



Article

A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks

Srđan Barzut ¹, Milan Milosavljević ², Saša Adamović ², Muzafer Saračević ^{3,*} , Nemanja Maček ⁴ 
and Milan Gnjatović ⁵

- ¹ Tehnikum Taurunum Department, Academy of Applied Technical Studies Belgrade, Nade Dimić 4, 11080 Belgrade, Serbia; sbarzut@tehtnikum.edu.rs
- ² Faculty of Informatics and Computing, Singidunum University, Danijelova 32, 11000 Belgrade, Serbia; mmilosavljevic@singidunum.ac.rs (M.M.); sadamovic@singidunum.ac.rs (S.A.)
- ³ Department of Computer Sciences, University of Novi Pazar, Dimitrija Tucovića bb, 36300 Novi Pazar, Serbia
- ⁴ School of Electrical and Computer Engineering, Academy of Technical and Art Applied Studies, Vojvode Stepe 283, 11000 Belgrade, Serbia; nmacek@viser.edu.rs
- ⁵ Department of Information Technology, University of Criminal Investigation and Police Studies, Cara Dušana 196, 11080 Belgrade, Serbia; milan.gnjatovic@kpu.edu.rs
- * Correspondence: muzafers@uninp.edu.rs

Abstract: Modern access controls employ biometrics as a means of authentication to a great extent. For example, biometrics is used as an authentication mechanism implemented on commercial devices such as smartphones and laptops. This paper presents a fingerprint biometric cryptosystem based on the fuzzy commitment scheme and convolutional neural networks. One of its main contributions is a novel approach to automatic discretization of fingerprint texture descriptors, entirely based on a convolutional neural network, and designed to generate fixed-length templates. By converting templates into the binary domain, we developed the biometric cryptosystem that can be used in key-release systems or as a template protection mechanism in fingerprint matching biometric systems. The problem of biometric data variability is marginalized by applying the secure block-level Bose–Chaudhuri–Hocquenghem error correction codes, resistant to statistical-based attacks. The evaluation shows significant performance gains when compared to other texture-based fingerprint matching and biometric cryptosystems.

Keywords: biometric cryptosystem; fuzzy commitment scheme; fingerprint recognition; machine learning; convolutional neural network



Citation: Barzut, S.; Milosavljević, M.; Adamović, S.; Saračević, M.; Maček, N.; Gnjatović, M. A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks. *Mathematics* **2021**, *9*, 730. <https://doi.org/10.3390/math9070730>

Academic Editor: Angel Martín-del-Rey

Received: 28 February 2021
Accepted: 25 March 2021
Published: 28 March 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2021 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

Fingerprints are one of the most common biometric modalities used for authentication. There are three fingerprint matching approaches: correlation-based matching (i.e., a direct comparison of corresponding pixels or small regions of two fingerprints), minutiae-based matching, and non-minutiae feature-based matching. Non-minutiae matching techniques are based on the insight that some features of lower distinctiveness, such as local orientation, frequency, ridge shape, and texture information, can be extracted more reliably than figureminutiae [1]. Despite this insight, the most popular and commonly used fingerprint matching technique is the one based on minutiae, while global fingerprint texture information is used primarily for fingerprints classification. However, the texture of fingerprints carries information about different spatial frequencies, orientations, and phases, which allows for fingerprint discrimination [2]. This line of research is pursued in this paper.

Biometric templates are digital representations of corresponding biometric sample. Regardless of the feature extraction technique used, the design of biometric templates is generally driven by the following requirements for increasing the system security: non-reversibility (i.e., recovering the original sample from a given template must be computationally very expensive) [3], high-level performance (i.e., employed protection mechanisms

should not affect the system accuracy), diversity (i.e., cross-matching across databases should not be feasible), and revocability (i.e., revoking a compromised template and generating a new one should be easily feasible) [1,4]. However, meeting these requirements remains a challenging task.

In general, there are three different ways to generate a protected biometric template: encryption using classical symmetric or public key algorithms, feature transformation, and biometric cryptosystems [4]. This paper contributes to the last research direction.

We propose a novel fingerprint biometric cryptosystem (BCS) that makes two separate but related contributions to the state of the art in the field. The first contribution is in building upon the seminal fingerprint matching method introduced by Jain et al. [2]. Their method is extended by introducing a novel approach to automatic feature extraction from the fingerprint texture based on convolutional neural networks (CNNs) and transfer learning. The AlexNet neural network [5] is trained to extract fixed-length features, which are then binarized using discretization and coding, making them appropriate for applying the Hamming distance as a matching metric. The second contribution is the introduction of a biometric cryptosystem intended to increase the security of the biometric templates. Instead of storing an unprotected biometric template or raw fingerprint image, in the dedicated authentication scenario, the fixed-length binary representation of a fingerprint is combined with associated cryptographic keys, hashed passwords, and other secret codes by applying error correction techniques. It is computationally difficult to retrieve the associated secret key (cryptographic keys, hashed password, or other secret code used) or the biometrics from the secured template, and the secret key is recreated only if a matching biometric is provided on verification. By applying different secret codes to the same biometrics, the secured templates are revocable and cannot be cross-matched. CNN trained on a different training set has a unique feature extractor, and it is an additional contribution to the template revocability and diversity across various system implementations.

The proposed biometric cryptosystem is intended for use in key-release systems or as a template protection mechanism in fingerprint matching biometric systems. At the practical level, the proposed system is insensitive to minor print rotations, which are often present in real-life conditions. On the other hand, it is not intended to work with partial prints, but rather with prints containing a reference point that is not located too close to the edge of the image. However, this requirement is not a limitation of the proposed system, since it is easily achieved in the context of commercial biometric systems.

2. Related Work

The well-known feature extraction technique proposed in [2] determines the region of interest (ROI) to the fingerprint image reference point. ROI is then tessellated into the sub-images (sectors) in a certain order. The feature vector contains features that are extracted from the local information of each sector and the ordered enumeration of the tessellation captures the invariant global relationships among the local patterns. This ensures that each sector contains local information individually, while due to a certain order of sectors, invariable global connections between local textures can be distinguished. The local discriminatory information of each sector needs to be decomposed into separate components. A Gabor filter bank is one of the well-known techniques for extracting useful information in specific bandpass channels, as well as to decompose this information into biorthogonal components in terms of spatial frequencies. These quantitative measurements are considered features when comparing. A single fingerprint feature vector, called a FingerCode [6], is a set of all features obtained from each sector individually. The comparison of the two prints is based on finding the Euclidean distance between their corresponding feature vectors.

The first sophisticated approach, combining biometrics and cryptography, was proposed in [7,8]. This approach is based on fingerprints and is the first to become commercially available under the trademark Biometric Encryption™, (later known as Mytec 1 and Mytec 2). The trademark was abandoned in 2005. The Fourier transform is used to extract

biometric characteristics, and the majority vote is used to obtain the code. This code is used to protect the predefined cryptographic key, by combining the key with a biometric input (key binding). One of the first approaches based on behavioral characteristics (specifically, keyboard typing dynamics) is a hybrid system intended to increase password security, proposed by Monrose, Reiter, and Wetzel in [9]. The system generates a short binary code, which is then combined with a password, which increases its entropy and the total number of possibilities up to 2^{15} times. A similar methodology was applied for the speech [10], where a 46-bit key was successfully generated, with a false rejection rate (FRR) of about 12%. In [11], 43 signing characteristics were defined and quantized, and a binary array was generated by merging. The average key entropy achieved was 40 bits, with an FRR of 28%.

A scheme that enhances identification and authorization in secure applications by binding a biometric template with authorization information on a token, such as a magnetic stripe card, was proposed in [12]. The majority coding of sampled biometric features of an iris is used to derive a key. The obtained error correction code (ECC) and the hash value of the biometric template are stored in a protected form and used for key reconstruction. The application of fuzzy logic in biometrics was proposed in [13], where a fuzzy commitment scheme (FCS) was developed, using the basics of cryptography and error correction techniques. This scheme represents a generalization and improvement of the approach proposed in [12], with improved security and shorter ECCs. In [14], a practical and safe method for the application of iris biometrics in cryptographic systems was introduced, based on the fuzzy commitment scheme. The iris code is 2048 bits long and it is obtained by demodulating the image of the iris with complex 2D Gabor wavelets. When comparing two samples of the same iris, there are differences between them, which represent an error. These errors can be divided into two groups: random errors and burst errors. Random errors are caused by sensor noise, iris distortion, etc. Burst errors originate due to undetected lashes and glare. To overcome this problem, the proposed system employs a two-layer error correction method of Hadamard and Reed-Solomon codes. Error correction techniques are applied to a cryptographic key, resulting in a 2048-bits-long iris pseudo-code. This code is then combined with the iris code by XOR operation, resulting in a protected code. The protected code and the hash value of the key do not reveal information about the key itself and form helper data that can be stored in smart cards in the proposed solution. Recently, advances in machine learning have led to the increased use of neural networks for classification, recognition, and separation of objects in images. The initial results of the application of CNNs in biometric matching or feature extraction are promising. In [15], a biometric verification system based on two CNN modules that extract features from two fingerprints was presented. The AlexNet network was chosen for feature extraction. A concatenation of the extracted features is used as input for the fully connected (FC) layer, which calculates the score of their coincidence. This approach does not use input processing and image enhancement—the entire system relies on CNN capabilities.

Wu et al. [16] present fingerprint patterns that were classified into six types, and the accuracy of the recognition were improved to facilitate the research on human personality characteristics. Based on this idea, a six-category fingerprint database is annotated manually, and CNN is proposed for identifying real fingerprint patterns. Nguyen et al. [17] show the proposed extractor classifies each pixel of a fingerprint image into a category of minutiae with a certain orientation or a non-minutia point, thus obtaining location and orientation information of minutiae simultaneously. In [18], a lightweight CNN structure based on the singularity region of interest is proposed.

The experimental results show that the accuracy of the testing set of the proposed structure achieves 93%. The proposed CNN model with fewer neurons can achieve better suppression of overfitting and robustness to noise. Li et al. in [19] present tap water fingerprinting using a convolutional neural network built from images of the coffee-ring effect. These experiments' results suggest that the unique and reproducible residue patterns of tap water samples that can be imaged with a cell phone camera and a loupe contain a wealth of information about the overall composition of the tap water.

3. Proposed Biometric Cryptosystem

The fingerprint ridges often run smoothly in parallel, but there are one or more regions, called singular regions, where papillary lines form distinctive shapes are characterized by high curvature, frequent ridge terminations, etc. These regions can be classified into a loop, arch, delta, and whorl. The core point of the fingerprint, defined as the point at which the papillary line has the maximum concave curvature in a given fingerprint image, was chosen as the reference point for the proposed method. However, determining this point precisely is a great challenge and still a subject of scientific research interest. The precise determination of the reference point greatly affects the accuracy of biometric systems based on the local textures. Determining a reference point is performed by defining an orientation field O for the fingerprint image, where $O(i, j)$ denotes the local orientation of the papillary line in the pixel (i, j) . Due to the complexity, the local orientation is determined at the block-level of a certain size, instead of the pixel-level of each, so the input image I is normalized to have a mean value of 0 and a standard deviation of 1 and is divided into $w \times w$ sized non-overlapping blocks. For each pixel, the gradients $\partial_x(i, j)$ and $\partial_y(i, j)$ are calculated using the Sobel operator.

The corresponding operator consists of two 3×3 convolutional matrices as depicted in Figure 1.

1	0	-1
2	0	-2
1	0	-1

1	2	1
0	0	0
-1	-2	-1

Figure 1. Horizontal and vertical Sobel kernels.

The local orientation field estimation O of each block is calculated at the central pixel of each block according to the following equations [20]:

$$V_x(i, j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=j-w/2}^{j+w/2} 2\partial_x(u, v)\partial_y(u, v), \tag{1}$$

$$V_y(i, j) = \sum_{u=i-w/2}^{i+w/2} \sum_{v=j-w/2}^{j+w/2} (\partial_x^2(u, v) - \partial_y^2(u, v)), \tag{2}$$

$$O(i, j) = \frac{1}{2} \tan^{-1} \left(\frac{V_y(i, j)}{V_x(i, j)} \right). \tag{3}$$

Mathematically speaking, O represents the orthogonal direction in relation to the dominant direction of the Fourier spectrum of each window. To smooth the orientation field in a local neighborhood, the estimated orientation field is filtered with a low-pass filter. The orientation image is previously converted to a continuous vector field:

$$\Phi_x(i, j) = \cos(2O(i, j)), \tag{4}$$

$$\Phi_y(i, j) = \sin(2O(i, j)), \tag{5}$$

where Φ_x and Φ_y are x and y components of the field vector, respectively. The resulting vector is then filtered:

$$\Phi'_x(i, j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u, v)\Phi_x(i - uw, j - vw), \tag{6}$$

$$\Phi'_y(i, j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u, v) \Phi_y(i - uw, j - vw), \quad (7)$$

where W is a two-dimensional low-pass filter, and a w_Φ and w_Φ denote dimensions of the filter. Based on the obtained values, the final smoothed orientation field O' is then calculated as:

$$O'(i, j) = \frac{1}{2} \tan^{-1} \left(\frac{\Phi'_y(i, j)}{\Phi'_x(i, j)} \right). \quad (8)$$

A two-step reference point determination has been implemented in the proposed biometric cryptosystem. In the first step, the method from [21] was applied, modified to run a couple of iterations with a fixed gradient variance 1, but with different block variance σ while determining the orientation field from [20,22].

In the first iteration, value $\sigma = 3$ is used. If the detection of the reference point does not occur, then $\sigma = 5$ is used, resulting in lower accuracy but a higher detection rate. In both steps, the following parameters were used: the length of step is set to 7, the number of starting points sampled along the x and y axes is set to 2, and the threshold is set to 2. In case the reference point is not detected, fixed reference values are used. Fingerprint image enhancement is performed to eliminate noise originating from the sensor and intensity variation originating from changeable finger pressure on the sensor. Based on the orientation field and the ridge frequency, a 2D symmetric Gabor filter is formed, which convolutes with the normalized input image [20].

Based on the threshold value, the image is converted to monochrome, as shown in Figure 2.

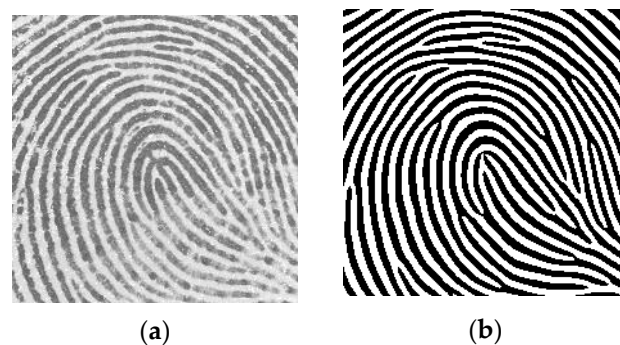


Figure 2. Image enhancement—input image (a) and enhanced image (b). The input image is taken from FVC2000 database, available online at <http://bias.csr.unibo.it/fvc2000/databases.asp>, (accessed on 17 February 2021).

3.1. Determining the Region of Interest and Forming a Training Set

Based on the reference point, the size of the region of interest is selected in accordance with the parameters of the applied neural network. For the AlexNet, the size of the input image is 227×227 pixels. The fingerprint image is cropped to those dimensions, placing the reference point at the center of ROI. CNNs require as many samples as possible for a training set. Their most common application is object recognition, where hundreds of training images are provided for each detection class. With fingerprints, this is not possible, since one identity class is created with only a few images, which significantly affects the accuracy of the neural network and represents a challenge for application in biometrics. To produce a larger training set, for each single input image, we generated multiple instances by rotating it relative to the reference point in the range of $\pm 24^\circ$ in $\pm 6^\circ$ increments, as shown in Figure 3. At the same time, we increased the accuracy of the system and its insensitivity to the usual small rotations during sampling.

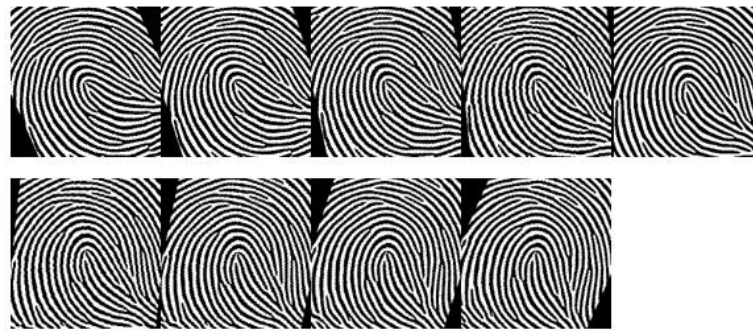


Figure 3. Generating a training set of one fingerprint.

In the proposed scheme, which is evaluated on the FVC2000 database, the first five samples of each identity class are used to make the training set for the convolutional neural network. Each sample is rotated in eight different angles, so each class is formed with a total of 45 images. When creating biometric templates, only the original images of the fingerprints are used to generate five independent templates stored in the template database.

3.2. Feature Extraction

CNN is named after the convolution, an operator often used in image processing to detect the edges or objects in images. Convolutional filters extract features from the images; based on those features, the network is trained to classify objects. In this scheme, features extracted by CNN are used in the biometric cryptosystem, in contrast to the traditional methods of extracting minutiae or information about global and local texture characteristics. Several different convolutional networks have been tested experimentally, and the best results, in terms of training speed and accuracy, have been achieved with AlexNet [5]. The network consists of five convolutional layers and three FC layers and was trained in 200 epochs, with an initial learning rate of 0.001 in series of size 96. The last FC layer was adapted to generate 1024 features, which forms a biometric template, i.e., a digital representation of the input fingerprint.

3.3. Discretization of Fingerprint Features

FCS requires a binary representation of fixed-length biometric features. Therefore, it is necessary to discretize the feature vector, which consists of real numbers. Quantization based on three limit values is applied to form four quantization ranges, where each element of the feature vector is coded with two bits:

$$(B_i)_t = \begin{cases} 00, & \text{if } (V_i)_t \leq (T_1)_t \\ 01, & \text{if } (T_1)_t < (V_i)_t \leq (T_2)_t \\ 11, & \text{if } (T_2)_t < (V_i)_t \leq (T_3)_t \\ 10, & \text{if } (V_i)_t > (T_3)_t \end{cases}, \quad (9)$$

where B_i denotes the discretized binary template, V_i is input feature value, and T_1 , T_2 , and T_3 are determined limit values. A binary representation of the feature vector in a fixed-length array of 2048 bits is formed. The limit values are experimentally determined for the selected CNN, where T_2 is constant and set to zero, while T_1 and T_3 are equal in absolute value but with opposite signs. The choice of the limit values T_1 and T_3 is in the direct correlation to the accuracy of the system; precisely the choice has an impact on the false acceptance rate (FAR) and the false rejection rate (FRR), as depicted in Figure 4: FAR increases and FRR decreases as the absolute limit value increases. Depending on the biometric application, different FAR and FRR requirements can be adopted.

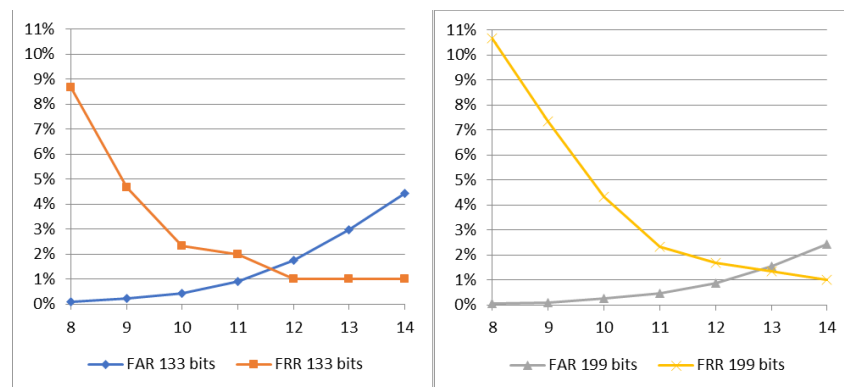


Figure 4. False acceptance rate (FAR) and false rejection rate (FRR) depending on absolute limit value T_1 and T_3 .

3.4. Forming a Biometric Cryptosystem

Biometric cryptosystems are developed to protect a cryptographic key using biometrics or to generate a key based on biometric features [23]. The problem of biometric invariance is solved by the application of helper data in biometric cryptosystems. The most common approach is to apply ECC, a technique for correcting errors in data transmission in telecommunications.

Two approaches are dominant in biometric key binding cryptosystems: the fuzzy commitment scheme [13] and the fuzzy vault [24]. The fuzzy commitment scheme is used if templates can always be represented with a fixed-length binary array. Performing the XOR operation over the template and error correction code of the same length with XOR operation produces a value called the difference vector. During authentication, the error correction code is obtained by performing the XOR operation over the sampled template and the saved difference vector. If the sampled template and the stored template originate from the same biometric source, the obtained value is close to the error correction code, which may be restored through a correction algorithm.

The proposed concept of the biometric cryptosystem is depicted in Figure 5. It is inspired by a pioneering iris cryptosystem proposed by Hao et al. in [14]. The input fingerprint image is segmented and enhanced. Based on the detected referential point, the image is cropped to the ROI. The trained CNN extracts a fixed-length feature array, and when the quantization is applied, a binary fingerprint code is formed. Error correction techniques are applied to the cryptographic key K , thus obtaining a pseudo-code θ_{ps} . The resulting code is then combined by the XOR operation with a binary fingerprint code of the same length θ_{ic} , thus obtaining the protected code θ_{lock} :

$$\theta_{lock} = \theta_{ps} \oplus \theta_{ic}. \tag{10}$$

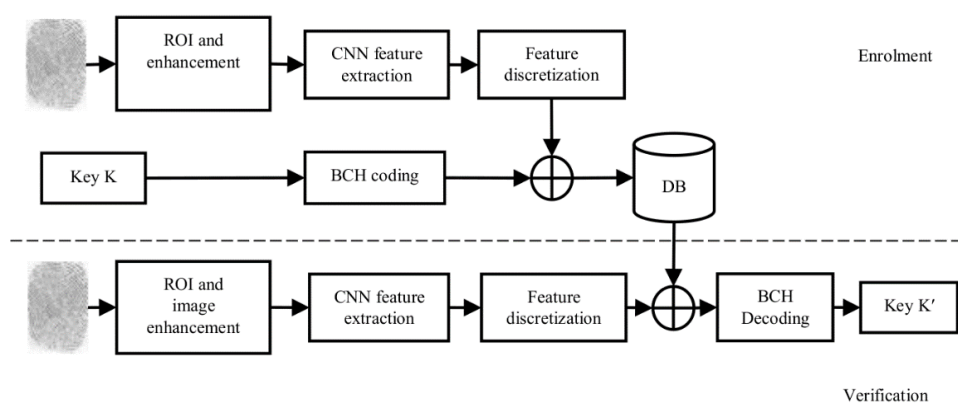


Figure 5. Enrolment and verification phases of the proposed biometric cryptosystem.

This code concurrently protects a cryptographic key and biometric template and can be stored in a database or another medium for later verification.

When reconstructing the key, the protected code is combined with the fingerprint code sample by the XOR operation, resulting in a pseudo-code:

$$\theta'_{ps} = \theta_{lock} \oplus \theta'_{ic} = \theta_{ps} \oplus \varepsilon. \quad (11)$$

If the fingerprint verification code originates from the same biometric source, the pseudo-code contains a cryptographic key K with an error due to biometric variability in sampling. However, by applying the error correction technique, the cryptographic key is restored. On the other hand, if the fingerprint verification code originates from a different biometric source, cryptographic key K cannot be restored.

3.5. Selection of Error Correction Technique

Failure of a biometric system generally leads to a breach of security in applications or facilities that it is designed to protect. Under certain circumstances, with sufficient resources and available time, any security system can be breached. A detailed analysis of vulnerabilities and attacks on authentication systems is beyond the scope of this paper. However, we analyzed some vulnerabilities specific to biometrics. In contrast to other authentication systems, where the final result is based on a simple comparison of input and stored data, the final decision of matching two biometrics is score-based, which opens the possibility for specific attacks at this stage. However, unlike conventional biometrics, BCS outputs the correct secret key or a failure message, which makes it inherently protected from attacks on the decision-making stage. However, due to the possibility that the attacker manages to gain access to the intermediate results, it is necessary to pay attention to known score-based and statistical attacks on BCS. This makes the selection of ECC important and crucial for security.

In order to develop a biometric cryptosystem, it is necessary to select an appropriate technique for error correction. All developed ECCs were designed for communication and data storage purposes. Errors that occur in a communication channel and data storage can be divided into burst error and bit-level errors. In [14], a two-layer error correction method was formed implementing the Hadamard and Reed–Solomon correction codes. Bit-level errors are corrected using the Hadamard codes, while the Reed–Solomon codes are used for sequence errors. Cryptographic keys, hashed passwords, and other secret codes are considered random and statistically independent, but error correction codes are not. When combined, ECC statistics can be used to attack BCS. The security analysis of ECCs in [25] discovered the vulnerabilities to statistical-based attacks. The authors discussed various attacks running an ECC in a soft decoding or erasure mode attack and an ECC histogram attack. All of these vulnerabilities are caused by the approach of splitting data into small chunks for encoding. A general conclusion is that all ECCs consisting of small chunks, such as Reed–Solomon and Hadamard codes, seem to be most vulnerable to the attacks exploiting the output statistics. Following this insight, in the proposed system we apply the single-block error correction technique—the Bose–Chaudhuri–Hocquenghem (BCH) code. In terms of resistance to known score-based attacks: Hill Climbing [26] and Nearest Imposter [25], if the applied BCH ECC error correction capacity is far less than $n/2$ (the length of the block), it is unlikely that the attacker would be able to deal with a huge quantization step.

BCH codes are cyclic error correction techniques that are defined using polynomials over a Galois finite field. A binary BCH code consists of three parameters, n, k, t , where n is the length of the block (i.e., the length of the biometric template) and its value is defined as $n = 2^m - 1$, k is the length of the message being encoded (i.e., the secret key length), and t is the number of bits that can be corrected. Due to parameter n , block length has to be 2047 bits, so the last bit of the biometric template is excluded. Our goal was to create a BCS with a 128-bit long key, which could later be used in symmetric cryptographic systems. Since the BCH code does not allow this particular key length as a valid parameter value

for the template length adopted in our approach, the next possible larger key length of 133 bits is selected. Applying the BCH decoding to the pseudo-code θ'_{ps} removes the error originating from the difference between two sampled biometrics of the same identity. The number of bits that can be corrected by the BCH code, for the adopted key length, is 365 bits. Due to the uneven relationship between the key length and the number of bits that can be corrected, for a key length of 199 bits, it is possible to correct 341 bits, and the system performance is not significantly changed. Increasing the key length, we lower the ECC capacity, which leads to lower FAR, but higher FRR.

4. Experimental Evaluation of the System

The proposed approach was evaluated on the FVC2000 DB2-A fingerprint database produced to conduct the fingerprint vendor competition in 2000 [1]. This database is widely used for testing fingerprint verification systems, and thus appropriate for comparative evaluation of the system accuracy. It contains eight images per hundred different fingers. Each sample is represented by an eight-bit greyscale image of size 256×364 pixels, captured by a capacitive sensor with a resolution of 500 dots per inch.

For evaluation of the proposed system, the first five images of each fingerprint class were used for training and enrolment, while the additional three images of the same class were used for verification. During the enrolment phase, five secured biometric templates were generated for each identity, by applying the same randomly generated secret key. Before the generation of the protected templates, the templates were assessed concerning their quality. All five templates of a given fingerprint class were compared with each other using the Hamming distance. Each template that did not match any of the other templates of the same class was rejected as unreliable and replaced.

The evaluation was conducted as follows. For each identity in the database, five corresponding protected templates were matched to three genuine fingerprints belonging to the same class and to all fingerprints belonging to the remaining 99 imposter identities in the database. In total, 1500 genuine (i.e., intra-class) comparisons and 148,500 imposter (i.e., inter-class) comparisons were conducted.

Tables 1 and 2 provide evaluation results of the proposed biometric cryptosystem obtained for the key lengths of 133 and 199 bits, respectively, and varying absolute limit values. The evaluation results are presented in terms of FAR, FRR, and genuine acceptance rate (GAR), which represents the inverse of FRR. As expected, FAR increases, and FRR decreases as the absolute limit value increases. Having the key length of 133 bits, the equal error rate performance is achieved for the absolute limit value of 11.5 (FAR of 1.25% and FRR of 1.00%). With a key length of 199 bits, the equal error rate performance is achieved for the absolute limit value of 11.5 (FAR of 1.15% and FRR of 1.33%).

Table 1. FAR, FRR and genuine acceptance rate (GAR) obtained for the key length of 133 bits and varying absolute limit values.

Limit Values	8	9	10	11	11.5	12	13	14
FAR	0.08%	0.22%	0.43%	0.90%	1.25%	1.75%	2.98%	4.45%
FRR	8.67%	4.67%	2.33%	2.00%	1.00%	1.00%	1.00%	1.00%
GAR	91.33%	95.33%	97.67%	98.00%	99.00%	99.00%	99.00%	99.00%

Table 2. FAR, FRR and GAR obtained for the key length of 199 bits and varying absolute limit values.

Limit Values	8	9	10	11	12	12.5	13	14
FAR	0.05%	0.10%	0.25%	0.47%	0.87%	1.15%	1.54%	2.43%
FRR	10.67%	7.33%	4.33%	2.33%	1.67%	1.33%	1.33%	1.00%
GAR	89.33%	92.33%	95.67%	97.67%	98.33%	98.67%	98.67%	99.00%

The comparative evaluation of the proposed biometric cryptosystem with respect to other relevant approaches is summarized in Table 3, in terms of FAR, FRR, equal error rate (EER), and the key length (where available).

Table 3. Comparative evaluation.

Method	FAR	FRR	EER	Key Length	Database
Fingercode [2]	4.59%	2.83%	/	/	[2]
Bakhishi and Veisi [15]	/	/	17.50%	/	FVC2002
Tuyls et al. [27]	5.2%	5.4%	5.3%	76	FVC2000
Imamverdiyev et al. [28]	0%	4.7%		76	FVC2000
Imamverdiyev et al. [28]	0%	10.67%		140	FVC2000
Proposed BCS	1.25%	1.00%	1.13%	133	FVC2000
Proposed BCS	1.15%	1.33%	1.23%	199	FVC2000

The results may be regarded as satisfactory, especially when keeping in mind that, apart from removing outlier templates, no further selection of fingerprint samples was performed. We recall that the proposed system is not intended to work with partial prints, i.e., prints with no reference point, or with a reference point located too close to the edge of the image. However, such prints were not removed from the database, to support the validity of the evaluation. In commercial applications of the proposed biometric cryptosystem, the requirement that fingerprint samples should contain appropriately located reference points could be easily meet, which would further improve the performance of the system.

5. Conclusions

In this paper, we proposed a biometric cryptosystem scheme for authentication with template protection and biometric-dependent cryptographic key-release. One of its main contributions is a novel approach to automatic discretization of fingerprint texture descriptors, based on CNN. In addition, by applying the appropriate error correction technique that meets the security requirements, we were able to create an FCS with a key length that can be used in other state-of-the-art cryptographic systems. The reported experimental results confirm the prospects of the proposed approach and open the possibility of future improvements and innovations.

Possible future research directions are related to electrocardiography (ECG) and electroencephalography (EEG) biometric identification. The method for ECG biometric identification introduced in [29] is based on cascaded CNN. In addition, a new CNN with a global spatial and local temporal filter reported in [30] works directly on raw EEG data, not requiring feature engineering. Due to the ever-increasing computational power, several CNN-based methods for ECG biometric identification have been recently proposed to increase identification performance and classification accuracy. In [31], Gurkan and Hanilci proposed an ECG-based biometric identification method using QRS images and two-dimensional CNN. These research lines will be pursued in our future work.

Author Contributions: Conceptualization, S.B.; Data curation, S.B. and M.G.; Formal analysis, S.B., N.M. and M.G.; Funding acquisition, M.M.; Investigation, M.M. and S.A.; Methodology, S.A., M.S. and N.M.; Resources, M.S. 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.

Informed Consent Statement: Not applicable.

Data Availability Statement: Publicly available datasets were analyzed in this study. The proposed approach was evaluated on the FVC2000 DB2-A fingerprint database. This data can be found in [1] as supplementary material.

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

References

1. Maltoni, D.; Majo, D.; Jain, A.K.; Prabhakar, S. *Handbook of Fingerprint Recognition*, 2nd ed.; Springer Science and Business Media: New York, NY, USA, 2009.
2. Jain, A.K.; Prabhakar, S.; Hong, L.; Pankati, S. Filterbank-Based Fingerprint Matching. *IEEE Trans. Image Process.* **2000**, *9*, 846–859. [[CrossRef](#)] [[PubMed](#)]
3. Adamović, S.; Mišković, V.; Maček, N.; Milosavljević, V.; Šarac, M.; Saračević, M.; Gnjatović, M. An Efficient Novel Approach for Iris Recognition Based on Stylometric Features and Machine Learning Techniques. *Future Gener. Comput. Syst.* **2020**, *107*, 144–157. [[CrossRef](#)]
4. Jain, A.K.; Nandakumar, K.; Nagar, A. Biometric Template Security. *EURASIP J. Adv. Signal Process.* **2008**, *2008*, 1–17. [[CrossRef](#)]
5. Krizhevsky, A.; Sutskever, I.; Hinton, G.E. ImageNet classification with deep convolutional neural networks. *Adv. Neural Inf. Process. Syst.* **2012**, *1*, 1097–1105. [[CrossRef](#)]
6. Jain, A.K.; Prabhakar, S.; Hong, L.; Pankanti, S. FingerCode: A filterbank for fingerprint representation and matching. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Fort Collins, CO, USA, 23–25 June 1999.
7. Soutar, C.; Tomco, G.J. Secure private key generation using a fingerprint. In Proceedings of the Cardtech/Securetech Conference, Atlanta, GA, USA, 5–8 May 1996.
8. Soutar, C.; Roberge, D.; Stoianov, A.; Gilroy, R.; Kumar, B.V. *Biometric Encryption, ICSA Guide to Cryptography*; McGraw-Hill: New York, NY, USA, 1999.
9. Monroe, F.; Reiter, M.K.; Wetzel, S. Password hardening based on keystroke dynamics. In Proceedings of the 6th ACM Conference on Computer and Communications Security, New York, NY, USA, 15–19 November 1999.
10. Monroe, F.; Reiter, M.K.; Li, Q.; Wetzel, S. Cryptographic key generation from voice. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 14–16 May 2001.
11. Hao, F.; Chan, C.W. Private key generation from on-line handwritten signatures. *Inf. Manag. Comput. Secur.* **2002**, *10*, 159–164.
12. Davida, G.L.; Frankel, Y.; Matt, B.J. On enabling secure applications through off-line biometric identification. In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, USA, 6 May 1998.
13. Juels, A.; Wattenberg, M. A fuzzy commitment scheme. In Proceedings of the 6th ACM Conference on Computer and Communications Security, Singapore, 15–19 November 1999.
14. Hao, F.; Anderson, R.; Daugman, J. *Combining Cryptography with Biometrics Effectively*; Technical Report 640; University of Cambridge: Cambridge, UK, 2005.
15. Bakhshi, B.; Veisi, H. End to end Fingerprint Verification Based on Convolutional Neural Network. In Proceedings of the 27th Iranian Conference on Electrical Engineering (ICEE), Yazd, Iran, 30 April–2 May 2019.
16. Wu, F.; Zhu, J.L.; Guo, X.M. Fingerprint pattern identification and classification approach based on convolutional neural networks. *Neural Comput. Appl.* **2020**, *32*, 5725–5734. [[CrossRef](#)]
17. Nguyen, V.; Liu, J.S.; Nguyen, T.H.; Kim, H. Universal fingerprint minutiae extractor using convolutional neural networks. *IET Biom.* **2020**, *9*, 47–57. [[CrossRef](#)]
18. Jian, W.; Zhou, Y.J.; Liu, H.M. Lightweight Convolutional Neural Network Based on Singularity ROI for Fingerprint Classification. *IEEE Access* **2020**, *8*, 54554–54563. [[CrossRef](#)]
19. Li, X.Y.; Sanderson, A.R.; Allen, S.S.; Lahr, R.H. Tap water fingerprinting using a convolutional neural network built from images of the coffee-ring effect. *Analyst* **2020**, *145*, 1511–1523. [[CrossRef](#)] [[PubMed](#)]
20. Thai, R. *Fingerprint Image Enhancement and Minutiae Extraction*; The University of Western Australia: Crawley, Australia, 2003.
21. Zhu, E.; Guo, X.; Yin, J. Walking to Singular Points of Fingerprints. *Pattern Recognit.* **2016**, *56*, 116–128. [[CrossRef](#)]
22. Kovese, P. MATLAB and Octave Functions for Computer Vision and Image Processing. Available online: <http://www.peterkovese.com/matlabfns> (accessed on 10 January 2021).
23. Rathgeb, C.; Uhl, A. A survey on biometric cryptosystems and cancellable biometrics. *EURASIP J. Inf. Secur.* **2011**, *2011*, 1–25.
24. Juels, A.; Sudan, M. A fuzzy vault scheme. In Proceedings of the IEEE International Symposium on Information Theory, Lausanne, Switzerland, 30 June–5 July 2002.
25. Stoianov, A.; Kevenaar, T.A.M.; Van der Veen, M. Security issues of biometric encryption. In Proceedings of the IEEE International Conference Science and Technology for Humanity, Toronto, ON, Canada, 26–27 September 2009.
26. Adler, A. *Vulnerabilities in Biometric Encryption System*; LNCS (Vol. 3546); Springer: Berlin/Heidelberg, Germany, 2005.
27. Tuyls, P.; Akkermans, A.; Kevenaar, T.; Schrijen, G.-J.; Bazen, A.; Veldhuis, R. Practical Biometric Authentication with Template Protection. In Proceedings of the International Conference Audio and Video Based Biometric Person Authentication, New York, NY, USA, 20–22 July 2005.
28. Imamverdiyev, Y.; Teoh, A.B.J.; Kim, J. Biometric cryptosystem based on discretized fingerprint texture descriptors. *Expert Syst. Appl.* **2013**, *40*, 1888–1901. [[CrossRef](#)]
29. Li, Y.Z.; Wang, K.Q.; Li, X.L. Toward improving ECG biometric identification using cascaded convolutional neural networks. *Neurocomputing* **2020**, *391*, 83–95. [[CrossRef](#)]

-
30. Chen, J.X.; Mao, Z.J.; Yao, W.X.; Huang, Y.F. EEG-based biometric identification with convolutional neural network. *Multimed. Tools Appl.* **2020**, *79*, 10655–10675. [[CrossRef](#)]
 31. Gurkan, H.; Hanilci, A. ECG based biometric identification method using QRS images and convolutional neural network. *Pamukkale Univ. J. Eng. Sci.* **2020**, *26*, 318–327. [[CrossRef](#)]