IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 23, 2021, accepted December 3, 2021, date of publication December 8, 2021,
date of current version December 20, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3133908

An Effective Multi-Mode Iris Authentication System on a Microprocessor-FPGA Heterogeneous Platform With QC-LDPC Codes

LONGYU MA, CHIU-WING SHAM, (Senior Member, IEEE), CHUN YAN LO, AND XINCHAO ZHONG
School of Computer Science, The University of Auckland, Auckland 1010, New Zealand
Corresponding author: Longyu Ma (lma792@aucklanduni.ac.nz)

The work was supported in part by Exploration Squared Limited (ES Ltd.), New Zealand.

ABSTRACT With the emergence and popularity of iris biometrics, there are increasing concerns regarding the feasibility of iris authentication systems and their corresponding variability reduction methods. The former issues are typically addressed by optimizing key factors, such as iris size, image quality and acquisition wavelength. As for the latter, introducing error correction codes to reduce intra-user variability in the enrolled identifiers becomes novelly promising. This paper proposes a conventional iris authentication system and a hardware-friendly QC-LDPC error correction code scheme on a microprocessor-FPGA platform. Different QC-LDPC codes in IEEE 802.16e were analyzed and selected. Suitable codes were applied, followed by the evaluation experiments. The proposed design achieves a competitive result with up to 0.20% EER and 0.50% ZeroFAR on the CASIA-IrisV4-Syn database. Cryptographic keys with lengths of up to 288 bits can also be generated and recovered. Such a device can be potentially used for applications such as an access control system in high-security areas, identity verification at the borders, biometric cryptography and related authentication scenarios.

INDEX TERMS Iris authentication, biometric, error correction codes, LDPC, QC-LDPC, FPGA, dynamic partial reconfiguration.

I. INTRODUCTION

Increased incidences of cybercrime have jeopardized the safety of individuals and businesses in today's digitalized society, when everything is done online, resulting in financial and other damages. Iris recognition is a sophisticated automated biometric verification system based on the mathematical pattern recognition techniques. Compared to other biometric systems, iris recognition outperforms them because it eliminates the danger of collusions or false matches even at cross-comparison among a large population. It has been considered highly secure and has become an essential tool in some countries' Department of Defense and border management. In the field of consumer electronics, some of handheld devices have also embedded iris recognition systems for authentication and security purposes. The increased use of such advanced security technology across a variety of industrial verticals has driven the development of biometric recognition market [1]. Nevertheless, implementing energy-efficient and uncompromised high-secure iris recognition-related systems for real-life applications is not viable to satisfy market requirements. One of the most challenging issues in the field of biometrics [2] is the unavoidable, innate deviation between different iris images, even though these iris templates are captured from the same authenticated identity. Such variance can cause unexpected false matches, leading to security breaches. The failure to provide hackproof security constrains the market growth of iris recognition technology to some extent. A fuzzy commitment scheme applied to change an iris image to iris codes is a common solution to alleviate the negative effect caused by unreliable bits in iris templates, but the level of granularity is difficult to balance. A better error tolerance will result in a less secure system because the detail loss after using the fuzzy commitment may increase the possibility of failure to distinguish two irises from different persons.

Introducing error correction codes to detect and correct error-prone iris codes is a novel method in the biometric field. Generally, the process of identifying a user consists of two phases.

The associate editor coordinating the review of this manuscript and approving it for publication was Yu-Cheng Fan.

- In the enrollment phase, iris templates are processed and stored in the designated memory space.
- In the verification or probe phase, a new iris template is extracted from the user waiting to be granted, and it is compared with the data (known as reference) already stored. If the comparison matches, the user is identified; otherwise, the grant is denied.

In a biometric channel model, the difference between the iris reference template and the query iris template is called ''noise''. In the enrollment phase, error correction codes are applied to encode the reference. In the probe phase, a combination of query iris and parity bits from the reference is fed into an error correction code decoder. If the error-correction capability is sufficient, the decoded results can ease the difficulty of sorting genuine and imposter requests under a certain threshold.

A further study is called iris cryptography. It is defined as a mechanism that binds a person's iris and a series of private passwords or keys. The error correction codes, such as low-density parity-check (LDPC) or Reed Solomon (RS) codes, are used to generate (encode) and recover (decode) passwords or keys. The key is retrieved only during the successful authentication.

In this paper, we propose a multi-mode iris authentication implementation on a microprocessor and field programmable gate array (FPGA) heterogeneous platform. Quasi-cyclic low-density parity-check (QC-LDPC) codes are used to improve the overall system performance. The main contributions of this work are presented as below:

- Several QC-LDPC codes in IEEE 802.16e were selected according to their error-correction capability for iris recognition. The most suitable candidate codes for iris recognition were selected for further implementation after a comprehensive set of experiments.
- We conducted a rigorous analysis of the special quantization relationship between the iris codes and their parity bits. We employed QC-LDPC soft-decision decoders in an iris authentication system with the most appropriate quantization.
- Multi-mode implementation was employed using Dynamic Partial Reconfiguration. This allows our proposed system to have the flexibility of real-time adjustment to achieve a better trade-off between power consumption and security level.
- We conducted experiments on the iris recognition system with a more difficult database, CASIA-IrisV4-Syn. The experimental results, in terms of EER and ZeroFAR (FRR when FAR $=0$), show that our proposed system is promising and competitive compared to previous works.

The remaining of this paper is structured as follows: In Section II, we briefly review the related studies. Then, the proposed architecture is presented in Section III, followed by experiments and conclusions in Sections IV and V, respectively.

II. RELATED WORKS

In the past few years, there have been numerous studies on the integration of error correction codes into the biometric field. The major challenges on biometric are basically: **(a)** The balance of the error-correction capability and quantity and distribution of errors in an iris. **(b)** A suitable hardware platform for pre-processing modules, such as iris image processing algorithms, and post-processing modules, such as error-correction and biometric key cryptography. **(c)** Multiple requirements in different scenarios, such as biometric system with error correction codes for the iris and another biometric.

To meet challenge **(a)**, information-theoretic analysis is adapted to select the appropriate region of irises in [3]. Moreover, RS error correction codes were adopted to mitigate intra-user variability. Based on different error-correction limits, a few different RS codes were tested thoroughly. With suitable RS codes, cropped iris region and interleaving systems, the proposed platform can also be used for additional biometric key verification. Reference [4] combined Hadamard error correction codes with convolutional neuron networks into their proposed iris classification model. The accurate rate cannot compete with other latest works mentioned above. Reference [5] presented an iris-based biometric cryptosystem in which LDPC error correction code scheme was applied, whereas the feasibility was not clarified. References [6] and [7] both implemented an LDPC code scheme onto a biometric system in the absence of soft information from the ''biometric channel''. It lost some parts of error-correction capability that it should have gained.

As for challenge **(b)**, [8] designs a resource-aware architecture for iris boundary detection algorithm, known as circular Hough transform, onto an FPGA. Owing to parallel-pipelined implementation, a high reduction in memory space is achieved with an up to 24.6% drop in the detection rate. Iris feature extraction is implemented on an FPGA in [9] and [10], but the algorithm precision is reduced significantly. The equal error rate (EER) can only be 12% on the CASIA-Iris database, whereas most of the studies can obtain an EER under 1%. Hence, this research contribution is not practical. To some extent, it indirectly proves that image processing algorithms, such as feature extraction, may not be suitable for FPGAs unless a thorough feasibility evaluation is performed.

Implementing LDPC codes, especially QC-LDPC codes onto FPGAs or application-specific integrated circuits (ASICs), are very common today. Comprehensive studies [11]–[13] have been conducted to reduce the complexity and improve the accuracy and throughput of the QC-LDPC decoders, such as applying appropriate calculations [14]–[17] and different structures of LDPC codes [18]–[20]. All the aforementioned studies adopt FPGAs or ASICs as their testing platforms in order to parallel and pipeline their decoding algorithm to the best extent.

With regard to challenge **(c)**, [21] combines iris and face recognition for the proposed architecture. RS codes are also applied to detect and correct the errors of the two correlated biometric features. References [22]–[24] introduced IEEE

802.11n compatible multiple-LDPC decoders onto iris recognition systems to rectify errors caused by intra-user variability, but the over-simplified system, except decoders, does not achieve competitive performance.

To address these challenges, we select two types of QC-LDPC codes from several candidates in IEEE 802.16e based on the balance of error-correction capabilities and iris error distributions. In the meantime, an iris-authentication-friendly hardware platform is proposed because it can keep image processing modules in a microprocessor section and employ QC-LDPC decoders onto a programmable logic section. This all-in-one design also includes a biometric key cryptography function and is able to activate any one of the modes on the fly using FPGA's Dynamic Partial Reconfiguration technology. An FPGA, as part of a consumer electronic platform, might not be a good one long before, but over the last decade, FPGA has become down-to-earth gradually for consumer electronics. Reference [25] presented an FPGA-based dedicated digital filter for high efficiency video coding (HEVC) standard and confirmed the suitability of the proposed design for ultra-high definition (UHD) consumer applications. Another study [26] proposed an FPGA-based frame grabber to process images or videos from a camera. In [27], apart from what they proposed, the authors also enumerated several latest different tier FPGAs that are adequate for image or video processing. Furthermore, a recent FPGA system-on-module(SoM) [28] has become an ideal edge-application platform [29] with competitive cost, compact design and sufficient hardware resources. This trend has been clarified by a white paper concerning FPGA involvement in the next generation of smart home appliances [30]. This is also the primary reason for considering a hybrid microprocessor-FPGA platform in our proposed architecture.

III. PROPOSED EMBEDDED IRIS RECOGNITION SYSTEM

A. HARDWARE PLATFORM

The complete designed modules are located in the Zynq UltraScale+ XCZU7EV MPSoC (multi-purpose system on chip) in Fig. 1. There are five primary components in this system: data collection subsystem, image processing subsystem, matching/decision subsystem, storage subsystem and QC-LDPC decoder subsystem. Each of the subsystems is discussed in detail late, as shown in Fig. 2.

In this MPSoC chip, hard-core ARM processors are attached to an AMBA AXI bus interconnection, which interfaces with memory and other peripherals, such as the USB controller connecting a near infrared (NIR) camera kit, the SD card controller storing reconfiguration bit files and iris codes, and hardware internal configuration access port (HWICAP) for partially reconfiguring QC-LDPC decoders.

1) DATA COLLECTION

The data collection subsystem refers to the NIR camera kit, USB controller and its control programs in the microprocessor. It can obtain an NIR raw image, which is the initial status

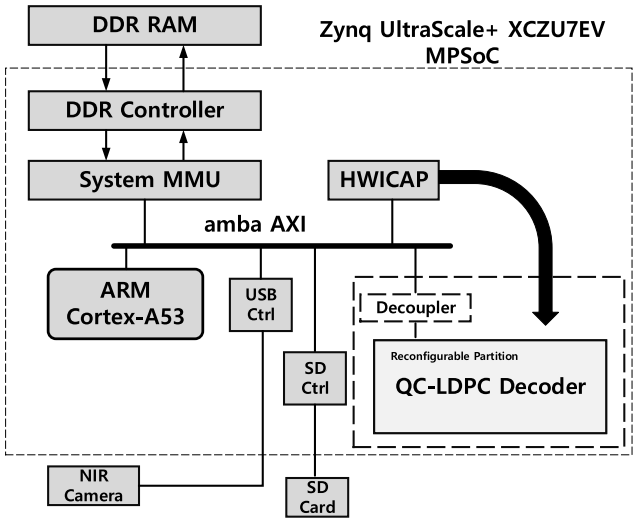


FIGURE 1. Target system architecture.

of the flowchart in Fig. 2. It should be noted that the iris data in the experimental section are from the CASIA database as it is convenient to compare with other works in terms of performance.

2) IMAGE PROCESSING SUBSYSTEM

The image processing subsystem marked by dotted-lines in Fig. 2 plays an essential role in iris detection, segmentation(Canny Edge Detection), normalization (Hough Transform) and feature extraction (One-dimensional (1D) Log-Gabor), which stem from the University of Salzburg Iris-Toolkit v3.0 [31]. The programs are executed in a Linux-based microprocessor.

3) STORAGE SUBSYSTEM

The storage subsystem contains a physical memory space in which the templates of the irises are stored. The iris codes generated from the Image Processing Subsystem will be stored here. Before that, if a key insertion or generation is requested, part of this subsystem in the microprocessor will be responsible for performing XOR operation between a key and enrolled iris codes. The new vector of iris codes is then transferred to a QC-LDPC encoder program run in the microprocessor. The encoded data, as the final reference data, are eventually stored in a section of an SD card. If no key insertion task is pending, the storage subsystem directly stores the iris codes in the SD card.

4) QC-LDPC DECODER SUBSYSTEM

The purpose of the QC-LDPC decoder Subsystem is to decode the query iris codes, to which the reference parity bits are attached and finally eliminate as many biometric errors as possible. The QC-LDPC decoders were implemented on the FPGA section in Fig. 1. In addition, if key recovery is permitted, the subsystem needs to retrieve the reference key and obtain the input data of the new decoder by performing

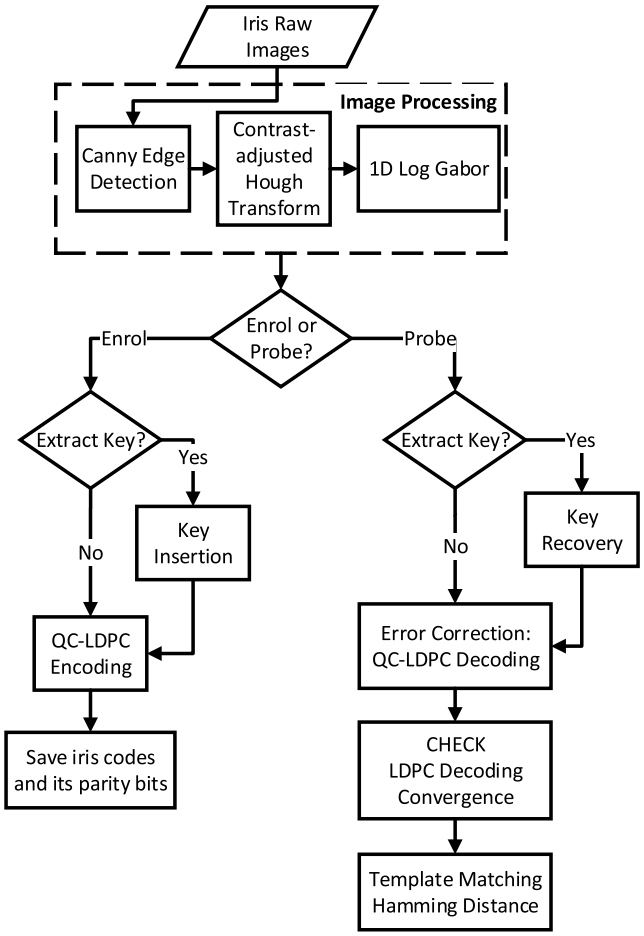


FIGURE 2. Basic data flowchart of the proposed system.

the XOR operation between query the iris codes and keys, as shown in Fig. 7.

5) MATCHING/DECISION

The matching algorithm is activated during the verification phase and compares the reference iris codes with the query iris codes. Specifically, a bit-to-bit hamming distance (HD) between these two irises' bit patterns is calculated. If A and B are denoted as these two irises, the HD calculation is based on Equation (1). Then, the result is compared to the pre-set threshold. If the result is less than the threshold, the system will grant the requester access. Otherwise, it denies the request. A block diagram is at the bottom of Fig. 2.

$$HD = \frac{1}{n}\sum_{i=1}^{n} A_i \oplus B_i \tag{1}$$

B. QC-LDPC SELECTION

An iris can be feature-extracted to 10,240 bits using the 1D Log-Gabor scheme and these bits should be encoded by one class of QC-LDPC codes to tolerate errors. For convenience, we focus on the IEEE 802.16e protocol, as it provides many QC-LDPC combinations with a variety of code rates and code lengths. Because not all of LDPC codes can fit in a biometric

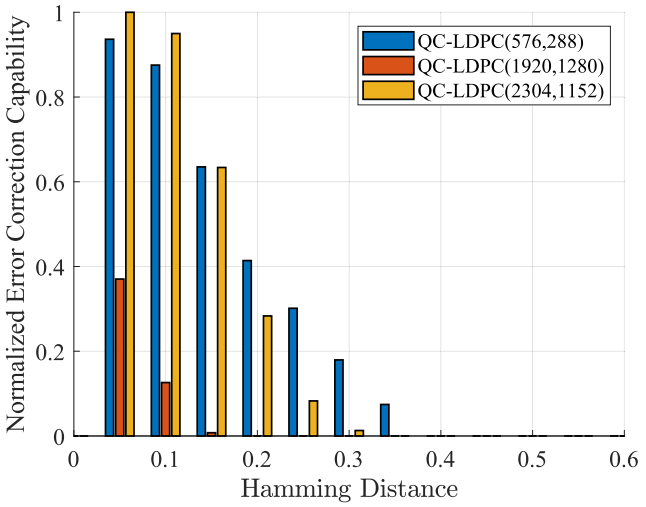


FIGURE 3. Normalized iris error-correction capability from three different QC-LDPC codes.

verification system and play a crucial role to correct errors, proposing a method to examine error correction codes cannot be omitted. In other words, how to measure the capability of correcting iris codes errors for each QC-LDPC code candidate should be done before implementation. Besides, avoiding the capability not greater than the minimum difference of inter-users also needs to be focused on.

We first determined the maximum error-correction capability among all types of QC-LDPC codes. It should be noted that if the LDPC code rate is close to zero, that is, the effort for channel coding will be considerably great [32]. The smallest code rate shown in IEEE 802.16e is 1/2. One QC-LDPC code (1920,1280) is also chosen for further comparison. Three typical QC-LDPC codes are chosen, and their practical error-correction capabilities are shown in Figure. 3. Because the input data for QC-LDPC encoders and decoders are iris codes, not randomized binaries, the distribution of error-correction capability for these three QC-LDPC codes are not general results. They are exclusive to the irises.

To present Fig. 3 more conveniently, we define a metric named LDPC contribution score (LCOS) to evaluate the improvement made by QC-LDPC encoding and decoding schemes.

In the single iris LCOS calculation, the length of iris codes after feature extraction denotes len_{iris}. In our case, len_{iris} is 10,240. For a QC-LDPC(n,k), num_{block} is denoted by the number of blocks that this decoder needs to decode in the verification/probe phase for a single iris. For example, if QC-LDPC(2304,1152) is selected, $num_{block} = \lceil 10240/1152 \rceil = 9$. $\mathbf{H}$ represents the parity matrix used to examine whether the decoder has managed to correct all errors of a block. If the product of this matrix multiplication (the syndrome), $\mathbf{H}^* \mathbf{M}$, is a vector of 0, all iris codes in the block are error-free. Otherwise, this block of iris codes cannot be corrected with no positive LCOS. We accumulate the number of clean iris codes in a single iris bit by bit, and the entire sum is defined as LCOS.

Algorithm 1 Single Iris LCOS Calculation

1: Initialization:$len_{iris} \leftarrow 10240, m_0 \leftarrow 0, y \leftarrow 0, LCOS \leftarrow 0$
2: $num_{block} = \lceil len_{iris}/k \rceil$
3: **while** $m_1 < num_{block}$ **do**
4: **if** $\mathbf{H}*\mathbf{M}[m_0k : (m_0+1)k-1] = 0$ **then**
5: $y \leftarrow y+1$
6: **end if**
7: $m_1 \leftarrow m_1 + 1$
8: **end while**
9: $LCOS = LCOS + y * k$

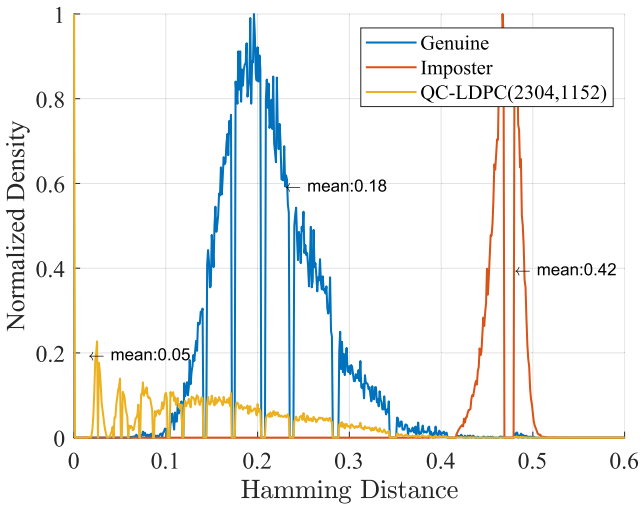


FIGURE 4. QC-LDPC codes (2304,1152) overlaid on top of the genuine and impostor normalized HD distributions.

A total of 40,000 intra-user comparisons are presented in Fig. 3. The X-axis represents the HD result of every comparison, and the Y-axis shows the Min-Max normalized LCOS sum, the maximum of which used to be 10,388. It can be observed that QC-LDPC(2304,1152) achieves a better error-correction capability than the other two when intra-user has fewer differences. If the two iris codes in the genuine comparison differ more significantly, QC-LDPC(576,288) outperforms the other two.

If the error-correction capability of some LDPC codes is over-qualified, there may be some unexpected issues, such as reducing the inter-user or imposter HDs. Depicted in Fig. 4, distribution of genuine and imposter from CASIA-IrisV4-Syn presents the same trend as the [33] in which it is reported that intra-user groups have a difference in iris codes [34] between 10% and 20%, while inter-user groups differ between 40% and 60%. This indicates that a suitable error correction code should show the best performance when HD is less than 0.2 and start to downplay the error after that. For 40,000 imposter groups, it was found that QC-LDPC(2304,1152) only increased 0.063 together in terms of HD. This means that the imposter distribution is nearly untouched, while QC-LDPC(576,288) brings a 207.687 increase. A more considerable undesirable imposter

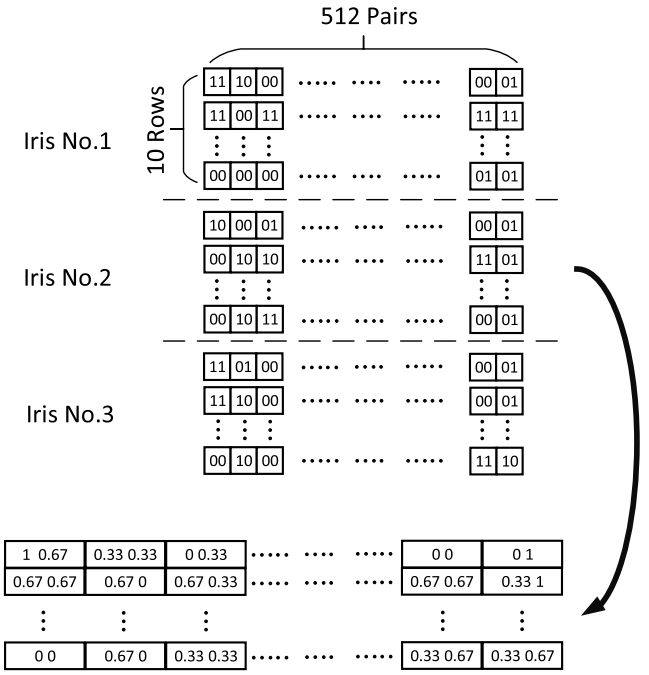


FIGURE 5. Multiple sampling for iris codes.

HD increase makes QC-LDPC(576,288) not the perfect option. Therefore, we chose the QC-LDPC(2304,1152) during iris authentication. The yellow curves denoting QC-LDPC(2304,1152) is the error-corrected genuine distribution with an average HD shown in Fig. 4.

C. MULTI-SAMPLING IRIS IMAGES SCHEME

Iris codes are generated using One-dimensional (1D) Log-Gabor on the iris source [35]. Our implementation applies a similar method based on 1D Log-Gabor wavelets, as a higher precision over 2D [36] in iris boundary detection can be reached [3]. The result is an array of complex numbers. In our case, one iris image is ultimately converted to a 512 x 10 complex number array. Each complex number includes a real part and an imaginary part, which means 10,240 numbers can represent an iris. The obtained matrix is then encoded according to the phase of the complex number mentioned in [37]. The samples of encoded matrices resemble any of the upper three depicted in Fig. 5. The multi-sampling method derives from a solution named "Majority voting" [38]. Instead of making a hard decision for phase-encoded numbers [38], we leverage the soft-decided iris codes to feed a soft-decision QC-LDPC decoder. One of the merits of using soft-decision decoders is that a soft-decision decoder performs better than a hard-decision decoder [39] and can provide 1–2 dB of additional net coding gain.

D. IRIS CODES AND PARITY BITS QUANTIZATION SCHEME

The aforementioned multi-sampled iris codes need to be quantized in fix-point precision. Its corresponding LDPC parity bits should also be obtained from a storage containing

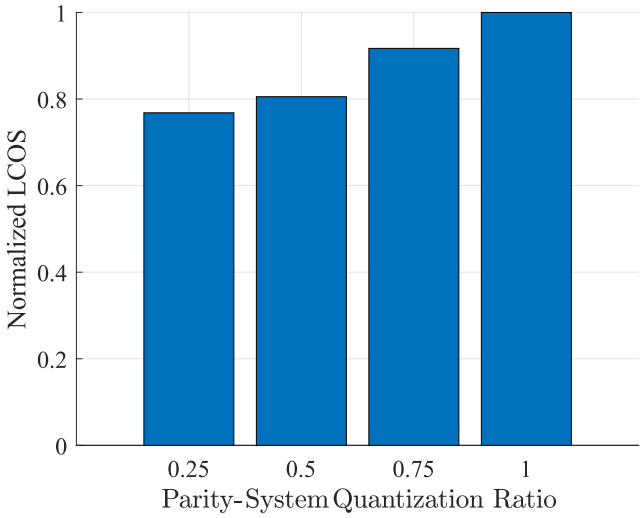


FIGURE 6. Normalized LCOS in parity-system ratios under different quantization schemes.

enrolled irises before both of them enter the activated soft-decision QC-LDPC decoder. Under normal telecommunication conditions, source data, also known as system bits, and their parity bits are conveyed via a communication channel. A united quantization scheme may be applied to the data and its parity, owing that both are distorted by the channel noise. However, we have no clue how to quantize the system bits with noise and the noise-free parity bits, as the parity bits in ''biometric channel'' model are not transmitted and very ''clean''. It should be noted that the proposed iris authentication system adopts a 32-bit fix-point Min-Sum decoding algorithm, where an integer can be represented in 32 bits. Therefore, we investigate four typical scenarios regarding the relationship between the domain of quantized multi-sampled iris codes and their parity bits. The QC-LDPC code chosen for this investigation was (2304,1152). Considering that parity bits are absolutely not error-prone, their quantized binary ''1'' or ''0'' should reach the maximum and minimum, which is $2^{32}-1$ or 0. As illustrated in Fig. 6, The discretized value ranges for the system bits are $[0, 0.25 * 2^{32}-1]$, $[0, 0.5 * 2^{32}-1]$, $[0, 0.75 * 2^{32}-1]$, $[0, 2^{32}-1]$, which are denoted by ''0.25'', ''0.5'', ''0.75'', ''1'' on X-axis separately. The y-axis measures the error-correction capability.

It can be easily found that if the same quantization scheme as parity bits is adopted by the system bits or iris codes, the error-correction capability of the QC-LDPC codes can reach the maximum.

E. BIOMETRIC KEY GENERATION AND RECOVERY

QC-LDPC(576,288) was chosen for the other purpose, which is the biometric key generation and verification. Under Zero-FAR as the threshold to grant a user's request, at least one block of iris codes can be recovered. The ability was statistically proved, because LCOS value is always positive under any of 40,000 testing groups we created from CASIA. We inserted the same key to every block of one user's iris codes. In our case, the number of blocks is $\lceil 10240/288 \rceil = 36$. When any one of blocks is fully error-corrected, a key with no more than 288 bits, which is the maximum information bits of (576,288), can be re-generated. Our proposed method is different from [3] which analyzed and extracted the iris regions of high entropy and used the regions as the carriers of biometric keys. Fig. 7 shows the detail of how a key is generated and gets involved in the proposed iris authentication system.

If a biometric key generation and recovery for identity verification is required, the whole system will execute additional procedures, such as the key insertion and key recovery in Fig. 2. After all iris codes are obtained, the key insertion module performs an XOR operation between a random number, known as a key, and iris codes. Then it will feed the combination (iris codes XOR the KEY) to an QC-LDPC encoder. Every block of iris codes need to be XORed with the same key and encoded by the QC-LDPC encoder. The key recovery ability is based on that at least one block of QC-LDPC codes can be fully error-corrected. The encoded output can be used later for recovering the key when an authenticated user send a request. During a key recovery process, new iris codes captured from a requester (highlighted with green) and the combination (highlighted with grey) will be involved in another XOR operation. The outcome is the key with some errors. With the corresponding parity bits, a new combination including a key, errors and parity bits are delivered to the QC-LDPC decoder. Any decoded block that can pass the verification mentioned in the Line 4 of Algorithm 1 will be considered as a valid key.

Note that QC-LDPC(2304,1152) is not a qualified candidate, because it was found that an iris to be verified may match the reference iris under a certain threshold, but no improvement related to the QC-LDPC was made in some of 40,000 same groups as QC-LDPC(576,288).

F. MULTI-MODE IMPLEMENTATION USING DYNAMIC PARTIAL RECONFIGURATION

Two types of QC-LDPC codes, namely (2304,1152) and (576,288), were selected for the proposed implementation. The scheduling mechanism for which the QC-LDPC codes should be activated on the FPGA is based on Dynamic Partial Reconfiguration [40]. DPR is a circuit-level FPGA technology, allowing users to set a dynamic partition and upload a configuration bit file to that partition without influencing other circuits on the FPGA. The uploaded configuration bit file, known as a partial bit file, containing only the necessary data, takes only a fraction of time compared to a full-version bit file for the entire FPGA.

The two selected QC-LDPC decoders were synthesized and compiled into bit files separately. The bit files are stored in the external memory, SD card as shown in Fig. 1. Microprocessors can control HWICAP to upload any required bit file to the FPGA section where bus decouplers are inserted into AMBA AXI bus and operate while one QC-LDPC decoder

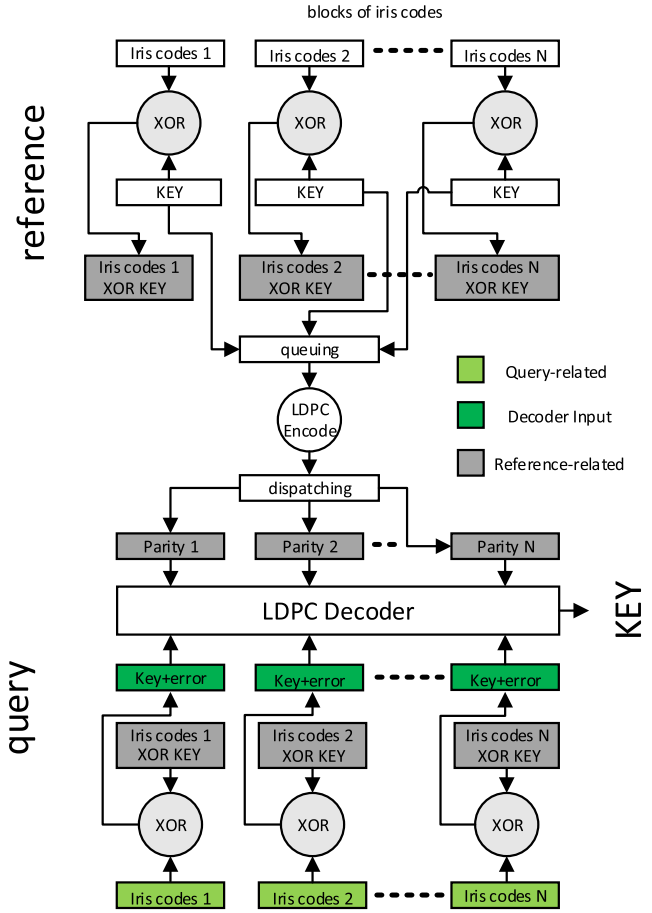


FIGURE 7. Cryptography using biometric key.

switches to another. This action was conducted to prevent any meta-stability.

IV. PERFORMANCE EVALUATION

The experiments for the evaluation of the proposed design were conducted using a Xilinx ZCU104 MPSoC development kit (Zynq UltraScale+ XCZU7EV-2FFVC1156). The platform can be equivalent to a combination of microprocessors and an FPGA with a high-speed on-chip bus and I/Os. Image processing algorithms, QC-LDPC encoders, matching and other control modules are executed on an ARM-based Linux OS. In terms of QC-LDPC decoders, they were deployed in the FPGA section. The communication between these two sections above is realized via AMBA AXI buses. The multi-mode switching function using DPR technology is activated or deactivated by the microprocessor on ZCU104.

CASIA-IrisV4-Syn is used as the iris dataset instead of camera capture in the following experiments. Different from these related studies choosing CASIA-IrisV4-Internal (real iris images), the iris textures in the subset CASIA-IrisV4-Syn are synthesized. They involve deformation, blurring and rotation; thus, they are more challenging for iris recognition. There are 10,000 iris images obtained from 1,000 subjects. Based on these images, 38,000 intra-groups and

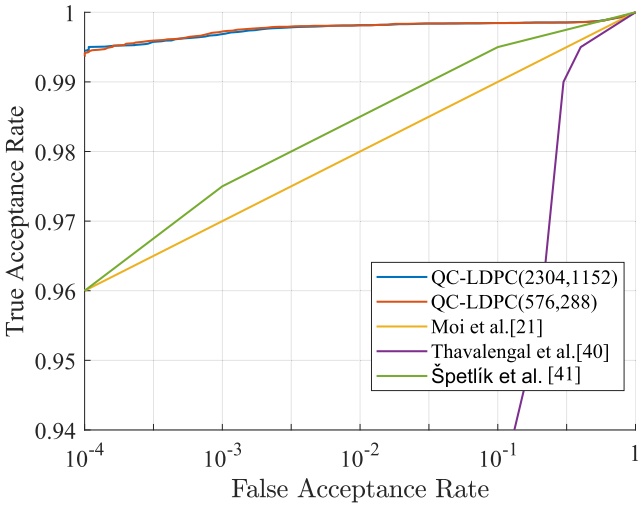


FIGURE 8. ROC curves comparison.

240,000 inter-groups were created and used to verify our proposed design and measure its performance.

The Experiments below are meant to analyze the system recognition accuracy, complexity and latency per block of iris codes, followed by a comparative study against some state-of-the-art designs.

A. ACCURACY

Receiver Operating Characteristic (ROC) Curves are provided in Fig. 8. It is one of the most common metrics used to report the performance of a biometric system. It can be found that after applying any one of two QC-LDPC codes, the True Acceptance Rate (TAR) of the proposed design yields an excellent result, outperforming other three state-of-the-art implementations, which is Moi and Yong [21], Thavalengal *et al.* [41], Špetlík and Razumenić [42].

Fig. 9 illustrates the FAR and False Rejection Rate (FRR) curves under different HD thresholds. The EER can be obtained at the point where False Acceptance Rate (FAR) equals FRR. Using QC-LDPC(2304,1152), the EER reached to 0.23%. The value of ZeroFAR was 0.5%. The ZeroFAR point indicates that the authentication system can recognize any imposter attack when its threshold is set up at ZeroFAR.

It is noteworthy that the DPR-based EER denoted by "EER of DPR" in Fig. 9, can reach 0.20%, which is even lower than the EER of QC-LDPC(2304,1152). This is the intersection of the purple and blue curves. According to the HD threshold, a user may switch decoders to pursue a better EER of the iris authentication system.

Table 1 provides the highlights of the performance comparison between our method and other related works. The proposed architecture with QC-LDPC codes is not only implementable but also provides better performance on an equivalent or more difficult database.

B. BIOMETRIC KEY TEST

The database, CASIA-IrisV4-Syn, in this section is identical to the one on which we tested the accuracy of the proposed

TABLE 1. Performance comparison with other designs implementing iris authentication systems.

	ERR(%)	ZeroFAR (%)	Database	Platform	Extra Enhancement Method
Proposed	**0.20 (DPR)**	**0.50**	**CASIA-IrisV4-Syn**	**MPSoC**	**Error-Correction using LDPC**
Liu-Jimenez *et al.* [9]	12	-	ICE 2005	PC+FPGA	
Liu-Jimenez *et al.* [10]	12	>2	ICE 2005	PC+FPGA	
Gong *et al.* [43]	0.3 - 0.8	0.7 - 2.1	-	ARM	Multi-spectral image capture
Kunik *et al.* [44]	0.26	-	-	Raspberry Pi	
Adamovic *et al.* [3]	1.26	-	CASIA	PC	RS codes
Sim *et al.* [21]	-	1	UBIRIS v.2	PC	Iris+Face
Li *et al.* [45]	-	0.9	-	PC	LDPC(255,45)
Nedjah *et al.* [37]	6.39	-	CASIA-IrisV4-Internal	-	
Marino *et al.* [46]	-	9.67	CASIA	-	
Moi *et al.* [47]	-	26	CASIA-IrisV1	-	
Moi *et al.* [48]	-	2.92	CASIA-IrisV1	-	RS codes
Seetharaman *et al.* [38]	2.44(RS) 0.41(LDPC)	-	CASIA-IrisV3	-	RS or LDPC codes
Feng Zhu *et al.* [49]	0.5 - 1	0.6 - 1	UBIRIS v.1	PC	Hadamard codes
Y. Cheng *et al.* [4]	-	1.81	CASIA-LampV4	PC	CNN, Hadamard codes

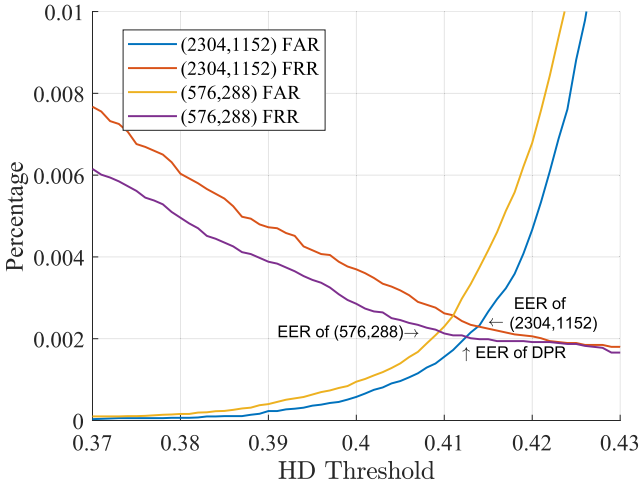


FIGURE 9. EER comparison.

TABLE 2. System performance for biometric key.

Error Correction Code Type	Key Length (bit)	ZeroFAR (%)
Our proposed QC-LDPC(576,288)	**288**	**0.61**
RS(127,10) [3]	200	1.26
RS(127,36) [5]	252	7
LDPC [7]	256	2

design. The QC-LDPC (576, 288) was employed and the key insertion and key recovery modules were activated using the method in Section III.F.

Table. 2 displays the results for generation of biometric keys in a comparison of other state-of-arts. Our proposed architecture performs best among all four designs, considering of key sizes, 288bits, and FRR when FAR equals 0 (0.61%). It is important to be noted that [3] also applied an interleaving module to improve their performance. More buffers and memory spaces must be also implemented in such a system to support the functionality of the interleaving. However, our proposed design leveraged the advance of QC-LDPC codes and achieved a more simplified and higher performance system.

TABLE 3. Utilization for synthesized QC-LDPC decoders.

	(576,288)	(2304,1152)	DPR Overhead
Q bits	32	32	-
BRAM	0 (0%)	0 (0%)	17(5.4%)
FF	12847(2.8%)	12732(2.8%)	2164(0.5%)
LUT	41531(18.0%)	46616(20.2%)	7878(3.4%)
Latency per block of iris codes	56.6us @ 100MHz	158us @ 100MHz	-
Dynamic power	677mW	782mW	133mW

C. FPGA IMPLEMENTATION RESULTS

The proposed heterogeneous platform design is implemented on a single SoC, including a microprocessor section and a programmable logic section. Each section of the system was implemented and verified individually. The microprocessor section with iris image processing algorithms and the FPGA section with QC-LDPC decoders are interconnected by high-speed on-chip buses. QC-LDPC decoders were implemented using Hardware Description Language (HDL). Table 3 shows the synthesized results of the QC-LDPC decoders as the major modules of the whole system. The overall clock frequency of QC-LDPC decoders was 100MHz. In addition to each of the QC-LDPC decoders, the overhead caused by DPR is also shown in Table 3. In order to meet the DPR's requirements, what we implement includes but is not limited to a lightweight soft core microprocessor to control the DPR workflow, buffers, such as FIFOs, around decoders and memory controllers, which are standing on [40]. Dynamic power consumption of both decoders and DPR modules are also displayed individually. It can be seen that the longer QC-LDPC code decoder consumes more energy than the short code, as the longer one is more complex. The DPR overhead costs an approximately 16% to 17% of a QC-LDPC decoder. However, this hardware cost is fixed as the number of decoders scales up or down.

V. CONCLUSION

The main aim of this research is to build a robust and reliable iris verification platform. Hence, we presented a multi-mode QC-LDPC code enhanced iris authentication system based

on a hybrid Microprocessor-FPGA platform. The QC-LDPC codes are used for acceptance rate improvement, cryptographic data generation and recovery purposes. A comprehensive analysis of selecting the most appropriate QC-LDPC codes for the proposed platform was conducted. In this project, we focused on evaluating the feasibility of QC-LDPC codes for this iris recognition system. We choose QC-LDPC (576.288), QC-LDPC (2304,1152) in IEEE 802.16e rather than other codes. It is because this set of codes have been proven to be efficient for implementation. The hardware resources, power and latency caused by the QC-LDPC codes are calculated as well. In this manner, a low EER (up to 0.23% contributed by (2304,1152)) and ZeroFAR were both achieved. Furthermore, with DPR applied in the proposed design, a time-division multiple-access scheme for more than one QC-LDPC decoder is attained. Thus, another QC-LDPC decoder, when necessary, can be used to generate and validate cryptographic keys. It can avoid an impostor's access if a stolen iris image is provided. The generated key length was up to 288 bits per iris. Furthermore, using the DPR real-time approach can achieve a lower EER(0.2%) if the two QC-LDPC codes we propose are combined. Because the overhead caused by DPR is fixed, the limited side effect can be omitted when more QC-LDPC codes or other error correction codes are required to fulfill more complex scenarios in the proposed architecture, such as power-sensitive, rapid response or cancelable iris template requirements. At present, our work has demonstrated the feasibility of integrating a dedicated hardware module, QC-LDPC decoders on the FPGA, in conventional iris authentication systems (microprocessor-based). Such a hybrid combination holds a significant potential for access control systems and even handheld devices related to iris authentication technology.

ACKNOWLEDGMET

Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the authors and do not necessarily reflect those of ES Ltd.

REFERENCES

[1] Research and Markets. (2021). *Global Iris Recognition Market Research Report 2021–2026*. [Online]. Available: https://www.prnewswire.com/news-releases/global-iris-recognition-market-research-report-2021-2026—booming-demand-for-smart-devices-to-play-a-key-role-in-market-development-301344116.html

[2] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, Sep. 2006.

[3] S. Adamovic, M. Milosavljevic, M. Veinovic, M. Sarac, and A. Jevremovic, "Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics," *IET Biometrics*, vol. 6, no. 2, pp. 89–96, Mar. 2017.

[4] Y. Cheng, Y. Liu, X. Zhu, and S. Li, "A multiclassification method for iris data based on the Hadamard error correction output code and a convolutional network," *IEEE Access*, vol. 7, pp. 145235–145245, 2019.

[5] F. Kausar, "Iris based cancelable biometric cryptosystem for secure healthcare smart card," *Egyptian Informat. J.*, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1110866521000049, doi: 10.1016/j.eij.2021.01.004.

[6] M. Baldi, M. Bianchi, F. Chiaraluce, J. Rosenthal, and D. Schipani, "On fuzzy syndrome hashing with LDPC coding," in *Proc. 4th Int. Symp. Appl. Sci. Biomed. Commun. Technol.*, 2011, p. 24.

[7] X. Dong, Z. Jin, L. Zhao, and Z. Guo, "BioCanCrypto: An LDPC coded bio-cryptosystem on fingerprint cancellable template," in *Proc. IEEE Int. Joint Conf. Biometrics (IJCB)*, Aug. 2021, pp. 1–8.

[8] H. T. Ngo, R. N. Rakvic, R. P. Broussard, and R. W. Ives, "Resource-aware architecture design and implementation of Hough transform for a real-time iris boundary detection system," *IEEE Trans. Consum. Electron.*, vol. 60, no. 3, pp. 485–492, Aug. 2014.

[9] J. Liu-Jimenez, R. Sanchez-Reillo, and B. Fernandez-Saavedra, "Iris biometrics for embedded systems," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 19, no. 2, pp. 274–282, Feb. 2009.

[10] J. Liu-Jimenez, R. Sanchez-Reillo, A. Lindoso, and O. Miguel-Hurtado, "FPGA implementation for an iris biometric processor," in *Proc. IEEE Int. Conf. Field Program. Technol.*, Dec. 2006, pp. 265–268.

[11] J. Tian, J. Lin, and Z. Wang, "A 21.66 Gbps nonbinary LDPC decoder for high-speed communications," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 65, no. 2, pp. 226–230, Feb. 2018.

[12] V. L. Petrović, M. M. Marković, D. M. El Mezeni, L. V. Saranovac, and A. RadoÅİević, "Flexible high throughput QC-LDPC decoder with perfect pipeline conflicts resolution and efficient hardware utilization," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 67, no. 12, pp. 5454–5467, Dec. 2020.

[13] M. Kalya and S. Kumar, "Low complexity LDPC error correction code for modified Anderson PUF to improve its uniformity," in *Proc. Int. Conf. Smart Electron. Commun. (ICOSEC)*, Sep. 2020, pp. 997–1002.

[14] C.-W. Sham, X. Chen, W. M. Tam, Y. Zhao, and F. C. M. Lau, "A layered QC-LDPC decoder architecture for high speed communication system," in *Proc. IEEE Asia–Pacific Conf. Circuits Syst.*, Dec. 2012, pp. 475–478.

[15] Q. Lu, Z. Shen, C.-W. Sham, and F. C. M. Lau, "A parallel-routing network for reliability inferences of single-parity-check decoder," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Oct. 2015, pp. 127–132.

[16] L. Ma and C. W. Sham, "Optimized layer architecture for layered LDPC code decoder," in *Proc. Int. Conf. Adv. Technol. Commun. (ATC)*, Oct. 2018, pp. 287–291.

[17] Y. Liu, W. Tang, and D. G. M. Mitchell, "Efficient implementation of a threshold modified min-sum algorithm for LDPC decoders," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 9, pp. 1599–1603, Sep. 2020.

[18] C.-W. Sham, X. Chen, F. C. M. Lau, Y. Zhao, and W. M. Tam, "A 2.0 Gb/s throughput decoder for QC-LDPC convolutional codes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 60, no. 7, pp. 1857–1869, Jul. 2013.

[19] Q. Lu, J. Fan, C.-W. Sham, W. M. Tam, and F. C. M. Lau, "A 3.0 Gb/s throughput hardware-efficient decoder for cyclically-coupled QC-LDPC codes," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 1, pp. 134–145, Jan. 2016.

[20] M.-R. Li, W.-X. Chu, H.-C. Lee, and Y.-L. Ueng, "An efficient high-rate non-binary LDPC decoder architecture with early termination," *IEEE Access*, vol. 7, pp. 20302–20315, 2019.

[21] S. Hiew Moi and P. Yee Yong, "A modified Reed Solomon error correction codes for multimodal biometrics recognition," in *Proc. 3rd Int. Conf. Control, Autom. Robot. (ICCAR)*, Apr. 2017, pp. 418–422.

[22] L. Ma and C. W. Sham, "Iris recognition system implementation improved by QC-LDPC codes," in *Proc. IEEE 2nd Global Conf. Life Sci. Technol. (LifeTech)*, Mar. 2020, pp. 88–99.

[23] L. Ma, X. Zhong, C. W. Sham, and C. Y. Lo, "An iris recognition system implementation with error correction capability by reusing WiFi standard LDPC codes," in *Proc. IEEE 9th Global Conf. Consum. Electron. (GCCE)*, Oct. 2020, pp. 265–267.

[24] L. Ma, C.-W. Sham, C. Y. Lo, and X. Zhong, "An embedded iris recognition system optimization using dynamically reconfigurable decoder with LDPC codes," 2021, *arXiv:2107.03688*.

[25] R. Peesapati, S. Das, S. Baldev, and S. R. Ahamed, "Design of streaming deblocking filter for HEVC decoder," *IEEE Trans. Consum. Electron.*, vol. 63, no. 3, pp. 1–9, Aug. 2017.

[26] P.-H. Lee, H.-Y. Lee, Y.-W. Kim, H.-Y. Hong, and Y.-C. Jang, "A 10-Gbps receiver bridge chip with deserializer for FPGA-based frame grabber supporting MIPI CSI-2," *IEEE Trans. Consum. Electron.*, vol. 63, no. 3, pp. 209–215, Aug. 2017.

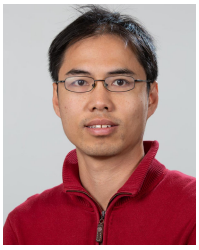
[27] M. J. Garrido, F. Pescador, M. Chavarrías, P. J. Lobo, and C. Sanz, "A high performance FPGA-based architecture for the future video coding adaptive multiple core transform," *IEEE Trans. Consum. Electron.*, vol. 64, no. 1, pp. 53–60, Feb. 2018.

[28] J. Khurana, Q. Hall, and G. Malipeddi, "Kria K26 SOM: The ideal platform for vision AI at the edge," Xilinx, San Jose, CA, USA, Tech. Rep. WP529, 2021. [Online]. Available: https://www.xilinx.com/support/documentation/white_papers/wp529-som-benchmarks.pdf

[29] A. Martínez-Rodrigo, B. García-Martínez, Á. Huerta, and R. Alcaraz, "Detection of negative stress through spectral features of electroencephalographic recordings and a convolutional neural network," *Sensors*, vol. 21, no. 9, p. 3050, Apr. 2021.
[30] Altera, "White paper FPGAs enable energy-efficient motor control in next-generation smart home," Altera Corp., San Jose, CA, USA, 2008. [Online]. Available: https://www.techonline.com/tech-papers/fpgas-enable-energy-efficient-motor-control-in-next-generation-smart-home-appliances/
[31] C. Rathgeb, A. Uhl, P. Wild, and H. Hofbauer, "Design decisions for an iris recognition SDK," in *Handbook of Iris Recognition*, K. W. Bowyer and M. J. Burge, Eds. London, U.K.: Springer, 2016, pp. 359–396, doi: 10.1007/978-1-4471-6784-6_16.
[32] D. J. C. Mackay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," *Electron. Lett.*, vol. 32, no. 18, p. 1645, 1996.
[33] J. Daugman, "The importance of being random: Statistical principles of iris recognition," *Pattern Recognit.*, vol. 36, no. 2, pp. 279–291, 2003.
[34] J. Daugman, "How iris recognition works," in *The Essential Guide to Image Processing*. Amsterdam, The Netherlands: Elsevier, 2009, pp. 715–739.
[35] L. Masek, "Recognition of human iris patterns for biometric identification," Ph.D. dissertation, Univ. Western Australia, Perth, WA, Australia, 2003.
[36] J. G. Daugman, "Uncertainty relation for resolution in space, spatial frequency, and orientation optimized by two-dimensional visual cortical filters," *J. Opt. Soc. Amer. A, Opt. Image Sci.*, vol. 2, no. 7, pp. 1160–1169, 1985.
[37] N. Nedjah, R. S. Wyant, L. M. Mourelle, and B. B. Gupta, "Efficient yet robust biometric iris matching on smart cards for data high security and privacy," *Future Gener. Comput. Syst.*, vol. 76, pp. 18–32, Nov. 2017.
[38] K. Seetharaman and R. Ragupathy, "LDPC and SHA based iris recognition for image authentication," *Egyptian Informat. J.*, vol. 13, no. 3, pp. 217–224, Nov. 2012.
[39] S. S. Haykin, *Digital Communications*. New York, NY, USA: Wiley, 1988.
[40] L. Ma, C.-W. Sham, J. Sun, and R. Valencia Tenorio, "A real-time flexible telecommunication decoding architecture using FPGA partial reconfiguration," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 10, pp. 2149–2153, Oct. 2020.
[41] S. Thavalengal, I. Andorko, A. Drimbarean, P. Bigioi, and P. Corcoran, "Proof-of-concept and evaluation of a dual function visible/NIR camera for iris authentication in smartphones," *IEEE Trans. Consum. Electron.*, vol. 61, no. 2, pp. 137–143, May 2015.
[42] R. Špetlík and I. Razumenić, "Iris verification with convolutional neural network and unit-circle layer," in *Pattern Recognition*, G. A. Fink, S. Frintrop, and X. Jiang, Eds. Cham, Switzerland: Springer, 2019, pp. 274–287.
[43] Y. Gong, D. Zhang, P. Shi, and J. Yan, "High-speed multispectral iris capture system design," *IEEE Trans. Instrum. Meas.*, vol. 61, no. 7, pp. 1966–1978, Jul. 2012.
[44] Z. Kunik, A. Bykowski, T. Marciniak, and A. Dabrowski, "Raspberry pi based complete embedded system for iris recognition," in *Proc. Signal Process., Algorithms, Architectures, Arrangements, Appl. (SPA)*, Sep. 2017, pp. 263–268.
[45] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian, "An effective biometric cryptosystem combining fingerprints with error correction codes," *Expert Syst. Appl.*, vol. 39, no. 7, pp. 6562–6574, Jun. 2012.
[46] R. Mariño, F. H. Álvarez, and L. H. Encinas, "A crypto-biometric scheme based on iris-templates with fuzzy extractors," *Inf. Sci.*, vol. 195, pp. 91–102, Jul. 2012.
[47] S. H. Moi, N. B. A. Rahim, P. Saad, P. L. Sim, Z. Zakaria, and S. Ibrahim, "Iris biometric cryptography for identity document," in *Proc. Int. Conf. Soft Comput. Pattern Recognit.*, 2009, pp. 736–741.
[48] S. H. Moi, P. Saad, N. A. Rahim, and S. Ibrahim, "Error correction on IRIS biometric template using Reed Solomon codes," in *Proc. 4th Asia Int. Conf. Math./Anal. Modelling Comput. Simulation*, May 2010, pp. 209–214.
[49] F. Zhu, P. Shen, and C. Chen, "A performance-optimization method for reusable fuzzy extractor based on block error distribution of iris trait," in *Security and Privacy in Communication Networks*, S. Chen, K.-K. R. Choo, X. Fu, W. Lou, and A. Mohaisen, Eds. Cham, Switzerland: Springer, 2019, pp. 259–272.

LONGYU MA received the B.Eng. degree in electronic and information engineering from Harbin Engineering University, China, in 2010, and the M.Eng. degree in integrated circuit engineering from Shanghai Jiao Tong University, China, in 2016. He is currently pursuing the Ph.D. degree in computer science with The University of Auckland, New Zealand.

His research interests include integrate-circuit-level optimization for error correction codes, such as LDPC codes, error-correction for iris recognition and joint source-channel coding LDPC hardware implementation.



CHIU-WING SHAM (Senior Member, IEEE) received the bachelor's (computer engineering), M.Phil., and Ph.D. degrees from The Chinese University of Hong Kong, in 2000, 2002, and 2006, respectively. He began his research work on digital design during the final year project as an undergraduate which focused on improving the performance, reducing the logic complexity of the systems, and power consumption. He has worked as an Electronics Engineer on the FPGA applications of a motion control systems and system security with cryptography at ASM Pacific Technology Ltd., Hong Kong. During his years at The Hong Kong Polytechnic University, he has also engaged in various university projects for the commercialization of technology, in particular a few optical communication projects which are in collaboration with Huawei. He also worked on the physical design of VLSI design automation. He was invited to work at Synopsys Inc., Shanghai, in Summer 2005, as a Visiting Research Engineer. He is currently working as a Senior Lecturer with The University of Auckland. He received the Best Paper Award in ISQED 2013 and the Best Paper Award in ATC 2015.

CHUN YAN LO received the B.Eng. degree in electronic and information engineering from The Hong Kong Polytechnic University, in 2018. He is currently pursuing the Ph.D. degree in computer science with The University of Auckland, Auckland, New Zealand. His research interests include the convolutional neural networks, hardware acceleration, and digital design.

XINCHAO ZHONG received the B.S. and M.S. degrees in electrical engineering from Tsinghua University, Beijing, China, in 1997 and 2001, respectively. He is currently pursuing the Ph.D. degree in computer engineering with The University of Auckland, New Zealand. He has 20 years of experience in IC design and verification with emphasis on SoC design for wireless communication, RFID, and motor control. His research interests include RISC-V, ARM, mixed signal, and low-power design in SoC.