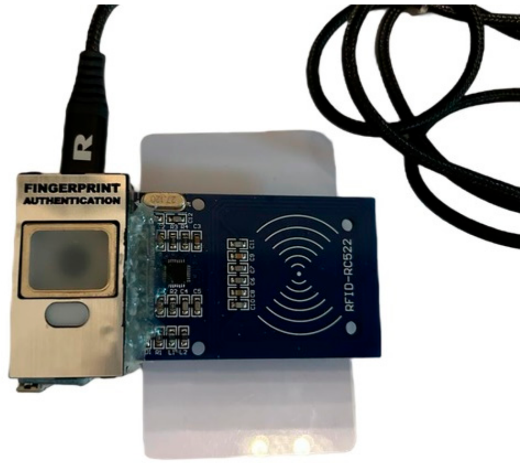
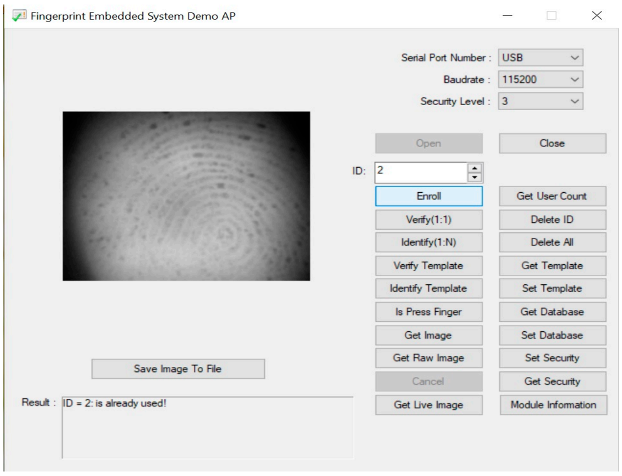


Figure 2. Hybrid authentication mechanism based on Arduino modules [16].

The authentication mechanism represents an efficient technical solution that optimizes the authentication process and integrates secure and reliable Arduino components, such as an Arduino Pro Micro 5 V/16 MHz development board integrated with a Radio Frequency Identification (RFID) reader and a powerful biometric fingerprint sensor module. The fingerprint and ID card serial data enrollment and the authentication algorithm are realized through Arduino Software IDE and its additional libraries MFRC522 and FPS_GT511C3.

The biometric information taken by the fingerprint sensor is saved onsite. The retrieval of the database and the performance of various operations such as registration, verification, and identification are carried out through a USB connection with the fingerprint sensor software, as can be seen in the screenshot of the application presented in Figure 3.


Fingerprint Embedded System Demo AP

Serial Port Number : USB
Baudrate : 115200
Security Level : 3

ID: 2

Result : ID = 2: is already used!

Figure 3. Fingerprint sensor software.

But the main focus of this paper consists in the biometric database encryption that is stored in the computer system. The encryption schemes used in this research are the partially homomorphic Paillier encryption algorithm and the fully homomorphic encryption algorithm BGV, special cases of asymmetric encryption that use a public key for encryption and a private key for decryption. The mentioned algorithms allow performing different operations on the encrypted data itself without the need to decrypt it, not only during transit and storage but also during computation.

The concept of homomorphic encryption presents a significant advantage because access to the encrypted information is restricted by the user, who is the only one who has total control over the information dissemination process. Personnel with administrative rights, such as the security administrator or system administrator, cannot access the original information stored in such encrypted databases. This advantage is determined by the fact that the user creates and manages his encryption keys and can restrict access to the original data. Similarly, the service providers that provide storage capacity for various cloud databases, such as Amazon Web Service (AWS), Oracle, Microsoft Azure, OpenStack, Google Drive, and MongoDB, cannot access the original information.

In the present research, we choose to implement and make a comparative analysis between two different homomorphic encryption algorithms because they represent an innovative technology that brings a major change in the way confidential information is protected, processed, and shared and fundamentally changes the course of the cryptographic process.

2.1. Homomorphic Encryption Using Paillier Algorithm

The Paillier encryption algorithm supports a partially homomorphic scheme based on addition operations that generates two types of keys for biometric data encryption: a public key (n, g), where n is the modulus and g is the encryption basis, that is publicly released and a private decryption key (λ, μ) that is kept secret.

This algorithm comprises the three main operations as specified in [17], key generation, encryption, and decryption. For the initial setup, the algorithm takes as input several parameters, such as two random large prime numbers p and q, n computed by using the formula $n = p \times q$, $\lambda(n) = l$ cm ($p - 1, q - 1$), a random integer g, and μ calculated with the modular multiplicative mathematical formula

$$\mu = \left(L\cdot\left(g^{\lambda}\cdot mod\ n^2\right)\right)^{-1} mod\ n \tag{1}$$

where function $L(x)$ represents a quotient of $(x - 1)$ divided by n.

The encryption phase generates a ciphertext using the formula

$$c = g^m \cdot r^n \left(mod\ n^2\right) \tag{2}$$

The number r is randomly selected for each message m, where $0 < r < n$ and $r \in Z^*_{n^2}$, respecting the condition gcd (r, n) = 1.

Decryption assumes the existence of a ciphertext that needs to be decrypted, $c \in Z^*_{n^2}$, using a private key (λ, μ), from which the message m = *Decrypt*(c; λ, μ) results. The decryption process is carried out as follows:

$$m = \frac{L\cdot\left(c^{\lambda} mod\ n^2\right)}{L\cdot\left(g^{\lambda} mod\ n^2\right)} \cdot mod\ n = L\cdot\left(c^{\lambda} mod\ n^2\right)\cdot\mu \times mod\ n \tag{3}$$

Considering two ciphertexts according to the encryption scheme presented below, the addition and multiplication operations are defined by the following equations:

$$c_1 = g^{m_1} \cdot r_1^n \left(mod\ n^2\right) \tag{4}$$

$$c_2 = g^{m_2} \cdot r_2^n \left(mod\ n^2\right) \tag{5}$$

$$\begin{aligned} E(m_1)\cdot E(m_2) &= \left(g^{m_1}\cdot r_1^n\ \left(mod\ n^2\right)\right)\cdot\left(g^{m_2}\cdot r_2^n\ \left(mod\ n^2\right)\right) \\ &= g^{m_1+m_2}\cdot\left(r_1\cdot r_2\right)^n\left(mod\ n^2\right)\big) \\ &= E(m_1) + E(m_2) \end{aligned} \tag{6}$$

2.2. Homomorphic Encryption Using BGV (Brakerski–Gentry–Vaikuntanathan) Algorithm

The BGV fully homomorphic encryption algorithm is based on a learning-with-error (LWE/RLWE) scheme composed of polynomial rings, which allows both additive and multiplicative operations. Both plaintext and ciphertext are defined on rings, so homomorphic ciphertext encryption and decryption are closely related to operations on plaintext rings [18].

Since the algorithm offers the possibility of processing data without being decrypted, it can be exploited in key areas with high-security requirements that require the adoption of optimized solutions for the protection of confidential information. Compared to the previous algorithm, characterized by the three operations of key generation, encryption, and decryption, the BGV algorithm involves an additional step that consists in evaluating the homomorphic circuit. The evaluation involves performing a function over the ciphertexts (c_1, c_2) without seeing the messages (m_1, m_2), which takes as an input point the ciphertexts from which the evaluated ciphertexts result. The encryption scheme will be defined by ε = (KeyGen, Encrypt, Decrypt, Evaluate) for a circuit *C*, having the input parameter *t*, the encryption key pair $(sk,\ pk)$ generated via the KeyGen function, the plaintext messages $m = (m_1, m_2 \ldots .m_t)$, and the encrypted texts $c = (c_1, c_2 \ldots .c_t)$, so that the result will be concretized by the formulas [19]

$$c_i = Encryption(pk, m_i) \tag{7}$$

$$Decryption(sk,\ Evaluation(pk,\ C,\ c)) = C(m_1, m_2 \ldots .m_t) \tag{8}$$

The specificity of the fully homomorphic encryption scheme BGV lies in the fact that it allows an arbitrary number of additive or multiplicative operations to be executed on the input ciphertexts without changing the content of the resulting ciphertext, in which the noise level expands simultaneously with the number of operations performed.

The addition operation increases noise considerably more slowly than the multiplication operation and does not involve refreshing the ciphertext after each operation is performed. Decryption operates correctly as long as this noise is below a certain bound, which limits the number of homomorphic operations one can accomplish.

This deficiency can be mitigated in the BGV encryption algorithm by implementing two additional procedures. The first procedure is called "Key Switching" or "Relinearization", and the second is "Modulus Switching" or "Modulus Reduction"; their purpose is to reduce the noise within the ciphertext to a manageable level and realize the decryption operation in a timely and efficient manner [20].

The phasing of the BGV encryption scheme can be rendered mathematically as follows:

2.2.1. Key Generation

This algorithm has as input the security parameter $\lambda \in Z$, a number representing the security level (128, 192, 256) of the algorithm; a vector *n*; an odd modulus *q*; a distribution noise χ over the ring *A*, which is usually chosen to be a Gaussian distribution, $N = [(2n+1)logq]$; and output a double key (*pk*, *sk*), where *pk* is the public key used for encryption and *sk* is the secret key used for decryption. It should be emphasized that the encryption scheme used will be characterized by a set of parameters (*q*, *d*, *n*, *N*) and by a noise distribution value χ as small as possible. The ring size *dj* and the noise distribution χj are independent of *L*, which indicates the operation level and can be denoted as $d = d_L$ and $\chi = \chi_L$, respectively.

The secret key *sk* is a collection of randomly selected vectors $\overrightarrow{s_j}$, where each vector $\overrightarrow{s} \leftarrow (1,\ s'_1,\ s'_2 \ldots ..s'_n) \in A_q^{n+1}$ and each $s' \leftarrow \chi^n$ [21].

Using the previously estimated parameters, a uniform matrix $A' \leftarrow A_q^{Nxn}$ and an *N*-dimensional noise vector $\overrightarrow{e} \leftarrow \chi^N$ are generated, so that $\overrightarrow{b} \leftarrow A's' + 2\overrightarrow{e}$. Thus, the public key is given by the collection $A'_j s$.

2.2.2. Encryption

Given $m \in A_2$, the message intended to be encrypted and the generated public key A, we set the vector $\overrightarrow{m} \leftarrow (m,\ 0,\ 0\ldots 0) \in A_q^{n+1}$ for the vector dimension n and modulus q defined in the parameter set in the previous sections. A random vector $\overrightarrow{r} \leftarrow A_2^N$ is usually chosen from a uniform distribution. After calculating the message vector $\overrightarrow{m}$, taking the randomly chosen vector $\overrightarrow{r}$, and given the public key A, we define the encrypted text by the formula $\overrightarrow{c} = \overrightarrow{m} + A^T r \in A_q^{n+1}$, where A^T denotes the transposition of the matrix A.

2.2.3. Decryption

To decrypt the ciphertext under a secret key $\overrightarrow{s_j}$, an inner product is executed, followed by two modulo operations, first with the ciphertext modulo q, followed by the plaintext modulo p. The decryption formula produces a plaintext message:

$$m \leftarrow \left[\left[\left\langle \overrightarrow{c}, \overrightarrow{s_j} \right\rangle\right]_q\right]_2 \tag{9}$$

2.2.4. Evaluation

During this phase, arithmetic operations that can be performed on ciphertexts are those of addition or multiplication, as follows:

- $EvalAdd(p_k, c_1, c_2)$—given two ciphertexts $c_1 = E(m_1)$ and $c_2 = E(m_2)$, the operation of adding the two will result in a new ciphertext that will contain the sum of the previous ones:
$$c_3 = E(m_1 + m_2) = E(m_1) + E(m_2) = c_1 + c_2 \tag{10}$$
- $EvalMult(p_k, c_1, c_2)$ that will contain a ciphertext with the product of the previous ones:
$$c_3 = E(m_1 \cdot m_2) = E(m_1) \cdot E(m_2) = c_1 \cdot c_2 \tag{11}$$

The BGV encryption algorithm is considered a secure encryption scheme because there are no known attacks published in the literature; the security comes from the hardness of the LWE/RLWE problem and the choice of optimal parameters that maximize results and respect security constraints.

3. Results and Discussion

In our comparative analysis, the proposed encryption homomorphic algorithms were tested using biometric fingerprints from ten different users who logged into computer systems with the Windows 10 operating system, generated by the hybrid mechanism of authentication, as presented in Figure 4. For the performance and efficiency evaluation of each encryption algorithm, several statistical parameters were applied, such as histogram analysis, mean squared error (MSE), peak signal-to-noise ratio (PSNR), the structural similarity index measure (SSIM), the correlation coefficient, the number of pixel change rate (NPCR), the unified average changing intensity (UACI), ciphertext dimensions, and average encryption time. The experimental results are developed and implemented in Python software and its open-source libraries dedicated to image processing, using biometric images extracted from the Arduino dataset.

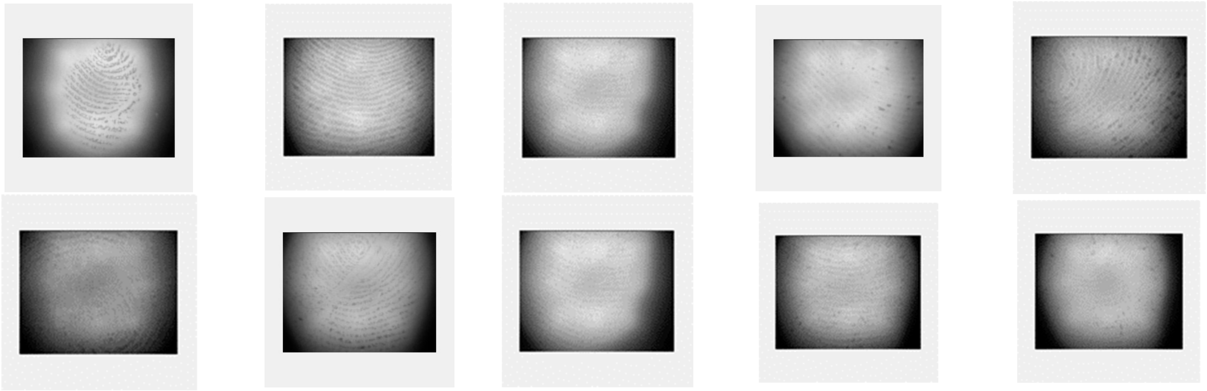


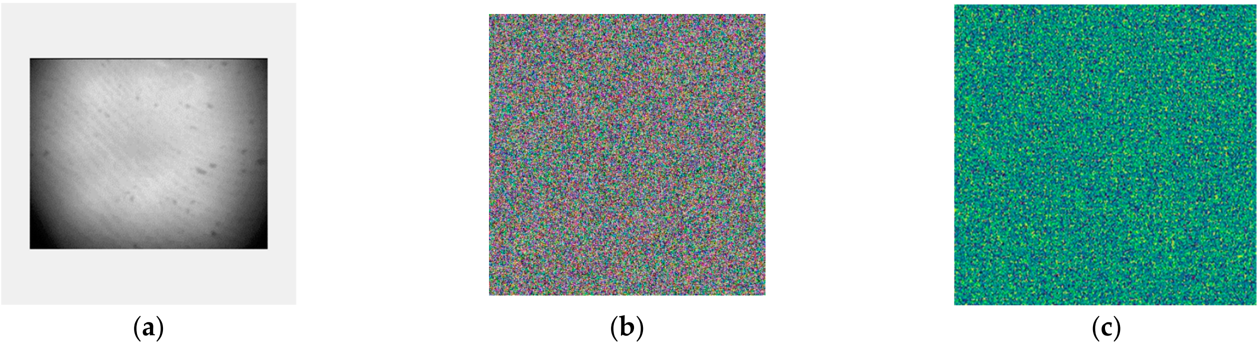
Figure 4. Users' biometric fingerprints used for experimental results.

In the following part, both algorithms are thoroughly analyzed with different file sizes as well as time estimates for encryption and decryption.

3.1. Histogram Analysis

As a primary step in evaluating the efficiency and security provided by the homomorphic encryption algorithms applied to an encrypted image, the histogram is a widely used instrument for image processing that displays the frequency distribution of every pixel intensity of the image in a gray-scale graphical representation, by generating different personalized patterns.

By examining the appearance and structure of the histograms presented in Figures 5 and 6, obvious differences regarding the pixel intensity and uniformity can be noted between the original image and its encrypted versions with the Paillier cryptosystem and the BGV fully homomorphic encryption algorithm. These three histograms highlight a significant difference in the gray level distribution, which is a mandatory condition for a perfectly secure algorithm, which must generate completely different and balanced histograms compared to the original image to avoid any suspicion concerning the clear template and to make it difficult or impossible for a potential attacker to distinguish and reconstruct the original.

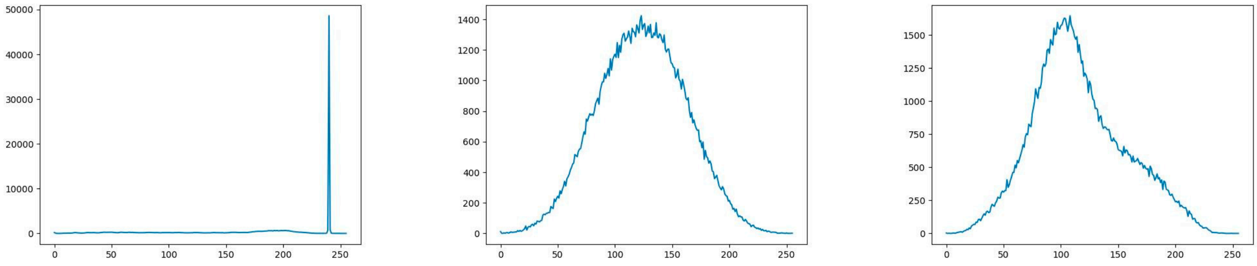


(**a**) (**b**) (**c**)

Figure 5. Graphical image representation: (**a**) Original biometric image, (**b**) Encrypted image using the Paillier algorithm, (**c**) Encrypted image using the BGV algorithm.

Even though all three histograms display unimodal distributions because they have only one peak, the first plotting histogram of the original image, which has a right-skewed distribution in the graphic bar, indicates a bright and luminous pixel distribution, while the other two histograms of the encrypted images are roughly symmetric and characterized by a reasonable and uniform distribution. Also, in the histograms below, essential information is given by the X-axis, which represents the pixel intensity, and the Y-axis, which shows the frequency of occurrence and indicates the degree of data uncertainty and diffusion.

In this case, the values of the *X*-axis are constant with the specific range bins between [0, 255], while the values of the *Y*-axis denote notably different values. Higher numbers on the *Y*-axis indicate better performance, and in this case, comparing the histograms of the encrypted images, slightly better values are obtained through the BGV encryption algorithm.



(**a**) (**b**) (**c**)

Figure 6. Histogram after different types of processing: (**a**) Histogram of the original biometric image, (**b**) Histogram of the encrypted image using the Paillier algorithm, (**c**) Histogram of the encrypted image using the BGV algorithm.

3.2. Mean Squared Error, Peak Signal-to-Noise Ratio, Structural Similarity Index Measure (SSIM), and Correlation Coefficient Analysis

Other reference parameters used for the statistical qualitative evaluation of an encrypted biometric image in digital image processing are the mean squared error (MSE), peak signal-to-noise ratio (PSNR), and the correlation coefficient, which can be represented mathematically as follows [22]:

$$\mathrm{MSE} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{\mathrm{i}=1}^{\mathrm{M}} \sum_{\mathrm{J}=1}^{\mathrm{N}} [\mathrm{M}(\mathrm{i},\mathrm{j}) - \mathrm{F}(\mathrm{i},\mathrm{j})]^2 \tag{12}$$

$$\mathrm{PSNR} = 10^{\mathrm{x}} \ln(\mathrm{f}_{\mathrm{max}}/\mathrm{MSE})^2 \tag{13}$$

$$\mathrm{r} = \frac{\sum_{\mathrm{m}} \sum_{\mathrm{n}} (\mathrm{A}_{\mathrm{mn}} - \overline{\mathrm{A}})(\mathrm{B}_{\mathrm{mn}} - \overline{\mathrm{B}})}{\sqrt{(\sum_{\mathrm{m}} \sum_{\mathrm{n}} (\mathrm{A}_{\mathrm{mn}} - \overline{\mathrm{A}})^2)(\sum_{\mathrm{m}} \sum_{\mathrm{n}} (\mathrm{B}_{\mathrm{mn}} - \overline{\mathrm{B}})^2}} \tag{14}$$

Preliminary research findings demonstrated that for obtaining a good image quality, the PSNR value increases gradually, satisfying the condition that the higher the value of the encrypted image, the better the image quality and the lower the errors. On the other hand, a small value of PSNR implies large numerical differences between images but suggests a good encryption algorithm. Also, lower MSE values approaching 0 indicate better accuracy and a lower level of errors between images. The values listed below provide significant results for image quality assessment, as illustrated in Table 1. While the PSNR is used to measure the quality between the original image and the encrypted version in the presence of noise, with values that usually range between 30 to 50 dB for an 8-bit image, the MSE is a regression indicator that measures the amount of error between these types of images, calculated by averaging the squared intensity difference of the pixels.

One of the most precise and novel measures for image quality assessment, which has grown in popularity lately among research communities, is the structural similarity index measure (SSIM), which according to [23] is based on a comparison between an original image *x* and a potentially modified version of the same image *y* and comprises three independent and highly structured components extracted at a single spatial scale (resolution): luminance (l), contrast (c), and structure (s). From a mathematical standpoint, these components can be calculated as described below:

$$\mathrm{SSIM}(x,y) = \left[l(x,y)\right]^{\alpha}\cdot[c(x,y)]^{\beta}\cdot[s(x,y)]^{\gamma} \tag{15}$$

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{{\mu_x}^2+{\mu_y}^2+C_1} \tag{16}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{{\sigma_x}^2+{\sigma_y}^2+C_2} \tag{17}$$

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y+C_3} \tag{18}$$

Table 1. Statistical analysis metrics.

Statistic Metrics Biometric Images	MSE		PSNR		Correlation Coefficient (Raw/Encrypted)		Correlation Coefficient (Raw/Decrypted)		SSIM	
	Paillier	**BGV**	**Paillier**	**BGV**	**Paillier**	**BGV**	**Paillier**	**BGV**	**Paillier**	**BGV**
User 1 fingerprint	0.1290	0.1484	27.942	27.927	0.1781	0.1607	0.9911	0.9931	0.9524	0.9698
User 2 fingerprint	0.1220	0.1402	27.948	27.937	0.1798	0.1608	0.9919	0.9949	0.9517	0.9707
User 3 fingerprint	0.1203	0.1427	27.857	27.936	0.1801	0.1570	0.9906	0.9946	0.9547	0.9778
User 4 fingerprint	0.1206	0.1396	27.954	27.937	0.1779	0.1623	0.9922	0.9962	0.9565	0.9721
User 5 fingerprint	0.1324	0.1459	27.894	27.958	0.1774	0.1568	0.9930	0.9970	0.9532	0.9738
User 6 fingerprint	0.1481	0.1556	28.001	27.953	0.3537	0.1578	0.9745	0.9785	0.9535	0.9733
User 7 fingerprint	0.1268	0.1432	27.953	27.946	0.3558	0.1582	0.9701	0.9741	0.9543	0.9737
User 8 fingerprint	0.1260	0.1464	27.943	27.928	0.3546	0.1594	0.9693	0.9733	0.9563	0.9743
User 9 fingerprint	0.1276	0.1448	27.941	27.944	0.3595	0.1646	0.9703	0.9743	0.9528	0.9753
User 10 fingerprint	0.1258	0.1448	27.958	27.948	0.3585	0.1590	0.9723	0.9763	0.9553	0.9739

The resulting values of the SSIM factor vary in the interval [0, 1], where values that are close to zero indicate low quality, no association, and noticeable differences between the analyzed images, in contrast to values that are approaching 1, which indicate perfect similarity and a high level of correspondence between images and mean that both images can be well perceived and distinguishable by the human visual system. Research paper [24] reveals several interesting aspects regarding the relationship between MSE and SSIM, in the sense that although SSIM is considered to be a perception-based index, and MSE is not a perception-based metric, they have a close liaison and perform similarly, a fact demonstrated by the tests developed on a range of images using different values for the specific coefficients involved in their mathematical formulas.

The correlation coefficient, defined as well as the correlation between adjacent pixels, is a relevant parameter in the context of statistical analysis when measuring the similarities and differences between two variables, the original biometric image, and the encrypted image, because its values indicate the capability of a device to face certain statistical attacks [25].

The correlation coefficient is distributed in the range [−1, 1], where the value −1 highlights a negative correlation and a considerable difference between the initial biometric image and its encryption, whereas the positive value of +1 illustrates a positive correlation and a perfect similarity and correlation between the images. Otherwise, if the correlation coefficient approaches 0, it indicates a lack of correlation and resemblance between the original image and its encrypted version, which emphasizes the strength of the encryption algorithm. Moreover, the achievement of higher efficiency for the implemented cryptographic algorithm applied to the designed system can be defined as low correlation coefficients between the raw and encrypted images but high correlation coefficients between the raw and decrypted images. We considered it necessary to extend the analysis of the correlation coefficient in these two categories (raw/encrypted, raw/decrypted), to observe the intervals in which the values vary and to have a clearer picture of the differences between the two algorithms, as shown in Table 1.

When interpreting the PSNR values, it can be seen that both homomorphic algorithms are similar; the lower values indicate a good encryption scheme applied for HE Paillier and BGV. On the other side, a small difference can be noticed between the MSE values; better average values approaching 0 are obtained with the Paillier algorithm, which suggests better implementation efficiency and accuracy compared to the BGV algorithm.

As evidenced in Table 1, the correlation coefficient between the original biometric image and the encrypted biometric image is close to 0, which means that there is no correlation between the two types of images, highlighting the encryption performance of the cryptographic algorithms chosen for implementation. Also, from the values generated by the cryptographic algorithms, it can be seen that the lower values are obtained through the BGV algorithm, which shows that this encryption scheme is better, providing an improved level of security. The correlation coefficient between the original biometric image and the decrypted biometric image is close to +1, which indicates that through the decryption process, the algorithm can practically achieve a similar image to the original without errors.

When comparing the SSIM values from Table 1, it becomes clear that better values are obtained through the BGV algorithm, although the differences seem to be relatively small. The SSIM values in the table highlight the efficiency of the BGV homomorphic encryption algorithm, in addition to the fact that through this algorithm an image with a level of similarity equivalent to the original can be obtained through the decryption process.

The small difference between the values of the calculated parameters denotes the high precision, accuracy, and stability of the biometric sensor used to design the authentication mechanism, a fact presented in the technical description of the device and demonstrated in this present research.

3.3. Number of Pixel Change Rate and Unified Average Changing Intensity Analysis

Two representative factors for the quantitative evaluation of the encryption algorithms' efficiency are the number of pixel change rate (NPCR) and the unified average changing intensity (UACI), used to measure the differences between two encrypted images C_1 and C_2 resulting from the application of cryptographic algorithms on plain templates. NPCR measures the number of different elements between the encrypted images C_1 and C_2 in percentage, with a percentage of 100% indicating that the images are totally different, while the UACI measures the average intensity of differences between the original encrypted image and the encrypted image resulting from the modification of the original image. Given two clear images, P_K—the biometric image obtained from the biometric sensor and $\overline{P_K}$-the image modified by changing one pixel, their encrypted forms C_K and $\overline{C_K}$, UACI, and NPCR can be defined by the following mathematical formulas [26]:

$$\mathrm{UACI} = \frac{1}{\mathrm{M} \times \mathrm{N} \times \mathrm{O}} \sum\nolimits_{\mathrm{X}=1}^{\mathrm{M}} \sum\nolimits_{\mathrm{Y}=1}^{\mathrm{N}} \sum\nolimits_{\mathrm{Z}=1}^{\mathrm{O}} \left[\frac{\mathrm{C_K}\big(\mathrm{X},\mathrm{Y},\mathrm{Z}\big) - \overline{\mathrm{C_K}}(\mathrm{X},\mathrm{Y},\mathrm{Z})\big)}{255} \right] \tag{19}$$

$$\mathrm{NPCR} = \frac{1}{\mathrm{M} \times \mathrm{N} \times \mathrm{O}} \sum_{\mathrm{X}=1}^{\mathrm{M}} \sum_{\mathrm{Y}=1}^{\mathrm{N}} \sum_{\mathrm{Z}=1}^{\mathrm{O}} \mathrm{D_K}(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) \tag{20}$$

$$\mathrm{D_K} = \begin{cases} 1, \text{ if } \mathrm{C_K}(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) \neq \overline{\mathrm{C_K}}(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) \\ 0, \text{ if } \mathrm{C_K}(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) = \overline{\mathrm{C_K}}(\mathrm{X}, \mathrm{Y}, \mathrm{Z}) \end{cases} \tag{21}$$

If the encryption process using the same encryption key generates different biometric images from similar clear images with a one-pixel difference between them, that algorithm is considered very sensitive to the original image. To simulate the values of the two factors, we used two simple templates with a difference of one pixel between them, encrypted with the Paillier encryption algorithm and the BGV, respectively. From the analysis of the parameters presented in Table 2, slightly higher results for the Paillier algorithm compared to the BGV algorithm outline its higher sensitivity to small changes in the initial simple template.

Table 2. NPCR and UACI analysis.

Statistic Metrics Biometric Images	UACI		NPCR	
	Paillier	BGV	Paillier	BGV
User 1 fingerprint	18.6440	17.2521	99.3299	99.2188
User 2 fingerprint	18.5907	17.2605	99.3103	99.2139
User 3 fingerprint	18.5643	17.2349	99.3370	99.1869
User 4 fingerprint	18.6101	17.3028	99.3519	99.2268
User 5 fingerprint	18.4522	17.2659	99.3422	99.2232
User 6 fingerprint	18.6086	17.2127	99.3292	99.2078
User 7 fingerprint	18.5953	17.2337	99.3084	99.2119
User 8 fingerprint	18.5916	17.2462	99.3390	99.2242
User 9 fingerprint	18.6445	17.2448	99.3184	99.2095
User 10 fingerprint	18.5927	17.2209	99.3302	99.1992

Figure 7 conveys information in a graphical form related to the significant difference between the analyzed encryption algorithms determined by minor changes in the initial image structure, the parameters being dispersed widely but also concentrated upon two central set points.

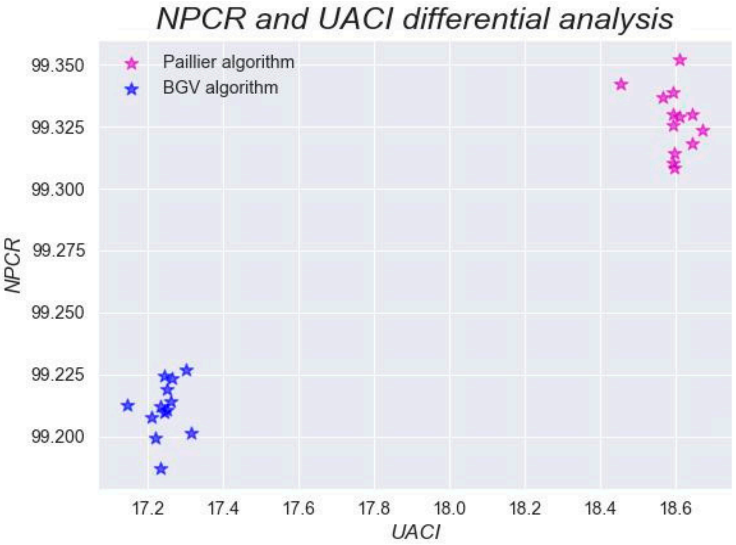


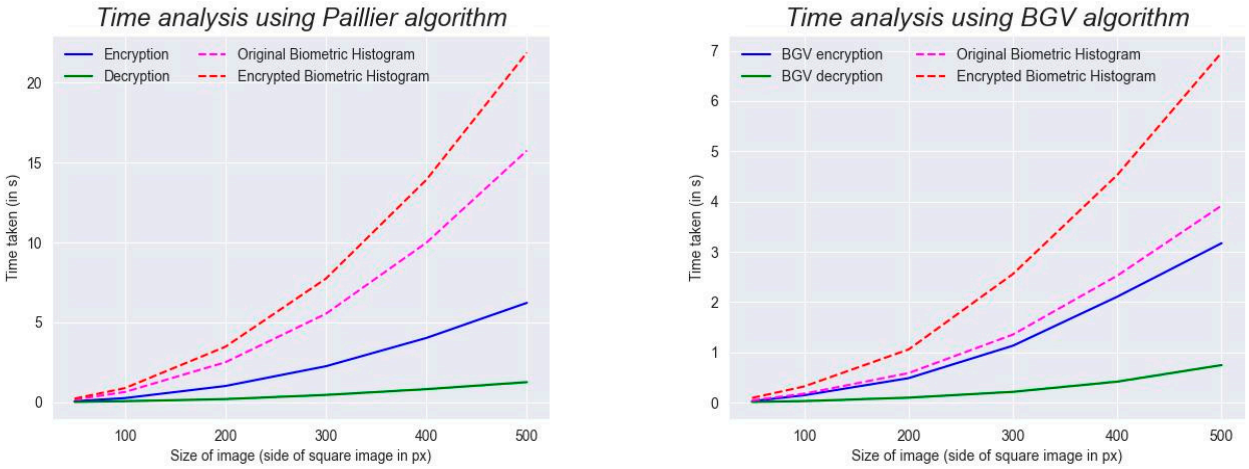
Figure 7. Graphical representation of NPCR and UACI parameters.

3.4. Time and Dimension Analysis

In order to demonstrate the cryptographic algorithm's efficiency as developed in this study, the two most representative factors can be considered the computational time and the dimension of the biometric template, whose values are influenced by the hardware and software characteristics of the system. Not only is the computational time that consists in the period of processing and transformation of the clear text into encrypted text through the use of specific keys important, but also the dimension of the encrypted image is an equally important factor to take into account when evaluating the strength of the cryptographic algorithm, which encompasses the storage size allocated during all the stages involved in the authentication process. An upgraded system involves choosing the appropriate parameters for the implementation of the encryption algorithm, so that the computational time and size for different operations should be minimal [27]. The evaluation of these parameters, which are directly proportional, validates the strength and the speed performance of our algorithm, indicating that this scheme is suitable for real-time applications.

This experiment was realized using the biometric images of the users' fingerprints extracted from the hybrid mechanism of authentication, and the execution time was generated using a Python script with its additional libraries.

Figure 8 displays the detailed time requirements while performing the encryption and decryption processes and also when generating the histograms of the original image and its encrypted version. Analyzing the graphs presented, on the axis of time, it can be observed that the operations of encryption and decryption of the biometric image, but also its histogram executed by means of the BGV algorithm, are much faster compared to the Paillier algorithm, because BGV spends up to 3 s for image encryption and 1 s for image decryption, while Paillier is more time-consuming and takes more than 6 s for image encryption and 2 s for image decryption. When speaking about the dimension of the encrypted templates, the situation is similar, because in the case of the BGV algorithm, the dimension approaches 70 Mb, while in the case of Paillier, the value approaches 75 Mb, as plotted in Figure 9.



(**a**) (**b**)

Figure 8. Time factor analysis using different homomorphic cryptographic algorithms: (**a**) Paillier encryption algorithm, (**b**) BGV encryption algorithm.

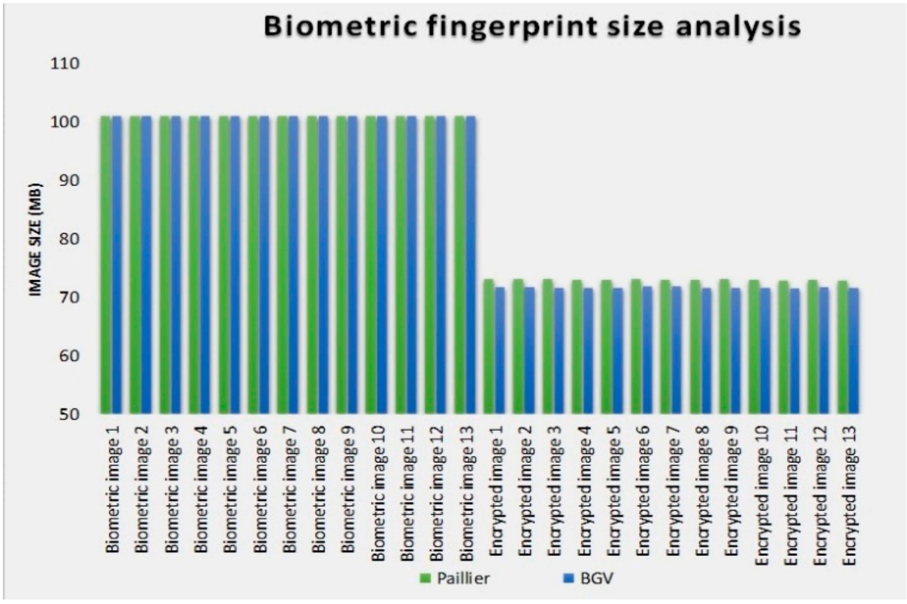


Figure 9. Biometric fingerprint size analysis.

These results highlight the fact that the BGV algorithm takes less computational time and has a smaller encrypted size than the other algorithm, which means it is better and more convenient in the process of encryption, increases the performance and level of security, and also proves its resistance against the various vectors of attacks.

Although some of the homomorphic algorithms are mainly used for theoretical purposes and are regarded with reluctance when implemented in diverse operations due to memory and time usage, we demonstrated the practicality of these algorithms and their capabilities when performing user authentication. A few research studies analyzed the efficacy of these algorithms by their applicability in different scenarios, such as cloud computing, big data, IoT, and healthcare systems, as evidenced in [28–31], but in this paper, we propose a new approach related to the development, execution, and assessment of the homomorphic encryption algorithms on a new type of hybrid mechanism of authentication, specially created for IT systems with high-security requirements.

As a result, these homomorphic algorithms provide a secure framework for practical application and ensure the protection of personal data according to the security rules of European regulations, such as the GDPR (General Data Protection Regulation), which draw clear guidelines with respect to the protection and dissemination of personal information.

Future research should focus not only on optimizing the computation parameters and reducing the noise level after applying additive and multiplicative operations to the encrypted data but also on the study and deepening of other specific factors in image processing for qualitative and quantitative image assessment.

4. Conclusions

This paper presents a comparative assessment of two different homomorphic encryption algorithms applied to images extracted from a novel hybrid mechanism of authentication that combines biometric fingerprint recognition with RFID card authentication. The comparisons and the results obtained show the performance and superiority of the BGV homomorphic algorithm, which is a more productive scheme in terms of security and privacy when it is implemented in data storage. The mechanism of authentication used for experiments was created to improve the overall security and accuracy of the user authentication process and to ensure the confidentiality, integrity, and availability of user credentials during real-time network authentication. Also, the device can be easily customized for different organizational needs and has high potential in various applications in embedded systems, especially in sensitive applications that have to face strict security requirements broken down into several levels of classification and requirements of strong authentication.

Experimental results based on biometric data suggest that fully homomorphic encryption meets the initial expectations and may be a viable practical solution and a reference point for accurate fingerprint matching and RFID authentication in the encrypted domain. It can also help prevent information leakage, maintain the privacy of users, and improve the level of security against unauthorized access.

Author Contributions: Conceptualization, G.C. and M.C.; methodology, G.C. and L.D.; software, G.C.; validation, G.C.; formal analysis, G.C.; investigation, G.C. and M.C.; resources, G.C.; data curation, G.C.; writing—original draft preparation, G.C. and M.C.; writing—review and editing, G.C. and M.C.; visualization, G.C.; supervision, L.D.; project administration, L.D. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The authors confirm that the data supporting the findings of this study are available within the article.

Acknowledgments: The results of this work have been presented to the 11th edition of the Scientific Conference organized by the Doctoral Schools of "Dunărea de Jos" University of Galati (https://cssd-udjg.ugal.ro/index.php/en/)(accessed on 15 June 2023, which was held on 8–9 June 2023 in Galati, Romania.

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

References

1. Lyastani, S.G.; Backes, M.; Bugiel, S. A Systematic Study of the Consistency of Two-Factor Authentication, 17 October 2022. Available online: http://arxiv.org/abs/2210.09373 (accessed on 10 May 2023).
2. Crihan, G.; Craciun, M.; Dumitriu, L. Hybrid methods of authentication in network security. *Ann. "Dunarea De Jos" Univ. Galati. Fascicle III Electrotech. Electron. Autom. Control Inform.* **2023**, *45*, 7. [CrossRef]
3. Acar, A.; Aksu, H.; Uluagac, A.C.; Conti, M. A survey on homomorphic encryption schemes: Theory and implementation. *ACM Comput. Surv.* **2019**, *51*, 79. [CrossRef]
4. Blanton, M.; Gasti, P. Secure and efficient protocols for iris and fingerprint identification. In Proceedings of the Computer Security–ESORICS 2011: 16th European Symposium on Research in Computer Security, Leuven, Belgium, 12–14 September 2011; pp. 190–209.
5. Rana, S.; Jadhav, O.; Rajput, S.; Bhansali, P.; Jyotinagar, V. Homomorphic image encryption. *Int. Res. J. Eng. Technol. (IRJET)* **2019**, *6*, 3934–3940.
6. Mahesh Kumar, M.; Prasad, M.V.; Raju, U.S.N. BMIAE: Blockchain-based multi-instance iris authentication using additive ElGamal homomorphic encryption. *IET Biom.* **2020**, *9*, 165–177. [CrossRef]
7. Noor, N.S.; Hammood, D.A.; Al-Naji, A.; Chahl, J. A fast text-to-image encryption-decryption algorithm for secure network communication. *Computers* **2022**, *11*, 39. [CrossRef]
8. Naït-Ali, A.; Fournier, R. *Signal and Image Processing for Biometrics*; Digital Signal and Image Processing Series; ISTE Ltd.: London, UK; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2012; pp. 263–279.
9. Boddeti, V.N. Secure Face Matching Using Fully Homomorphic Encryption Algorithm, 13 July 2018. Available online: http://arxiv.org/abs/1805.00577, (accessed on 28 March 2023).
10. Morampudi, M.K.; Prasad, M.V.; Verma, M.; Raju, U.S.N. Secure and verifiable iris authentication system using fully homomorphic encryption. *Comput. Electr. Eng.* **2021**, *89*, 106924. [CrossRef]
11. Thabit, F.; Can, O.; Alhomdy, S.; Al-Gaphari, G.H.; Jagtap, S. A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing. *Int. J. Intell. Netw.* **2022**, *3*, 16–30. [CrossRef]
12. Malik, H.; Tahir, S.; Tahir, H.; Ihtasham, M.; Khan, F. A homomorphic approach for security and privacy preservation of Smart Airports. *Future Gener. Comput. Syst.* **2023**, *141*, 500–513. [CrossRef]
13. Morampudi, M.K.; Sandhya, M.; Dileep, M. Privacy-preserving and verifiable multi-instance iris remote authentication using public auditor. *Optik* **2023**, *274*, 170515. [CrossRef]
14. Bassit, A.; Hahn, F.; Veldhuis, R.; Peter, A. Hybrid biometric template protection: Resolving the agony of choice between bloom filters and homomorphic encryption. *IET Biom.* **2022**, *11*, 430–444. [CrossRef]
15. Rahulamathavan, Y. Privacy-Preserving Similarity Calculation of Speaker Features Using Fully Homomorphic Encryption, 14 March 2022. Available online: http://arxiv.org/abs/2202.07994 (accessed on 28 March 2023).

16. Crihan, G.; Crăciun, M.; Dumitriu, L. An efficient hybrid authentication mechanism based on biometric fingerprint recognition and homomorphic encryption. International Journal of Modeling and Optimization (accepted). In Proceedings of the International Conference on Artificial Inteligence applied in the field of Space Lauching Systems, Aerospace, Robotics, Manufacturing Systems, Mechanical Engineering, Power Energy, Technology of Materials and Neurorehabilitation, SLS&OPTIROB, Jupiter, Romania, 30 June 2023.
17. Regueiro, C.; Seco, I.; De Diego, S.; Lage, O.; Etxebarria, L. Privacy-enhancing distributed protocol for data aggregation based on blockchain and homomorphic encryption. *Inf. Process. Manag.* **2021**, *58*, 102745. [CrossRef]
18. Huang, J.; Wu, D. Cloud storage model based on the BGV Fully Homomorphic encryption in the blockchain environment. *Secur. Commun. Netw.* **2022**, *2022*, 8541313. [CrossRef]
19. Weir, B. Homomorphic Encryption. Master's Thesis, University of Waterloo, Waterloo, ON, Canada, 2013.
20. Albrecht, M.; Chase, M.; Chen, H.; Ding, J.; Goldwasser, S.; Gorbunov, S.; Halevi, S.; Hoffstein, J.; Laine, K.; Lauter, K.; et al. Homomorphic Encryption Standard. In *Protecting Privacy through Homomorphic Encryption*; Springer International Publishing: Berlin/Heidelberg, Germany, 2021; pp. 31–62.
21. Crawford, J.L.H. Fully Homomorphic Encryption Applications: The Strive towards Practicality. Department of Electronic Engineering and Computer Science Queen Mary, University of London, London, UK, January 2019.
22. Wang, Z.; Bovik, A.C.; Sheikh, H.; Simoncelli, E.P. Image quality assessment: From error measurement to structural similarity. *IEEE Trans. Image Process.* **2004**, *13*, 600–613. [CrossRef] [PubMed]
23. Bakurov, I.; Buzzelli, M.; Schettini, R.; Castelli, M.; Vanneschi, L. Structural similarity index (SSIM) revisited: A data-driven approach. *Expert Syst. Appl.* **2022**, *189*, 116087. [CrossRef]
24. Nilsson, J.; Akenine-Möller, T. Understanding SSIM, 29 June 2020. Available online: http://arxiv.org/abs/2006.13846 (accessed on 13 July 2023).
25. Nalini, M.K.; Radhika, K.R. Encryption on multimodal biometric using hyper chaotic method and inherent binding technique. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 630–642.
26. Annadurai, S.; Manoj, R.; Jathanna, R.D. A novel self-transforming image encryption algorithm using intrinsically mutating PRNG. In Proceedings of the 1st International Conference on Smart System, Innovations and Computing, Jaipur, India, 15–16 April 2018; Springer: Singapore; Volume 79, pp. 203–214.
27. Kim, M.; Harmanci, A.O.; Bossuat, J.-P.; Carpov, S.; Cheon, J.H.; Chillotti, I.; Cho, W.; Froelicher, D.; Gama, N.; Troncoso-Pastoriza, J.; et al. Ultrafast homomorphic encryption models enable secure outsourcing of genotype imputation. *Cell Syst.* **2021**, *12*, 1108–1120. [CrossRef] [PubMed]
28. Zhang, Q.; Yang, L.T.; Castiglione, A.; Chen, Z.; Li, P. Secure weighted possibilistic c-means algorithm on cloud for clustering big data. *Inf. Sci.* **2019**, *479*, 515–525. [CrossRef]
29. Liu, Y.; Luo, Y.; Zhu, Y.; Liu, Y.; Li, X. Secure multi-label data classification in cloud by additionally homomorphic encryption. *Inf. Sci.* **2018**, *468*, 89–102. [CrossRef]
30. Trivedi, H.S.; Patel, S.J. Homomorphic cryptosystem-based secure data processing model for edge-assisted IoT healthcare systems. *IoT* **2023**, *22*, 100693. [CrossRef]
31. Zaraket, C.; Hariss, K.; Chamoun, M.; Nicolas, T. Cloud based private data analytic using secure computation over encrypted data. *J. King Saud Univ. Comput. Inf. Sci.* **2022**, *34*, 4931–4942. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.