applied sciences

MDPI

Article

Preliminary Experiments of a Real-World Authentication Mechanism Based on Facial Recognition and Fully Homomorphic Encryption

Georgiana Crihan *, Luminița Dumitriu and Marian Viorel Crăciun

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

Abstract: In the current context in which user authentication is the first line of defense against emerging attacks and can be considered a defining element of any security infrastructure, the need to adopt alternative, non-invasive, contactless, and scalable authentication mechanisms is mandatory. This paper presents initial research on the design, implementation, and evaluation of a multi-factor authentication mechanism that combines facial recognition with a fully homomorphic encryption algorithm. The goal is to minimize the risk of unauthorized access and uphold user confidentiality and integrity. The proposed device is implemented on the latest version of the Raspberry Pi and Arduino ESP 32 modules, which are wirelessly connected to the computer system. Additionally, a comprehensive evaluation, utilizing various statistical parameters, demonstrates the performance, the limitations of the encryption algorithms proposed to secure the biometric database, and also the security implications over the system resources. The research results illustrate that the Brakerski–Gentry–Vaikuntanathan algorithm can achieve higher performance and efficiency when compared to the Brakerski–Fan–Vercauteren algorithm, and proved to be the best alternative for the designed mechanism because it effectively enhances the level of security in computer systems, showing promise for deployment and seamless integration into real-world scenarios of network architectures.

Keywords: biometric authentication; fully homomorphic encryption; facial features; Raspberry Pi; Arduino modules; information security

Citation: Crihan, G.; Dumitriu, L.; Crăciun, M.V. Preliminary Experiments of a Real-World Authentication Mechanism Based on Facial Recognition and Fully Homomorphic Encryption. *Appl. Sci.* **2024**, *14*, 718. https://doi.org/10.3390/app14020718

Academic Editor: Nuno Silva

Received: 17 December 2023
Revised: 11 January 2024
Accepted: 12 January 2024
Published: 15 January 2024

1. Introduction

The continuous development of cybersecurity threats in real-world systems has raised serious concerns regarding the maintenance of personal information confidentiality because it can be exploited in both positive and negative manners determined by the purposes and how they are anticipated, as specified in [1], and can produce overwhelming effects. In this context, in which the presentation attacks, spoofing attacks, and Denial-of-Service (DoS) attacks acquire new valences, that are undetectable, difficult to neutralize, and are becoming increasingly virulent against biometric information, a resounding and relevant incident is Biostar Suprema 2, which occurred in 2019 and consisted of large amounts of biometric data used for authentication, such as over a million fingerprints and facial patterns that had been leaked and revealed online, and created a serious threat to various organizations' infrastructure security. The affected database platform belongs to the Korean company Suprema and the main cause of this information leakage was the lack of implementation of efficient data encryption methods to safeguard sensitive information.

Another representative example of a biometric data breach that compromised data traveler facial information occurred in 2019 at the U.S. Customs and Border Protection, where a subcontractor called Perceptics, responsible for protecting sensitive data, stole the facial database and placed it on the dark web using its servers, which subsequently

experienced a malicious ransom-ware attack. Obviously, this situation had a negative impact on the government information system security level, including damage to public perception of the government's use of biometric data as mentioned in [2].

As a direct consequence of recent incidents, there is growing interest in developing reliable, versatile, and scalable authentication mechanisms to provide stricter control on all levels of the security chain and improve authentication capabilities in network architecture and standalone systems. One of the best solutions, which can be adopted to mitigate these threats and defend against unauthorized access, is the complementary association and implementation of two or more factors of authentication, based on "something you are", "something you have", or "something you know" [3].

To accomplish the goal of improving authentication systems, an innovative and optimized technical solution for authentication is designed and proposed in this paper, by interconnecting the biometric component ("something you are") and the cryptographic component ("something you have"), two promising factors that play a pivotal role in securing information in contemporary access control systems. According to [4], the general technical requirements for digital identity proofing and enrollment are described and classified into three main identity assurance levels to validate user genuineness and accuracy; the present mechanism of authentication, which comprises biometric factors and cryptographic algorithms, corresponds to Identity Assurance Level 3, which imposes the strongest conditions for authentication.

The main reason for choosing the implementation of the biometric component arises from the fact that real-time facial detection and recognition represent an active area of research, a complex, contactless, and non-intrusive factor for identification and authentication, based on the unique physical characteristics of the individual, which minimizes the risk of someone else using an unauthorized identity and also provides the accuracy and efficiency of the identity process. Despite its several drawbacks, which have been presented in the literature as described in [5,6], face detection is a mature and reliable technique, with great potential for development if it is associated with the right technology, such as liveness detection, thermal recognition, 3D-three-dimensional shape and infrared technology, machine learning, deep learning, block-chain, or cryptographic algorithms that can be integrated into real-world scenarios of network architecture and seriously enhance the level of security of a system.

Therefore, the security of the authentication mechanism is improved by using an additional authentication factor represented by a fully homomorphic cryptographic algorithm, an outstanding and cutting-edge technology with a strong foundation that relies on public and private keys and allows computation over encrypted data without revealing sensitive data and without degrading the accuracy of the processed information. The objective of this factor is to encrypt the facial biometric database stored on the external device, with the purpose of ensuring user privacy according to the principles of processing personal data imposed by the European Union General Data Protection Regulation (GDPR) [7], California Consumer Privacy Act (CCPA), and Health Insurance Portability and Accountability Act (HIPAA), which strictly stipulates special cases and purposes when biometric data can be processed or any other available regulation or standard designated for information security.

The present article focuses on research contributions that are developed in two main directions as follows:

1. Propose a novel, non-invasive, and two-structural-layered research model of user authentication that combines facial biometric features and cryptographic encryption, a technical solution based on Raspberry Pi and Arduino modules, that outperforms traditional approaches dedicated to controlling access to extremely sensitive areas and services (especially in the military field), where the number of those who have access to them and should use this system is limited.
2. Provide a detailed quantitative and qualitative analysis between two fully homomorphic encryption algorithms, namely the Brakerski–Fan–Vercauteren (BFV) and Brakerski–Gentry–Vaikuntanathan (BGV) algorithms tested on a real biometric fa-

cial database to identify the best alternative for improving storage security and recognition accuracy.

This study makes some noteworthy contributions to the existing literature because it focuses on the development of an innovative facial authentication mechanism dedicated to systems with a certain level of protection, providing a cost-effective and efficient alternative to existing mechanisms that are integrated with an emerging type of encryption algorithm, which revolutionizes and changes the traditional encryption process. This technical solution allows flexibility and customization at the configuration level. In addition, the research includes performance evaluations, comparing encryption algorithms, and highlighting the potential capabilities and limitations of homomorphic encryption over biometric facial information. As a result, this study proposes a new approach and preliminary experiments on a real-world mechanism of authentication that distinguishes it from existing published materials in this research area.

The work is structured as follows: in the Introduction, a brief description of the state-of-the-art review is realized; Section 2 provides a detailed background regarding the existing cryptographic algorithms used to secure biometric information in literature; Section 3 describes the architecture of the proposed mechanism used for experimentation and its mode of operation; Section 4 presents a comprehensive evaluation based on several statistical parameters to demonstrate the efficiency and the reliability of the proposed device and comprises a series of possible scenarios of implementation. Finally, Section 5 concludes the paper and summarizes the main benefits of implementing this solution.

2. Related Work

The association and implementation of biometric recognition and different cryptographic algorithms have been broadly used in a wide spectrum of activities in various fields, but still represent a challenging task for researchers because of the continuous development of the technical elements and measures that underpin these technologies.

It is worth pointing out that the combination of these two niche factors significantly improves the authentication capabilities of a system compared to traditional methods such as passwords and tokens, especially in standalone systems or dedicated networks with high-security requirements to defend against unauthorized disclosure or access and mitigate the risk of leaking information.

2.1. Biometric Authentication

Among the best approaches proposed to strengthen the user authentication process are biometric methods based on unique patterns such as physiological and behavioral traits that have demonstrated a very tangible positive effect on ensuring account security in various fields of activity.

Recognition that uses physiological traits such as fingerprints [8,9], face [10–12], iris [13,14], ear [15,16], veins [17,18], heartbeat [19], electroencephalography (EEG) [20], palm geometry [21], and odor [22] is widely studied and implemented in different types of privacy-preserving information schemes used in real-world applications for cyber security, radio networks, cloud computing, Internet of things, etc. The main advantage of biometrics based on the user's physiological characteristics is that acquiring the authentication data is a non-invasive process, and many parts of the body show a high degree of stability throughout an individual's life.

In contrast to biometric physiological traits that comprise physical characteristics to verify an individual's identity, behavioral traits consist of checking the behavioral characteristics of a person displayed during interaction with a device to confirm their identity. These unique patterns include signature recognition [23], gait recognition [24], voice recognition [25,26], and keystroke movement [27], which can be successfully used for identification and authentication.

An alternative to single-factor authentication based on biometric information is represented by multimodal biometric authentication systems that combine different biometric

traits. Several multimodal biometric schemes of authentication were developed to increase the level of protection for the access control mechanisms as presented in [28–32].

Despite the advantages of biometrics and its various combinations, these are not considered secure enough to authenticate users with a high enough degree of confidence, so researchers have studied and developed diverse biometric template protection schemes, which include biometric cryptosystems, cancellable biometrics, and homomorphic encryption.

2.2. Homomorphic Encryption Approaches

To overcome the limitations of traditional schemes of encryption and introduce an alternative to the aforementioned approaches, such as biometric cryptosystems and cancellable biometrics, homomorphic encryption algorithms represent a promising option for protecting biometric templates through encryption while allowing computations directly on encrypted data without the need for decryption for highly accurate identity verification.

Comprehensive research and detailed analysis regarding the state-of-the-art homomorphic encryption (HE) algorithms in the context of biometrics were provided in [33], such as the evolution of HE algorithms, possible attacks that can be initiated against HE on biometrics, various HE-based approaches to the security of the main biometric user features: iris, face, voice, fingerprint, and also focused on the presentation of the main benefits of integrating HE with other technologies for biometric security.

Several research papers in the specialized literature have used homomorphic encryption for template protection in biometric recognition systems. Initially, the application of Partially Homomorphic Encryption (PHE) and Somewhat Homomorphic Encryption (SWHE) for enhancing security for biometric traits was investigated in [34–38]. These schemes allow performing a limited type of arithmetic operations such as addition and multiplication in the encryption process. Moreover, in [39], an authentication scheme that combines three components is designed: classic user authentication (based on username, password, and a message with a code using short message service (SMS)), biometric authentication, and a searchable encryption scheme that uses the Rivest–Shamir–Adleman (RSA) cryptosystem. In [40], an encoding method that incorporates the Paillier homomorphic algorithm into the inner product protocol applied on the FaceNet dataset achieved 98.78% recognition accuracy. Fully Homomorphic Encryption (FHE) was introduced because these systems proved to be vulnerable to quantum attacks.

FHE systems based on integers and polynomial rings support an unlimited number of addition and multiplication operations in the encrypted domain over the facial biometric templates. In the surveyed literature, different and relevant approaches are given as follows. In [41], a privacy-preserving face verification scheme based on fully homomorphic encryption and a garbled circuit is proposed. In [42], a hybrid scheme for the protection of biometric templates, which combines cancellable biometrics methods and homomorphic encryption using different state-of-the-art face recognition models (ArcFace, ElasticFace, and FaceNet) is developed. Moreover, in [43], an efficient and improved use of coefficient packing for homomorphically protected biometric templates tested on public datasets is presented. Other secure and privacy-preserving methods for biometric template protection using fully homomorphic encryption evaluated on public datasets, that proved to be computationally efficient and practically feasible with no loss in recognition accuracy, are described in [44–47].

Table 1 presents a comparison of the proposed mechanism of authentication with other various existing methods of authentication that combine different biometric templates with encryption algorithms presented in the specialized literature.

Table 1. Comparison of the proposed model with existing authentication models.

Authentication Scheme	Element Description	Encryption Time	Distribution	Level of Implementation	Recognition Accuracy
Proposed system	Face/BGV	1 s	Client/Server/ Radio/Surveillance	Hardware	96.80%
Yang et al. [11]	Face dataset/CKKS SEAL	1.712 s	Client/Server/Cloud	Software	96.71%
Morampudi et al. [13]	Iris dataset/BFV	1.1938 s	Client/Server/Cloud	Software	98.12%
Huang and Wang [41]	Face dataset/BFV/garbled circuit	0.53 s	Client/Server/Cloud	Software	N/A
Bodetti [45]	Face dataset/BFV	280.19 ms	Client	Software	96.74%
Drozdowski et al. [46]	Face dataset/BFV Face dataset/CKKS	2.5 ms 7 ms	Client/Server Client/Server	Software Software	95%
Tamiya et al. [48]	Face dataset/BGV	49.5 ms	Client	Software	N/A
Mfungo and Fu [49]	Face/RSA/Paillier/Chaos	1.9870 s	Client	Software	N/A
Pradel and Mitchell [50]	Face dataset/TFHE	456 s	Client/Server	Software	N/A
Jindal et al. [44]	Face/CKKS HEEAN	2.83 ms	Client	Software	96.10%

The major difference between the authentication scheme proposed in this research paper and the other works consists of the implementation level as we can see in Table 1. Our mechanism of authentication is developed at the hardware level, which is considered superior to software implementation in terms of security, and tested on real user faces, compared with the other methods developed and tested on facial datasets available online.

Analyzing the encryption time resulting from the application of the different homomorphic encryption algorithms, it can be seen that this mechanism provides an acceptable time of encryption compared with the other face-recognition schemes, achieving the operational objectives established in the initial phase. Obviously, there are differences, including for the same encryption algorithm generated by the implementation mode and various factors related to the operational environment of simulation.

Taking into account that this mechanism of authentication is designed for closed systems and networks that require a high level of information protection, it can be a suitable choice for both client and server distribution, but also for radio and surveillance networks. Because cloud platforms present a risk of data confidentiality and are dependent especially on an internet connection and centralized infrastructure managed by a third party, they do not represent a reliable distribution option in the present case.

In terms of recognition accuracy, this mechanism of authentication provides a slightly better level of accuracy and direct interaction with human characteristics. The matching tests that are carried out in real environmental conditions are influenced by the appearance of several factors such as the degree of luminosity, brightness, the subject's position, movement, the processing power at the level of system components, and the bandwidth required for communication between components, elements that can impact recognition accuracy, but offer more significant and relevant results compared to the previous proposed facial methods that are based on predefined datasets with fixed background conditions and controlled image acquisition.

In contrast to the biometric and cryptographic methods described above, the originality of this research derives from the preliminary experiments that are performed using the technical solution based on Raspberry Pi 4 and Arduino ESP 32 modules and different FHE algorithms used for encrypting the biometric database that is generated and stored on the external device, designated not only for standalone systems but also for network systems.

3. Materials and Methods

From a technical point of view, the present authentication mechanism used for experimentation comprises two main physical components: a Raspberry Pi 4 Model B system with an 8 GB LPDDR4 SDRAM and 1.5 GHz quad-core processor, interconnected with an Arduino ESP32 microcontroller, powerful tools of the last generation that integrate Wi-Fi and Bluetooth wireless capabilities for connections, as displayed in Figure 1. The Raspberry Pi microprocessor acts as an active hotspot that can be accessed by other devices and establishes a connection with the Arduino ESP 32 development board and the PC via Wi-Fi, which are considered to be Wi-Fi clients.

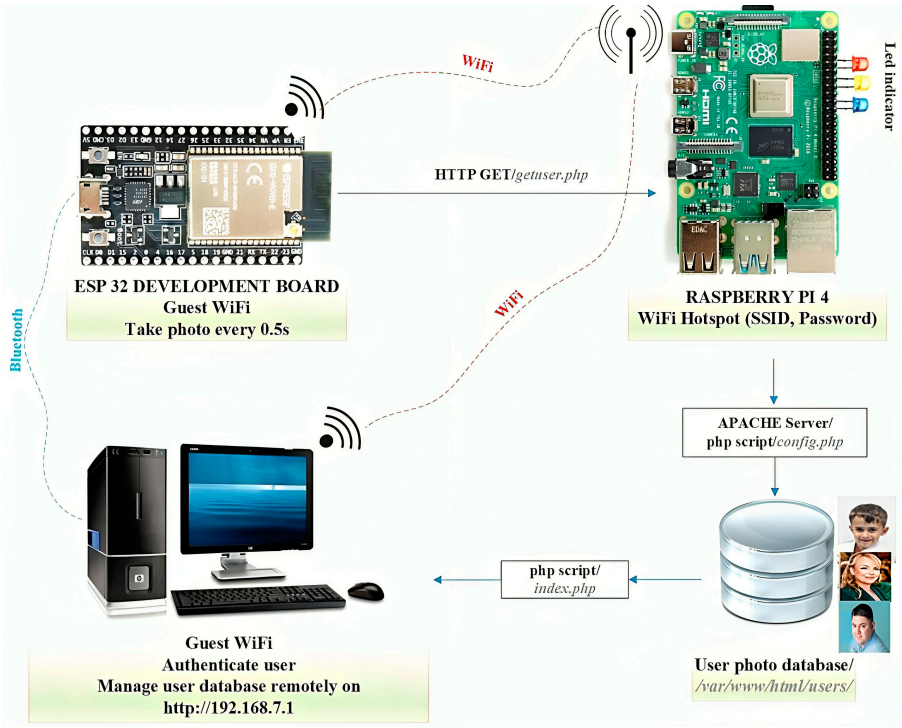

Figure 1. Authentication mechanism architecture based on Raspberry and Arduino modules.

Considering the process description, the proposed authentication mechanism is a complex system that implies several configurations using different software environments, namely:

- The configuration of the Arduino ESP 32 development board with the open-source software Arduino Integrated Development Environment (IDE), version 1.8.19 and its additional libraries
- The COM port is unlocked using the C++ environment in Dev-C++, version 5.11 to realize the connection between the application running on Raspberry Pi and the specified serial port of the PC to read and report the collected data.
- The installation and configuration of the Raspberry Pi 4 with Python software, version 3.10, 64-bit and its standard libraries for image processing OpenCV 4.9.0.80, Face-Recognition 1.3.0 were used for identification and authentication.

More than that, an advanced configuration in the Windows registry key and group policy management is needed to have sufficient rights to execute facial recognition and distinguish individuals based on their physical features. In addition, a secure graphical web interface in PHP and Apache is created for the users' database management, which can be accessed online using a link associated with a static IP address, as shown in Figure 2.

During the authentication process, Raspberry Pi 4 scans the user faces found in the frame and compares them with those in the biometric database; if one face is identified, it provides the login information to ESP32 via Wi-Fi. Raspberry acts as a hotspot and ESP32 as a Wi-Fi client, as presented in the picture above.

This mechanism comprises two main stages. The first stage consists of creating a database with user accounts and their pictures centralized on the external device, whereas the second stage includes the processes of identification, authentication, and authorization of users in the IT system.

The second stage involves scanning users' images using an appropriate sensor included in the Arduino ESP 32 development board, extracting distinctive features, producing feature vectors as biometric templates, and storing them in a database. The decision to accept or reject depends on a comparison between the pictures stored in the

database and the feature vector resulting from the processes of identification, authentication, and authorization.

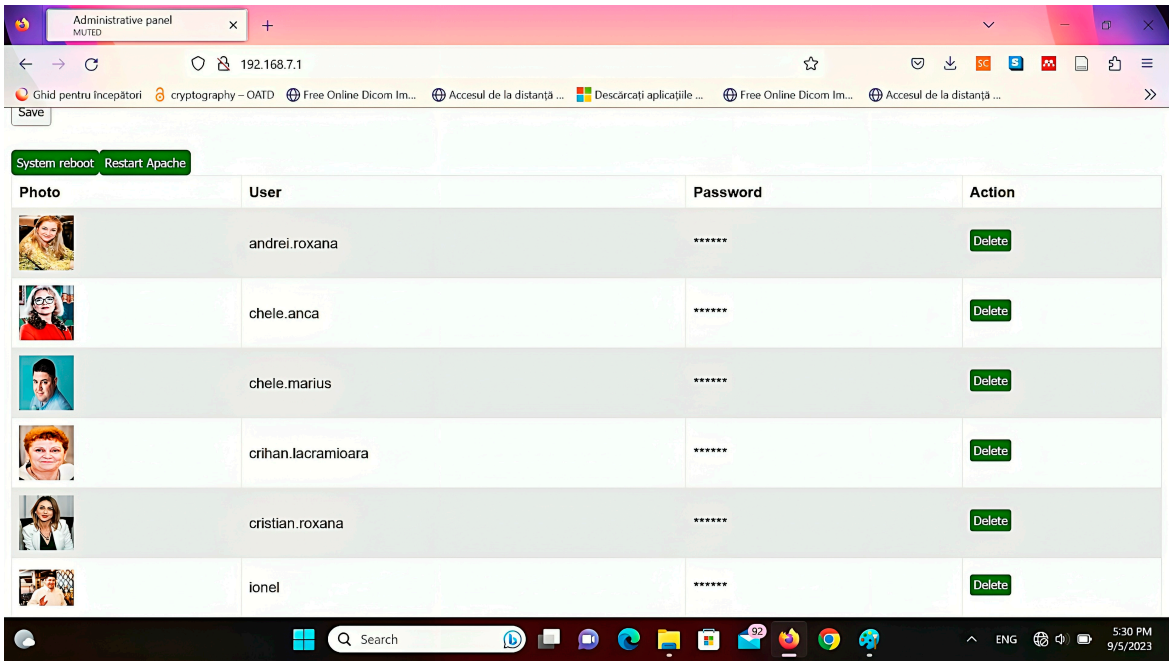

Figure 2. Web interface for users' database administration.

The user's facial database is centralized, stored, and encrypted externally on the Raspberry Pi 4 device and provides remote database management via a web-based console by an administrator or authorized individuals, which is one of the main advantages of this mechanism. The access to the web console is protected by a password established by authorized personnel to execute database management, to enhance the database's level of security. The liveness detection property embedded in the system is another important advantage that considerably improves the accuracy of the detection process and minimizes the possibilities of presentation attacks or replay attacks against this technology.

The complexity of this system derives from using different types of homomorphic cryptographic algorithms including the FHE BFV and BGV algorithms, which are implemented and tested for encrypting the biometric database that contains the users' facial templates, to preserve data confidentiality, integrity, and availability. Among the various methods used for biometric encryption, homomorphic algorithms are considered to be strong and special types of asymmetric encryption, which use both a public key for encryption and a private key for decryption and allow performing different operations over the encrypted information without the need to decrypt it, while the information is in transit, storage, or computation [51]. The data owner has control over the entire information and decides who needs access to the original data, and when and how the template can be used, facts that represent a major advantage in reducing privacy risks and vulnerabilities and preventing the leakage of biometric information.

In the current research, we chose to implement two homomorphic encryption algorithms and test them using several types of statistical parameters because it represents 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. Although significant differences and similarities between the BFV and the BGV algorithms have been highlighted in the literature, at a theoretical level, specifically for ciphertexts, we present an alternative approach for testing fully homomorphic encryption schemes at the implementation level in a real experimentation environment on facial biometric images.

The BFV and BGV fully homomorphic encryption algorithms are structured on the hardness of the Ring Learning with Errors (RLWE) problem composed of polynomial rings, which allows several additive and multiplicative operations over the encrypted data without modifying the content of the resulting ciphertext. The resulting noise after performing the specific operations for each algorithm is considered a crucial aspect of these encryption schemes and expands simultaneously with the number of operations performed as specified by [52]. It increases exponentially during the encryption process and key generation to achieve the hardness properties, but extra noise accumulates substantially during the homomorphic multiplications. For noise management and encryption scheme optimization, bootstrapping, relinearization, and modulus-switching are specific procedures implemented to minimize the noise level and keep it under a certain limit for executing efficient and timely decryption.

Both algorithms have similar capabilities because they support only integer arithmetic operations as specified by [53], and are based on the generation of two types of keys for biometric data encryption: a public key, which is publicly released, and a private decryption key that is kept secret and shares the same plaintext space $\mathcal{R}_t$ for an integer t > 1.

The mathematical description of the considered homomorphic algorithms is given in [54,55], which are characterized by three main operations: key generation, encryption, and decryption. The first phase comprises key generation (secret key, sk; and public key, pk) based on the initial parameters λ and L, where λ represents the security level of the HE scheme, and L is the highest depth of the homomorphic circuits.

The second phase, which consists of text encryption, generates ciphertext (ct) by encrypting plaintext (pt) using public key pk, such that $(pt \in \mathfrak{R}_p, pk) \rightarrow ct$. The plaintext is a ring expressed by $\mathcal{R}_p = Z_P[x]/(x^n + 1)$, while the ciphertexts are considered to be pairs of polynomials in $\mathcal{R}_p = Z_P[x]/(x^n + 1)$.

In the last phase, decryption implies the existence of a ciphertext (ct) that needs to be decrypted, using a private key (sk) from which the original message is obtained: $\text{Decrypt}(ct, sk) \rightarrow pt$. Another important step described by [56] includes the evaluation of the homomorphic circuit that encompasses the development of a supplementary function over the ciphertexts (ct_1, ct_2) without seeing the messages (pt_1, pt_2), which takes ciphertexts as input points from which the evaluated ciphertexts result. The encryption scheme comprises four main operations, namely KeyGen, Encrypt, Decrypt, Evaluate, for circuit C, considering the input parameter t, the encryption key pair (sk, pk) generated via the KeyGen function, the plaintext messages $pt = (pt_1, pt_2 \dots pt_t)$, and the encrypted texts $ct = (ct_1, ct_2 \dots ct_t)$, so that the result can be concretized using the following formulas:

$$ct_i = \text{Encryption}(pk, pt_i) \quad (1)$$

$$\text{Decryption}(sk, \text{Evaluation}(pk, C, ct)) = C(pt_1, pt_2 \dots pt_t) \quad (2)$$

We decided to test these two emerging encryption techniques and appealing solutions for the research community, to evaluate their performance and efficiency for protecting confidential information deployed in potentially dangerous environments where attack vectors are continuously evolving and to overcome the security and privacy issues from real-world applications.

In this study, the optimization of the authentication process is achieved by combining different architectural approaches, implementing an efficient solution to improve existing technologies, overcoming the drawbacks of traditional authentication methods, and bringing innovation in terms of security and resilience. The evaluation performed on the biometric database using several representative statistical parameters specific to image processing has the main objective of minimizing encryption time, increasing encryption speed, and providing a higher level of security.

4. Results and Discussion

The BFV and the BGV cryptographic algorithms' implementation over the facial biometric images were realized in Python 3.10 programming language and its specific

libraries. We used an Intel core i5, 2.4 GHz, 8 GB RAM, and 500 GB SSD running Windows 11 Pro for the experimental environment. The statistical parameters used to identify the best algorithm for the authentication mechanism are applied to several facial biometric images, including a pair of identical male twins, all of which correspond to different users and comprise the histogram analysis, the mean square error (MSE), the 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), and the average encryption time for different image sizes (256×256, 512×512, 1024×1024, and 2048×2048 pixels).

4.1. Histogram Analysis

The first statistical parameter used in the present research is the histogram of the facial biometric image, calculated for 512-pixel images. According to [57], this concept is defined by the distribution of every pixel intensity per grayscale image, estimating the data density and providing a grayscale personalized representation.

When we analyze the histograms displayed in Figure 3, generated for the original biometric image and its encrypted variants using the BFV and the BGV encryption algorithms, in terms of visual effects, we can observe significant differences in pixel intensity dissemination. While the users' original biometric images have a left-skewed distribution or right-skewed distribution which indicates a positive or negative luminous pixel distribution in the image structure, for the encrypted images, characterized by unimodal distribution, it can be seen that stability and uniformity dominate and the values, as well as the shape of the image, are centrally located and have a constant shape with very small differences.

In the histograms below, the X-axis indicates the pixel intensity distribution with the specific range intervals between [0, 255], and the Y-axis displays the frequency of occurrence, which means the degree of data uncertainty and diffusion. It is clear from the graphical representations of the histograms on the Y-axis that higher values are acquired through the BFV algorithm compared to the BGV encryption algorithm, which indicates that it provides an improved level of security, making it impossible to discern the original image through its histogram for the attack vectors. The minimum correlation between the cipher and the original image outlines the performance and effectiveness of the analyzed algorithms.

To resolve a challenging task and to make this study more complete, we recruited a pair of identical male twins for the experimental results to check the ability of the proposed device to distinguish almost identical physical characteristics and verify the accuracy of the authentication process. This hypothesis of effective recognition and authentication on twins is necessary to verify the acceptance error rate in the system because the possibility of errors is maximum due to the inaccuracies generated by feature extraction, matching, or verification.

Figure 3 shows the histograms from a pair of identical male twins. While the histograms of the encrypted images with the BFV algorithm are identical, the histograms generated on encrypted images with the BGV algorithm have almost similar shapes and almost identical values but show a series of differences visible to the naked eye. We can deduce from these results that the BGV algorithm is more suitable for implementation. It generates different histograms even for almost identical people, which is an advantage because it makes it difficult to decipher them in case of a potential attack.

The reliability and accuracy of the proposed device and its automatic facial recognition algorithm were demonstrated while trying to authenticate and distinguish the twins in the system. The experimental results proved the possibility of differentiating the twins in short period of time and with high precision by the biometric sensor.

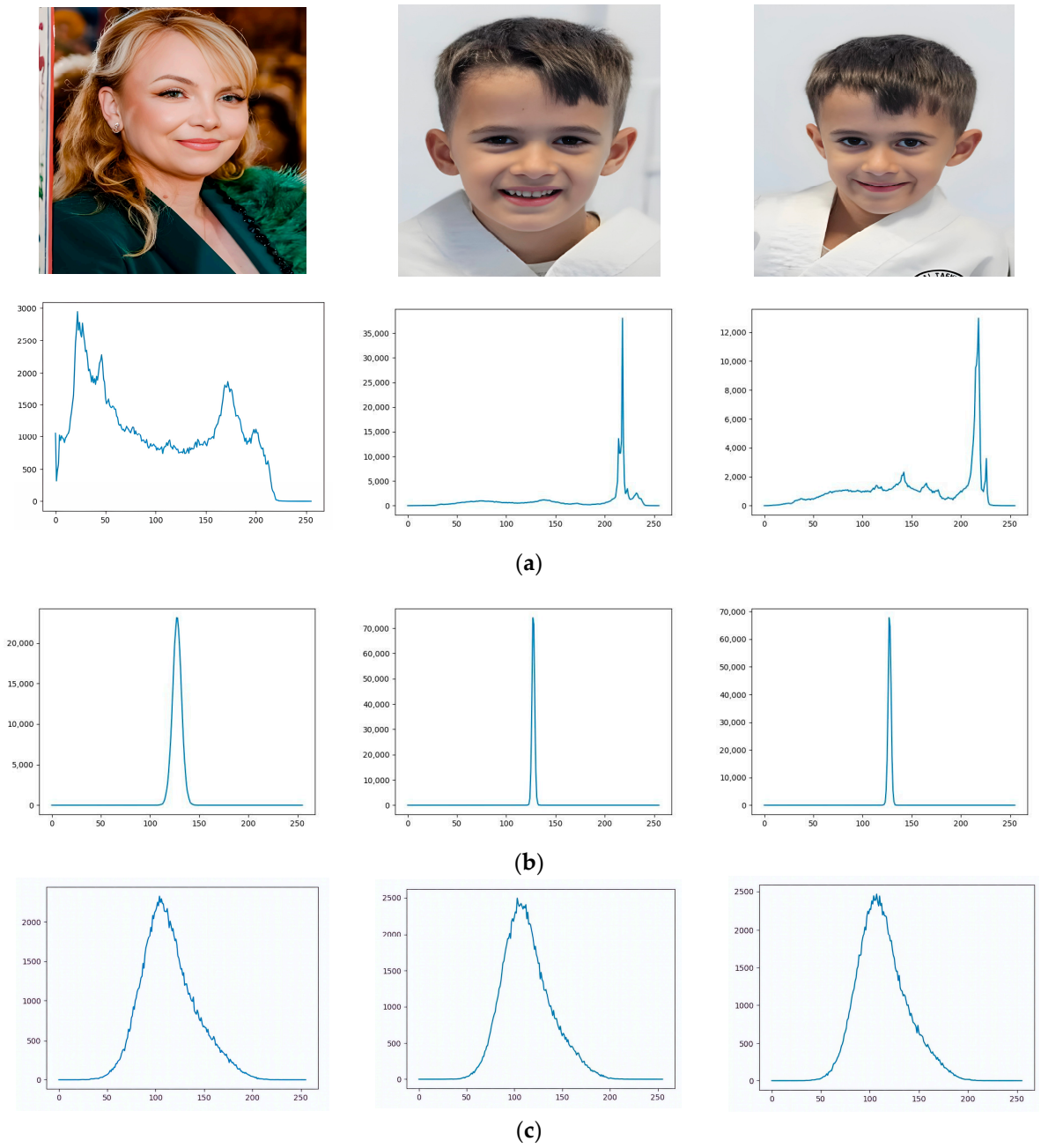

Figure 3. Histogram graphical representation of users 1, 2, and 3. (**a**) Original biometric image. (**b**) Encrypted image using the BFV algorithm. (**c**) Encrypted image using the BGV algorithm.

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

In our analysis, the following parameters implemented for qualitative evaluation, are the mean squared error (MSE) and peak signal-to-noise ratio (PSNR), which are defined by the equations [58]:

$$\mathrm{MSE} = \frac{1}{\mathrm{M} \times \mathrm{N}} \sum_{i=1}^{M} \sum_{j=1}^{N} [\mathrm{M}(i,j) - \mathrm{F}(i,j)]^2 \quad (3)$$

$$\mathrm{PSNR} = 10^{x} \ln(f_{max}/\mathrm{MSE})^2 \quad (4)$$

where M represents the matrix features of the original biometric image, F represents the matrix features related to the encrypted image, m represents the number of rows of pixels of the image, i represents the index of each row, n represents the number of columns of

pixels of the image, j represents the index of each column, and f_{max} is the maximum value of the signal that exists in our original image.

The PSNR is a full reference metric that comprises the noise ratio between the original biometric image and the encrypted image using the homomorphic encryption algorithm. In our current analysis, we are interested in obtaining lower values for the PSNR parameter which indicates a higher level of noise. Consequently, a significant difference identified between the original biometric image and its encrypted version indicates better encryption algorithms, while higher values of PSNR indicate better image quality and accuracy, but not a good encryption algorithm.

In contrast to the PSNR, the MSE is a regression factor that calculates the average squared difference between the pixels of the biometric image and its encrypted version, and lower MSE values approaching 0 indicate better accuracy and a lower level of errors between images, which is a mandatory condition for an efficient algorithm.

Another important parameter used to assess the performance of our proposed algorithms is the structural similarity index measure (SSIM), which measures the structural similarity between the original image and its modified version, capitalizing on three main components derived from the structure of these images: luminance (l), contrast (c), and structure (s). This parameter and its components are mathematically represented by the following equations [59]:

$$\mathrm{SSIM}(x,y) = \left[l(x,y)\right]^{\alpha} \cdot \left[c(x,y)\right]^{\beta} \cdot \left[s(x,y)\right]^{\gamma} \tag{5}$$

$$l(x,y) = \frac{2\mu_x\mu_y + C_1}{{\mu_x}^2 + {\mu_y}^2 + C_1} \tag{6}$$

$$c(x,y) = \frac{2\sigma_x\sigma_y + C_2}{{\sigma_x}^2 + {\sigma_y}^2 + C_2} \tag{7}$$

$$s(x,y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3} \tag{8}$$

where x is the reference image, y is a modified version of the original image, μ calculates the mean intensity of x and y, σ is the standard deviation, α, β, and γ are parameters used to adjust the relative importance of the three components luminance (l), contrast (c), and structure (s), and C_1, C_2, C_3 are numerical stabilizing constants.

As shown in Table 2, no remarkable differences between the resulting values were identified, and the MSE and the PSNR values calculated using the homomorphic encryption algorithms are very tight. The lower PSNR values indicate a higher level of noise and there is a weak correlation between the two types of images, highlighting the encryption performance of the cryptographic algorithms. However, the similarly lower values for the MSE and PSNR obtained when applying the BFV and the BGV algorithms over the biometric images indicate that through the implementation of these schemes, a suitable level of security and efficiency can be achieved.

Table 2. Qualitative parameter analysis.

Statistical Metrics					
MSE		**PSNR**		**SSIM**	
BFV	**BGV**	**BFV**	**BGV**	**BFV**	**BGV**
0.0574	0.0649	27.897	27.896	0.87244	0.87244
0.0532	0.0676	28.141	27.959	0.92221	0.92221
0.0665	0.0755	28.100	27.911	0.91185	0.91185
0.0280	0.0520	27.818	27.962	0.86908	0.86908
0.0443	0.0288	27.726	27.820	0.95722	0.95722
0.0408	0.0549	27.827	27.968	0.91097	0.91097
0.0455	0.0583	27.830	27.978	0.77493	0.77493
0.0615	0.0691	28.056	27.922	0.92674	0.92674
0.0543	0.0684	27.888	27.976	0.91349	0.91349
0.0375	0.0513	27.793	27.891	0.82885	0.82885

Similar behavior to the previously calculated parameters can be observed for the SSIM index values presented in Table 2, where the values calculated for both cryptographic algorithms are slightly different for each image. The obtained results for the SSIM index approaching 1 indicate a high level of resemblance based on the structural features involved in the present analysis and a close relation between the analyzed images and highlight the efficiency and strength of both homomorphic encryption algorithms.

Considering the values obtained during the simulations using the MSE, PSNR, and SSIM parameters, we deduce that both algorithms are suitable for image encryption, and can be integrated into the proposed authentication mechanism to protect the biometric information.

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

Other parameters dedicated to quantitative assessment that validate the strength and robustness of the encryption algorithms against minor changes and resistance to different attacks are the number of pixel change rate (NPCR) and the unified average changing intensity (UACI). These parameters depict the disparity between two encrypted images, after performing encryption operations over the original biometric image and the image that suffers slight adjustment by changing one bit in a pixel, keeping the encryption keys unchanged. If a slight modification in the original biometric image determines a significant difference in its encrypted version, the level of diffusion and confusion will be sufficiently high enough in order to obtain ideal values for these parameters.

According to [60], the NPCR calculates the number of different pixels between two encrypted images, where a percentage of 100% indicates that the images are completely different, while the UACI measures the average percentage of differences in grey levels between the original encrypted image and the encrypted image resulting from the modification of the original image, and both are expressed algebraically by the following equations:

$$\mathrm{UACI} = \frac{1}{\mathrm{M} \times \mathrm{N} \times \mathrm{O}} \sum_{X=1}^{M} \sum_{Y=1}^{N} \sum_{Z=1}^{O} \left[\frac{\mathrm{C_K}(X, Y, Z) - \overline{\mathrm{C_K}}(X, Y, Z))}{255} \right] \tag{9}$$

$$\mathrm{NPCR} = \frac{1}{\mathrm{M} \times \mathrm{N} \times \mathrm{O}} \sum_{X=1}^{M} \sum_{Y=1}^{N} \sum_{Z=1}^{O} \mathrm{D_K}(X, Y, Z) \tag{10}$$

$$\mathrm{D_K} = \begin{cases} 1, \; if \; \mathrm{C_K}(X, Y, Z) \neq \overline{\mathrm{C_K}}(X, Y, Z) \\ 0, if \; \mathrm{C_K}(X, Y, Z) = \overline{\mathrm{C_K}}(X, Y, Z) \end{cases} \tag{11}$$

where $\mathrm{C_K}$ represents the encrypted original biometric image and $\overline{\mathrm{C_K}}$ is the encrypted image that has been slightly adjusted by changing one element in a pixel.

The scores for the UACI parameters presented in Table 3 indicate significant differences between the two algorithms and better results for the BGV encryption algorithm compared to the BFV algorithm. In addition, when considering the values for the BGV cryptographic algorithm, one can observe the stability and uniformity of the generated values, although the analyzed images come from different users and implicitly have different characteristics, whereas the values computed with the BFV cryptographic algorithm are oscillating and uneven.

Table 3. Comparison of NPCR and UACI scores.

Statistical Metrics			
UACI		**NPCR**	
BFV	**BGV**	**BFV**	**BGV**
3.1859	11.9184	96.0777	98.9309
4.5067	11.9885	97.2286	98.9483
3.4986	11.9526	96.4557	98.9465
0.6274	11.9540	79.6688	98.9451
4.4925	11.9864	97.1691	98.9465
2.2003	11.9685	94.1913	98.9576
2.6066	11.9624	95.1431	98.9602
3.2036	11.9662	96.0029	98.9798
1.6305	11.9662	92.2580	98.9549
3.2219	11.9343	96.1250	98.9255

The same situation is not valid for the NPCR parameter; in this case, the generated values are close, presenting an insignificant difference between them, and both algorithms approach the maximum percentage. Thus, we can notice the superiority of the BGV algorithm in the encryption process over biometric images, being more suitable for integration in the proposed multi-factor authentication system because it enhances the strength and security of the users' database.

4.4. Time Analysis

Finally, we focus our attention on the last parameter, probably one of the most relevant elements when we analyze the performance of cryptographic algorithms represented by the computational time that should be minimal for performing privacy-preserving face authentication and encryption in an attempt to achieve the best results and develop a robust and reliable mechanism of authentication. Time plays a crucial role in the entire encryption and decryption process, and a wide variety of external and internal factors related to computer performance such as hardware components, software applications, and cryptographic algorithm structure influence it.

For the current study, we analyzed biometric images from different users, using different dimensions as shown in the graphs presented below. As displayed in Figures 4 and 5, there is a major distinction between the homomorphic encryption algorithms; the BGV algorithm is clearly superior to the BFV algorithm in terms of time encryption for facial biometrics in all image dimensions.

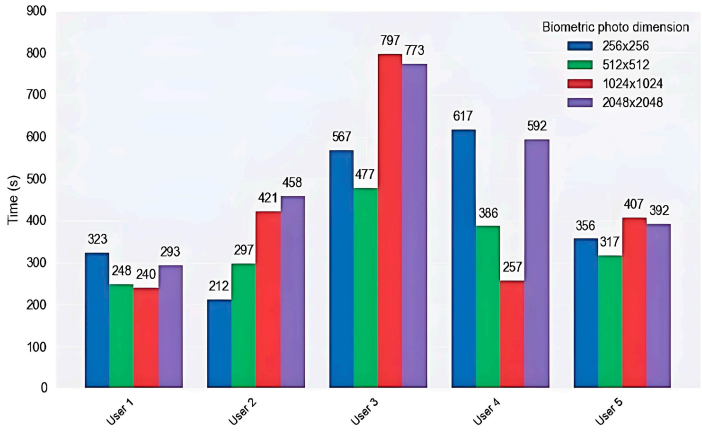

Figure 4. Time factor analysis using BFV encryption algorithm.

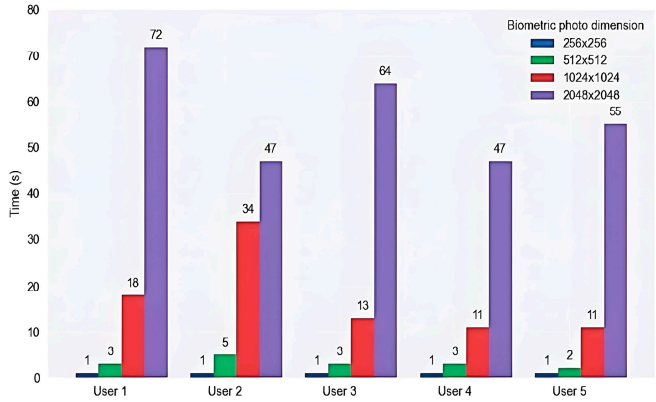

Figure 5. Time factor analysis using BGV encryption algorithm.

Considering the graphs below, it can be emphasized, that the smallest values for time encryption are obtained through the BGV algorithm, which spends up to 1 s for image encryption for the biometric image with 256 pixels that we used for experimentation. However, the highest value for the BGV algorithm is obtained for biometric images with

a size of 2048 pixels, which validates the assertion that time is directly proportional to the increase in image size.

In contrast to the BGV algorithm, the resulting values for the BFV algorithm are distributed over a larger interval of time and indicate that this is a time-consuming alternative that uses important computational resources for realizing image encryption. Also, the results prove that this is not a viable solution to be implemented in real-time applications, because it takes more time than expected for encryption even for the smallest biometric image sizes, and needs significant optimization in order to be applied in practice.

In addition, the values obtained indicate the lack of uniformity of the time factor when encryption is performed with this algorithm, which oscillates in large intervals of time as can be seen in Figure 4, between 212 and 797 s. This is an enormous amount of time, without being able to establish any rule in the encryption process, specifically the rule regarding the direct correlation between time encryption and image dimension which is not valid in this case or to identify a potential factor that generates these noteworthy differences.

The best option for an effective implementation that can reasonably be applied to the proposed authentication mechanism is obviously the BGV algorithm because it requires less computational time for different image sizes than the other algorithm, which means it provides reliability and is more convenient when applied to the encryption process.

Overall, the preliminary experimental results reveal that the BGV fully homomorphic encryption algorithm should be applied to improve the security level in the authentication process because it offers a major advantage in terms of performance and efficiency for the proposed system capabilities designed especially for IT systems with high-security requirements. Considering the tests performed, the optimal operating parameters of this algorithm are for an image of 512 pixels, to ensure a sufficient image accuracy and a suitable encryption time. Despite its potential benefits, we identified a limitation that significantly influences the encryption process related to the performances of the computational resources, so that for an optimized time for the process of information encryption and decryption, it is necessary to provide powerful resources, especially regarding the CPU and system memory.

4.5. Security Vulnerability Assessment

The vulnerable points of the facial mechanism, used in the present research, can be found both at the level of the structural elements and at the level of the authentication process stages, starting from the process of enrollment, verification, and authorization, and including the database information storage and the data transmission channel, as can be seen in Figure 6.

Even though biometric authentication systems represent one of the most secure and robust ways of authentication, their accuracy can be negatively influenced by several intrinsic failures such as position, make-up, illness, lighting conditions, facial expression, aging process, the heterogeneity of which can affect the sensor's ability to capture the data successfully, which implies the risk of rejection of a user enrolled in the system.

The first vulnerable point of the mechanism, exploited by attackers who want to penetrate the system through various techniques and attack tools to manipulate digital facial features, present from the early phase of the authentication process is found at the biometric sensor level. There are well-known attacks such as the presentation attack [61], also known as the spoofing attack which involves various misleading means such as photographic paper, high-resolution photos, video footage, or authentication masks (2D, 3D), the morphing attack [62] which consists of creating artificial facial biometric samples by integrating several faces into a single face, and Deepfake technologies based on artificial intelligence algorithms and deep learning which aim to create fake digital images as persuasive as possible or videos that achieve similarity between two users.

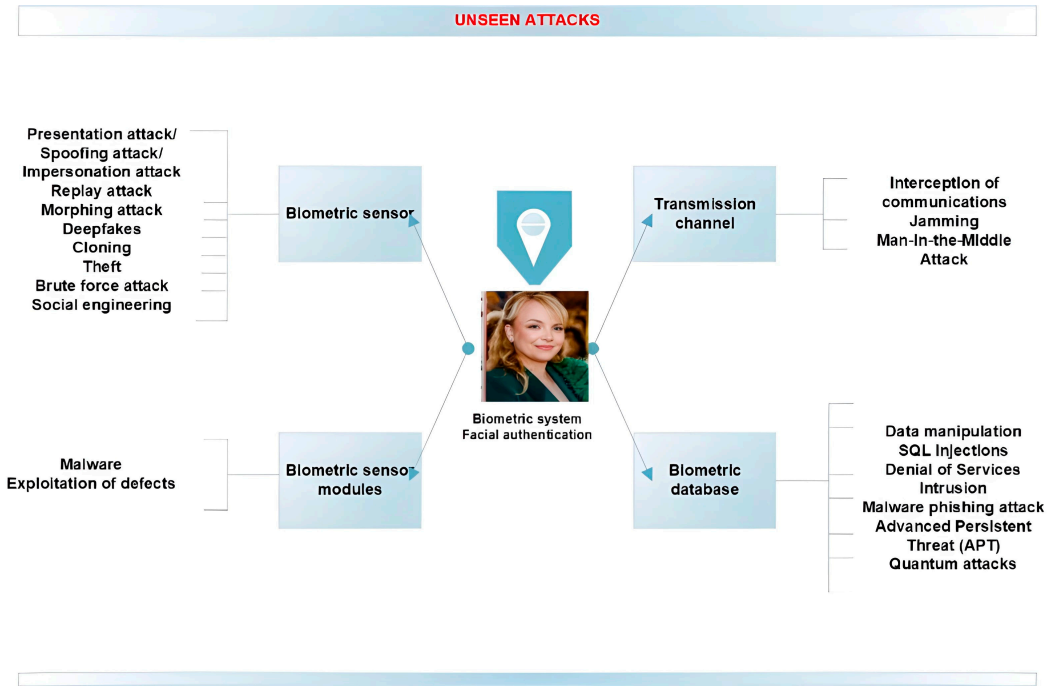

Figure 6. Emerging attacks on the biometric component.

Another vulnerable point of the mechanism is the biometric database, which can be hacked, either by coercion of the system administrator, by completely bypassing the security rings around the database, or by an external attacker who can steal the administrator privileges and the access credentials to directly modify the data stored in the database. Various information can also be injected into the database that can compromise it or alter the biometric templates so that the system can no longer function at optimal parameters.

New attack vulnerabilities can also be identified on the information transmission channel by manipulating the information content, the MAC address (ARP spoofing), or the Wi-Fi signal (honeypots) to impersonate the system users, but also exploiting it through various cyberattacks such as DoS (Denial of Service), malware, phishing, and Advanced Persistent Threat (APT).

An attacker can escalate all of the presented vulnerabilities and perform various attacks to compromise the security of the authentication system, such as accessing private information, obtaining elevated authorization permissions, manipulating access control systems, or accessing unauthorized facilities. As a result, there is an urgent need to implement additional measures to increase the accuracy and performance of facial recognition systems, including the implementation of motion-based features, image quality-based features, adaptive authentication, capitalizing on deep-learning and machine learning algorithms, and developing multimodal systems and cryptographic algorithms.

Making a comparative analysis of these defensive techniques based on cost versus security factors, the techniques that use additional hardware involve additional costs but have a better level of robustness and security compared to software techniques that have lower costs but ensure relatively lower security.

From this perspective, for this research, we selected for implementation the hardware defensive techniques that execute user authentication in different real situations, independently of the host computer to limit the extension of security breaches.

4.6. Scenarios of Implementation

The versatility of the designed authentication mechanism can be illustrated by the various scenarios and the variety of domains where it can be implemented, which involve a high level of information protection and strict requirements for preserving user confidentiality.

A first scenario for the implementation of the proposed authentication mechanism includes the integration of these access protection tools in a single-channel military radio network transmitting data in the HF range as presented in Figure 7. The HF radio subsystem is of particular importance in the military communications infrastructure, as it provides real-time informational support for the various missions in the battlefield that underpin the command and control act, characterized by flexibility, portability, and interoperability. The HF radio stations in the data networks function by allocating radio frequencies in specific working bands and are configured with appropriate cryptographic algorithms to ensure a secure flow of data. Supplementing the safety measures by securing the access of authorized users within the computer system contributes to the efficient management of user identity, so that access to information is ensured only to those who need it, at the right time and in a timely manner.

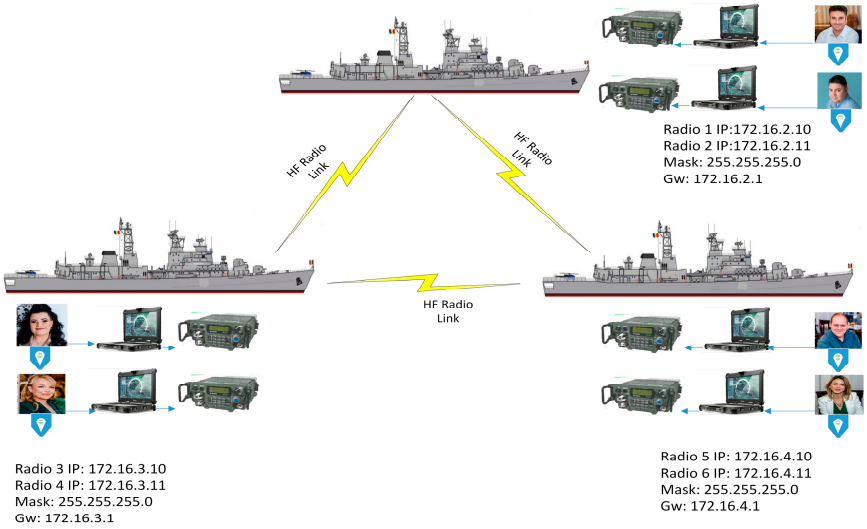

Figure 7. Implementation of authentication mechanism in HF radio data networks.

Another scenario for the implementation of the designed authentication mechanism, represented graphically in Figure 8, consists of incorporating it into the architecture of a contemporary video surveillance system through which real-time monitoring is carried out, a system that represents a key element in reducing existing risks at the organizational level and optimizing the level of security and safety.

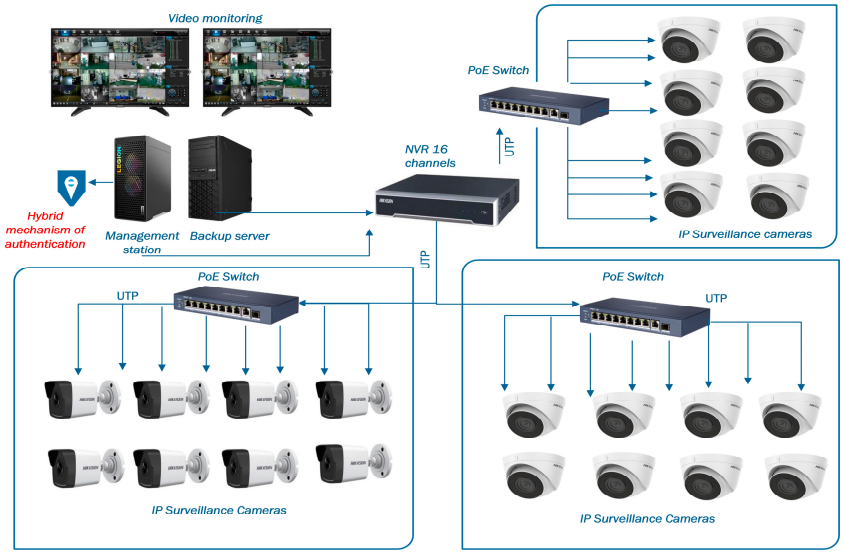

Figure 8. Securing access within a video surveillance system.

5. Conclusions

The emergent development of new technologies in biometrics and cryptography has provided new opportunities for enhancing information security in different types of applications. The objective of this research is to integrate and capitalize on the great potential of these powerful techniques to create a real experimental environment for user authentication and also to control remotely the entire resources involved in the authentication process and protect them against attack vectors.

Therefore, in this study, we succeeded in developing two main directions that were established at the beginning of our work, so we designed a cost-effective technical solution for authentication in different standalone systems and network devices using facial biometrics for detection and recognition combined with fully homomorphic encryption, a relatively complex and compact system based on Raspberry Pi and Arduino modules. These modules offer several advantages, including reasonable acquisition costs, a user-friendly interface, flexibility, and versatility in developing custom solutions. This mechanism can be deployed in different scenarios where the need to ensure user confidentiality is very high. However, it is important to highlight some drawbacks associated with fully homomorphic encryption. One of these drawbacks is the need to ensure powerful computation resources to obtain an optimized time for information encryption and decryption.

The statistical measurements that were carried out, over the biometric facial database using the BFV and the BGV homomorphic encryption algorithms, provided a deeper understanding of biometric encryption status and helped us to identify the best alternative for enhancing storage security and optimizing the system capabilities, thus proving its performance and superiority in improving overall security.

In summary, the novelty of the proposed approach lies in the design of a multi-factor authentication mechanism, a closed system with restricted access based on the system-on-device architecture that performs real-time user authentication and provides a user-friendly web interface for remote administration.

The future development directions to improve the level of security and user accuracy in the authentication process would be the implementation of an additional factor based on iris features, to create a multimodal mechanism, and also the improvement of the facial and iris recognition algorithm structure by using deep learning and convolutional neural network (CNN) algorithms. Finally, the optimization of the encryption algorithm to minimize the noise level and keep it below a certain limit favorable to perform efficient and timely encryption and also to enhance the execution time would be a mandatory direction.

Author Contributions: Conceptualization, L.D. and G.C.; methodology, G.C. and M.V.C.; software, G.C.; validation, G.C.; formal analysis, G.C. and L.D.; investigation, G.C. and M.V.C.; resources, G.C.; data curation, G.C.; writing—original draft preparation, G.C.; writing—review and editing, G.C. and M.V.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.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

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

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

Abbreviations

APT	Advanced Persistent Threat
ARP	Address Resolution Protocol
BFV	Brakerski–Fan–Vercauteren
BGV	Brakerski–Gentry–Vaikuntanathan
CNN	Convolutional Neural Network
CPU	Central Processing Unit
DoS	Denial-of-Service
EEG	Electroencephalography
FHE	Fully Homomorphic Encryption
HE	Homomorphic Encryption
HF	High Frequency
IDE	Integrated Development Environment
MAC	Message Authentication Code
PHE	Partially Homomorphic Encryption
RLWE	Ring Learning with Errors
RSA	Rivest–Shamir–Adleman
SWHE	Somewhat Homomorphic Encryption

References

1. Chang, C.C. Privacy-Preserving Information Hiding and Its Applications. Ph.D. Thesis, University of Warwick, Coventry, UK, 2019.
2. Department of Homeland Security. *Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot*; Department of Homeland Security: Washington, DC, USA, 2020. Available online: https://www.oig.dhs.gov/reports/2020/review-cbps-major-cybersecurity-incident-during-2019-biometric-pilot/oig-20-71-sep20 (accessed on 3 September 2023).
3. Boonkrong, S. *Authentication and Access Control: Practical Cryptography Methods and Tools*; Apress: Berkeley, CA, USA, 2021; pp. 45–69.
4. Temoshok, D. *Digital Identity Guidelines Online, National Institute of Standards and Technology*; NIST SP 800-063-4 IPD; NIST: Gaithersburg, MD, USA, 2022.
5. Alonso-Fernandez, F.; Fierrez, J.; Ortega-Garcia, J. Quality measures in biometric systems. *IEEE Secur. Priv.* **2022**, *10*, 52–62.
6. Yang, J. *New Trends and Developments in Biometrics*; IntechOpen: Rijeka, Croatia, 2012; p. 31.
7. European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Off. J. Eur. Union* **2016**, *L119/1*, 1–209.
8. Yang, W.; Wang, S.; Yu, K.; Kang, J.J.; Johnstone, M.N. Secure fingerprint authentication with homomorphic encryption. In Proceedings of the Digital Image Computing: Techniques and Applications (DICTA), Melbourne, Australia, 29 November–2 December 2020.
9. Murillo-Escobar, M.A.; Cruz-Hernández, C.; Abundiz-Pérez, F.; López-Gutiérrez, R.M. A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Syst. Appl.* **2015**, *42*, 8198–8211. [CrossRef]
10. Zulfiqar, M.; Syed, F.; Khan, M.J.; Khurshid, K. Deep Face Recognition for Biometric Authentication. In Proceedings of the 2019 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Swat, Pakistan, 24–25 July 2019.
11. Yang, Y.; Zhang, Q.; Gao, W.; Fan, C.; Shu, Q.; Yun, H. Design on Face Recognition System with Privacy Preservation Based on Homomorphic Encryption. *Wirel. Pers. Commun.* **2022**, *123*, 3737–3754. [CrossRef]
12. Ali, M.A.S.; Meselhy Eltoukhy, M.; Rajeena, F.P.P.; Gaber, T. Efficient thermal face recognition method using optimized curvelet features for biometric authentication. *PLoS ONE* **2023**, *18*, e0287349. [CrossRef] [PubMed]
13. Morampudi, M.K.; Prasad, M.V.N.K.; Verma, M.; Raju, U.S.N. Secure and verifiable iris authentication system using fully homomorphic encryption. *Comput. Electr. Eng.* **2021**, *89*, 106924. [CrossRef]
14. Khoury, F.E. *Iris Biometric Model for Secured Network Access*; CRC: Boca Raton, FL, USA, 2013.
15. Chowdhury, R.; Ghosh, D.; Agarwal, P.; Kumar, S. Ear based biometric authentication system. *World J. Res. Technol.* **2016**, *2*, 224–233.
16. Annapurani, K.; Sadiq, M.A.K.; Malathy, C. Ear authentication and template protection using bio-key. *Res. J. Appl. Sci. Eng. Technol.* **2014**, *8*, 1450–1455. [CrossRef]
17. Madhusudhan, M.V.; Udayarani, V.; Hegde, C. Finger vein recognition model for biometric authentication using intelligent deep learning. *Int. J. Recent Technol. Eng.* **2020**, *8*, 5403–5408. [CrossRef]
18. Gupta, P.; Srivastava, S.; Gupta, P. An accurate infrared hand geometry and vein pattern based authentication system. *Knowl. Based Syst.* **2016**, *103*, 143–155. [CrossRef]
19. Islam, M.S. Heartbeat biometrics for remote authentication using sensor embedded computing devices. *Int. J. Distrib. Sens. Netw.* **2015**, *11*, 549134. [CrossRef]

20. Jeswani, D.; Govarthan, P.K.; Selvaraj, A.; Thomas, C.B.; Thomas, J.; Ronickom, J.F.A. A feasibility study on using EEG for biometric trait authentication system. *Curr. Dir. Biomed. Eng.* **2023**, *9*, 690–693. [CrossRef]
21. Sharma, S.; Dubey, S.R.; Singh, S.K.; Saxena, R.; Singh, R.K. Identity verification using shape and geometry of human hands. *Expert Syst. Appl.* **2015**, *42*, 821–832. [CrossRef]
22. Rashed, A.; Santos, H. Odour user interface for authentication: Possibility and acceptance: Case study. In Proceedings of the International Multi Conference of Engineers and Computer Scientists, Hong Kong, 17–19 March 2010.
23. Yevetskyi, V.; Horniichuk, I. Selection of handwritten signature dynamic indicators for user authentication. *Inf. Technol. Secur.* **2020**, *8*, 19–30. [CrossRef]
24. Isaac, E.R.H.P.; Elias, S.; Rajagopalan, S.; Easwarakumar, K.S. Template-based gait authentication through Bayesian thresholding. *IEEE/CAA J. Autom. Sin.* **2019**, *6*, 209–219. [CrossRef]
25. Kang, Y.; Kim, W.; Lim, S.; Kim, H.; Seo, H. Deep Detection: Privacy-enhanced deep voice detection and user authentication for preventing voice phishing. *Appl. Sci.* **2022**, *12*, 11109. [CrossRef]
26. Meng, Z.; Altaf, M.U.B.; Juang, B.H. Active voice authentication. *Digit. Signal Process.* **2020**, *101*, 102672. [CrossRef]
27. Neacsu, T.; Poncu, T.; Ruseti, S.; Dascalu, M. DoubleStrokeNet: Bigram-Level keystroke authentication. *Electronics* **2023**, *12*, 4309. [CrossRef]
28. Velmurugan, S.; Selvarajan, S. A multimodal authentication for biometric recognition system using hybrid fusion techniques. *Clust. Comput.* **2019**, *22*, 13429–13436. [CrossRef]
29. Elmir, Y.; Al-Maadeed, S.; Amira, A.; Hassaine, A. Multi-modal biometric authentication system using face and online signature fusion. In Proceedings of the Qatar Foundation Annual Research Forum, Doha, Qatar, 21–23 October 2012.
30. Abozaid, A.; Haggag, A.; Kasban, H.; Eltokhy, M. Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion. *Multimed. Tools Appl.* **2019**, *78*, 16345–16361. [CrossRef]
31. Sujatha, E.; Chilambuchelvan, A. Multimodal biometric authentication algorithm using iris, palm print, face and signature with encoded DWT. *Wirel. Pers. Commun.* **2018**, *99*, 23–34. [CrossRef]
32. Singh, K.K.; Barde, S. A feasible adaptive fuzzy genetic technique for face, fingerprint, and palmprint based multimodal biometrics systems. *J. Curr. Sci. Technol.* **2023**, *14*, 1–15.
33. Yang, W.; Wang, S.; Cui, H.; Tang, Z.; Li, Y. A review of homomorphic encryption for privacy-preserving biometrics. *Sensors* **2023**, *23*, 3566. [CrossRef]
34. Barni, M.; Bianchi, T.; Catalano, D.; Di Raimondo, M.; Labati, R.D.; Failla, P.; Fiore, D.; Piuri, V.; Piva, A.; Scotti, F. A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates. In Proceedings of the 2010 Fourth IEEE International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington, DC, USA, 27–29 September 2010.
35. Upmanyu, M.; Namboodiri, A.M.; Srinathan, K.; Jawahar, C.V. Blind Authentication: A secure crypto-biometric verification protocol. *IEEE Trans. Inf. Forensics Secur.* **2010**, *5*, 255–268. [CrossRef]
36. Qin, Y.; Zhang, B. Privacy-preserving biometrics image encryption and digital signature technique using Arnold and ElGamal. *Appl. Sci.* **2023**, *13*, 8117. [CrossRef]
37. Gomez-Barrero, M.; Maiorana, E.; Galbally, J.; Campisi, P.; Fierrez, J. Multi-biometric template protection based on homomorphic encryption. *Pattern Recognit.* **2017**, *67*, 149–163. [CrossRef]
38. Cheon, J.H.; Chung, H.; Kim, M.; Lee, K.W. Ghostshell: Secure Biometric Authentication Using Integrity-Based Homomorphic Evaluations. Available online: https://eprint.iacr.org/2016/484 (accessed on 15 May 2023).
39. Mihailescu, M.I.; Nita, S.L. A searchable encryption scheme with biometric authentication and authorization for cloud environments. *Cryptography* **2022**, *6*, 8. [CrossRef]
40. Li, X.; Chen, Z.; Gao, J. Ciphertext face recognition system based on secure inner product protocol. *J. Inf. Secur. Appl.* **2024**, *80*, 103681. [CrossRef]
41. Huang, H.; Wang, L. Efficient privacy-preserving face verification scheme. *J. Inf. Secur. Appl.* **2021**, *63*, 103055. [CrossRef]
42. Shahreza, H.O.; Rathgeb, C.; Osorio-Roig, D.; Hahn, V.K.; Krivoku, V.; Marcel, S.; Busch, C. Hybrid protection of biometric templates by combining homomorphic encryption and cancelable biometrics. In Proceedings of the 2022 IEEE International Joint Conference on Biometrics (IJCB), Abu Dhabi, United Arab Emirates, 10–13 October 2022; pp. 1–10.
43. Bauspieß, P.; Olafsson, J.; Kolberg, J.; Drozdowski, P.; Rathgeb, C.; Busch, C. Improved homomorphically encrypted biometric identification using coefficient packing. In Proceedings of the 2022 International Workshop on Biometrics and Forensics (IWBF), Salzburg, Austria, 20–21 April 2022.
44. Jindal, A.K.; Shaik, I.; Vasudha, V.; Chalamala, S.R.; Rajan, M.; Lodha, S. Secure and privacy preserving method for biometric template protection using fully homomorphic encryption. In Proceedings of the IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Guangzhou, China, 29 December 2020–1 January 2021.
45. Boddeti, V.N. Secure Face Matching Using Fully Homomorphic Encryption. 2018. Available online: http://arxiv.org/abs/1805.00577 (accessed on 20 May 2023).
46. Drozdowski, P.; Buchmann, N.; Rathgeb, C.; Margraf, M.; Busch, C. On the application of homomorphic encryption to face identification. In Proceedings of the 2019 International Conference of the Biometrics Special Interest Group (BIOSIG 2019)—Lecture notes in Informatics (LNI), Darmstadt, Germany, 18–20 September 2019.

47. Alsaedi, E.M.; Farhan, A.K. Retrieving encrypted images using Convolution Neural Network and Fully Homomorphic Encryption. *Baghdad Sci. J.* **2023**, *20*, 206–220. [CrossRef]
48. Tamiya, H.; Isshiki, T.; Mori, K.; Obana, S.; Ohki, T. Improved post-quantum-secure face template protection system based on packed homomorphic encryption. In Proceedings of the 2021 International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, 15–17 September 2021.
49. Mfungo, D.E.; Fu, X. Fractal-based hybrid cryptosystem: Enhancing image encryption with RSA, homomorphic encryption, and chaotic maps. *Entropy* **2023**, *25*, 1478. [CrossRef] [PubMed]
50. Pradel, G.; Mitchell, C. Privacy-Preserving Biometric Matching Using Homomorphic Encryption. 2021. Available online: http://arxiv.org/abs/2111.12372 (accessed on 15 September 2023).
51. Macmillan, J. *INFOSEC Strategies and Best Practices: Gain Proficiency in Information Security Using Expert-Level Strategies and Best Practices*; Packt Publishing: Birmingham, UK, 2021.
52. Kim, A.; Polyakov, Y.; Zucca, V. Revisiting homomorphic encryption schemes for finite fields. In *Advances in Cryptology—ASIACRYPT 2021*; Springer International Publishing: Berlin/Heidelberg, Germany, 2021; pp. 608–639.
53. Jiang, L.; Ju, L. FHEBench: Benchmarking Fully Homomorphic Encryption Schemes. 2022. Available online: http://arxiv.org/abs/2203.00728 (accessed on 28 July 2023).
54. Iliashenko, I.; Zucca, V. Faster homomorphic comparison operations for BGV and BFV. *Proc. Priv. Enhancing Technol.* **2021**, *2021*, 246–264. [CrossRef]
55. Introduction to the BGV FHE Scheme, Washington, USA. Available online: https://www.inferati.com/blog/fhe-schemes-bgv (accessed on 30 July 2023).
56. Crihan, G.; Crăciun, M.; Dumitriu, L. A comparative assessment of homomorphic encryption algorithms applied to biometric information. *Inventions* **2023**, *8*, 102. [CrossRef]
57. Deng, W.; Liu, L.; Chen, H.; Bai, X. Infrared image contrast enhancement using adaptive histogram correction framework. *Optik* **2022**, *271*, 170114. [CrossRef]
58. Kumar, A.; Rani, R.; Singh, S. Encoder-Decoder architecture for image steganography using skip connections. *Procedia Comput. Sci.* **2023**, *218*, 1122–1131. [CrossRef]
59. 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]
60. Firdous, A. Symmetric Image Encryption Using Chaos and Hash. Ph.D. Thesis, Islamia University of Bahawalpur, Punjab, Pakistan, 2019.
61. Khairnar, S.; Gite, S.; Kotecha, K.; Thepade, S.D. Face liveness detection using artificial intelligence techniques: A systematic literature review and future directions. *Big Data Cogn. Comput.* **2023**, *7*, 37. [CrossRef]
62. Hamza, M.; Tehsin, S.; Humayun, M.; Almufareh, M.F.; Alfayad, M. A comprehensive review of face morph generation and detection of fraudulent identities. *Appl. Sci.* **2022**, *12*, 12545. [CrossRef]