Towards Practical Privacy-Preserving Processing over Encrypted Data in IoT: An Assistive Healthcare Use Case

Jiang, Linzhi; Chen, Liqun; Giannetsos, Thanassis; Luo, Bo; Liang, Kaitai; Han, Jinguang

Published in:
IEEE Internet of Things Journal

Link to article, DOI:
10.1109/JIOT.2019.2936532

Publication date:
2019

Document Version
Peer reviewed version

Citation (APA):
Jiang, L., Chen, L., Giannetsos, T., Luo, B., Liang, K., & Han, J. (2019). Towards Practical Privacy-Preserving Processing over Encrypted Data in IoT: An Assistive Healthcare Use Case. *IEEE Internet of Things Journal*, *6*(6), 10177-10190. https://doi.org/10.1109/JIOT.2019.2936532

Towards Practical Privacy-Preserving Processing over Encrypted Data in IoT: An Assistive Healthcare Use Case

Linzhi Jiang ✉, Liqun Chen, Thanassis Giannetsos, Bo Luo, Kaitai Liang, *Member, IEEE,* and Jinguang Han, *Senior Member, IEEE,*

***Abstract*—With the advancement of Internet of Things (IoT), a large number of electronic devices are connected to the Internet. These connected electronic devices acquire, transmit information and respond to any received actions. In medical ecosystem, hospitals can implement medical diagnosis with medical sensors, especially for remote auxiliary medical diagnosis. But, in this context, patients privacy is paramount importance, and confidentiality of medical data is crucial. Therefore, the main challenge ahead is how to realize remote auxiliary medical diagnosis while protecting confidentiality of the medical data and ensuring patients privacy. In this paper, based on somewhat homomorphic encryption (SHE) scheme addressed by Junfeng Fan and Frederik Vercauteren (FV), we provide the first instance of a new efficient SHE scheme for homomorphic evaluation over Single Instruction Multiple Data (SIMD). We also implement a new set of efficient SIMD homomorphic comparison and division schemes. Based on these findings, we implement efficient privacy-preserving and SIMD homomorphic surf and multi-retina-image matching schemes. Offered functionalities include SIMD homomorphic feature point detection, multi-retina-image matching and lesion detection for the encrypted retinal image of diabetic retinopathy. Finally, we provide a proof-of-concept application implementation towards remote auxiliary diagnosis systems for diabetes in order to showcase the core security and privacy pillars of our solution. In the meantime, our IoT system designed with lattice-based cryptography preserves data confidentiality under quantum computation and quantum computers.**

***Index Terms*—Somewhat homomorphic encryption, Surf algorithm, Internet of Things, Medical diagnosis.**

I. Introduction

INTERNET of Things (IoT) [1] is a very large network connecting every electronic device all over the world, and this emerging trend is currently changing the communication landscape. By connected house appliances, users enjoy convenient and intelligent services of life [2]. Connected sensors, such as humidity sensors, temperature sensors, light sensors and so on, can realize automatic and intelligent industrial manufacturing and agricultural cultivation [3]. Sensors in the vehicles [4] can sense status of vehicles and roads in real time. In hospitals, doctors can utilize sensors to monitor patients in real time too [5] [6]. Sensors can also be used for auxiliary disease diagnosis and treatment remotely [7] [8] [9].

But, transmission, storage and utilization of the data acquired from sensors of IoT involve in data confidentiality and users privacy [10] [11] [12]. With the acquired data from sensors in a house, the malicious attackers can control and take advantage of house appliances, and even spy users life. Egregious attacks can destroy industrial and agricultural production, and so far as to threat users life in intelligent driving. For industrial and agricultural users, commercial competitors can fulfill attacks to sensors to destroy industrial and agricultural production of their competitors. In the field of intelligent driving, once attackers acquire data of your vehicle sensors, they can not only obtain driving states and tracks of your vehicle, but also cause malicious traffic accident by controlling vehicle sensors.

Especially, in the health and medical ecosystems, patients health condition and medical information, which can only be accessed by their attending physicians, are sensitive (e.g. Acquired Immune Deficiency Syndrome (AIDS), Hepatitis, Cardiopathy, Diabetes, etc.). The leak of sensitive health condition and medical information would cause great distress and discrimination against patients, and indeed affect their treatment, work and life[13]. To protect data confidentiality and patients privacy, we can utilize traditional encryption schemes to encrypt all of data acquired from medical sensors. Encrypted data from the medical sensors is transmitted and stored in IoT.

Nonetheless, the traditional encryption schemes can not support direct computational operation for the encrypted data [14], such as the Advanced Encryption Standard scheme (AES), the Triple Data Encryption Algorithm (DEA), the Elliptic Curve Integrated Encryption Scheme (ECIES), etc. [15] [16] [17]. After acquiring encrypted patients medical data by the medical sensors, doctors decrypt the encrypted medical data, and do with the decrypted medical data to make a diagnosis for patients diseases. Another case is that doctors want to make full use of a cloud server for the auxiliary diagnosis to reduce their heavy workloads. When doctors use a cloud server to perform auxiliary diagnosis with machine leaning algorithms, a cloud server firstly decrypts the encrypted medical data ac-

Linzhi Jiang is with Guilin University of Electronic Technology, China; and the Surrey Centre for Cyber Security, University of Surrey, UK. E-mail: linzjiang@hotmail.com, linzhi.jiang@surrey.ac.uk.

L. Chen and K. Liang are with the Surrey Centre for Cyber Security, University of Surrey, UK.

Thanassis Giannetsos is with the Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark.

Bo Luo is with Department of Electrical Engineering and Computer Science, University of Kansas, Lawrence, KS.

J. Han is with the Centre for Secure Information Technologies (CSIT), Institute of Electronics, Communications and Information Technology (ECIT), Queens University Belfast, Belfast, Northern Ireland, BT3 9DT, United Kingdom.

quired from medical sensors, and then utilizes the decrypted medical data and machine learning algorithms to perform efficient auxiliary diagnosis directly. Neither of both cases preserves data confidentiality from the medical sensors, because the medical data is decrypted when performing medical diagnosis. Therefore, there is the possibility of breaching patients privacy.

And all the time, the rapid development of quantum computation and computer heralds the advent of the era of quantum computation [18], while traditional encryption schemes are not quantum-resistant encryption schemes, such as Triple DEA, ECIES, Paillier, etc. [19] [20]. In order to perform the auxiliary diagnosis with encrypted data and machine learning schemes via a cloud server, and protect users privacy at the era of quantum computation, an efficient quantum-resistant homomorphic encryption scheme is one of the best options.

Motivation & contributions: A cloud server has powerful computation and storage capabilities. With a cloud server, doctors can utilize medical data from sensors and machine learning algorithms to perform efficient auxiliary diagnosis to reduce their heavy workloads. Simultaneously, patients living in the remote areas can also hold high levels of disease diagnosis. In order to preserve data confidentiality from medical sensors and patients privacy, and avail of a cloud server to complete auxiliary diagnosis with machine leaning algorithms over encrypted medical data, we propose a secure and efficient medical diagnosis system, which can carry out the following functionalities: (1) High efficient and complex homomorphic evaluation. Efficiency of encryption scheme is very important for tiny appliance of IoT (e.g. fast encryption and decryption, low storage and communication cost, efficient homomorphic evaluation, etc.). Image processing and machine learning algorithms require complex homomorphic evaluation, such as homomorphic comparison and division over the encrypted data. Our designed homomorphic encryption scheme supports small encryption key and encrypted image size, low communication cost, efficient and complex homomorphic evaluation. (2) Homomorphic image processing and machine learning. In our medical IoT system, all computations are performed with homomorphic evaluation. A doctor can directly utilize a cloud server to perform auxiliary medical diagnosis by homomorphic image processing and machine learning. This greatly reduces doctors workloads, and improves the diagnosis efficiency of doctors and service capability of hospitals. (3) Quantum Resistance. Quantum computation model makes many hard problems (in classical computation) used in cryptography not to be hard. The quantum computer would render all widely used traditional encryption schemes insecure [21]. Our homomorphic encryption scheme based on lattice is quantum resistance. All of the medical data in our IoT system is also secure under the quantum computation model and a quantum computer. Medical data can be securely transmitted and stored in our IoT system for a long time.

To realize above functionalities, we use somewhat homomorphic encryption (*SHE*) proposed by Junfeng Fan and Frederik Vercauteren (*FV*) as the basic encryption scheme [22]. The *FV* scheme is based on ideal lattice (quantum resistance), and has small public key. In the meantime, we employ Single Instruction Multiple Data (*SIMD*) to pack multi-bits into a single ciphertext, and perform parallel homomorphic evaluation. Packing technology can compress ciphertext for transmission and storage. Parallelism improves the efficiency of homomorphic evaluation. With the help of above optimized *FV* scheme, we design the new efficient homomorphic comparison and division schemes. Homomorphic comparison scheme has low communication cost between two parties. Utilizing above our designed homomorphic schemes, a cloud server can implement medical image processing (*SIMD* is very efficient for image processing [23]) and machine learning about auxiliary medical diagnosis over the encrypted medical data.

Our IoT system acquires patients retinal images of diabetic retinopathy (*DR*) by the camera sensor connected to a Raspberry Pi (*RP*) [24]. The acquired retinal images are encrypted with our homomorphic encryption in a *RP*. The encrypted retinal images are transmitted in our IoT system, and stored in a cloud server, which performs efficient auxiliary diabetes diagnosis. We proved that our IoT system is the known plaintext attack (*KPA*) [25] and the ciphertext only attack (*COA*) [26] security in *honest-but-curious* [25]. *KPA* security is an attack, in which an attacker has samples of both the plaintext and corresponding ciphertext. An attacker conducts an analysis with samples of both the plaintext and corresponding ciphertext to get the secret key used to encrypt and decrypt the information. *COA* security is an attack, in which an attacker has only the knowledge of ciphertext. An attacker conducts an analysis ciphertext to get the secret key used to encrypt and decrypt the information. The *honest-but-curious* model is a secure computation (or a protocol), where attackers are restricted to follow all of the computation steps (or a protocol), but after implementing computation steps (or a protocol), they may analyze the data they have received to try to recover inputs. In our IoT system, encrypted retinal images of *DR* are just like in a black box. Homomorphic image processing and machine learning algorithms can not reveal image content and diagnostic results. A good balance about storage overhead, communication cost, computational efficiency and privacy protection is achieved by our IoT system.

The rest of this paper is organized as follows: Sec. II presents our system model & threat model. Then, we provide security and privacy requirements of our system in Sec. III. In Sec. IV, we describe preliminaries and related work before providing system architecture in Sec. V. Then, in Sec. VI, the detailed system scheme is offered. Next, We give out the detailed security and privacy analysis of our system in Sec. VII, and describe system performance evaluation in Sec. VIII. Finally, we provide conclusion of the paper in Sec. XI.

II. System Model & Threat Model

In this section, we present our system model & threat model.

A. System Model

Our IoT system implements privacy-preserving auxiliary diabetes diagnosis with sensors as showed in Fig. 1. Our system model includes the following constituent elements:

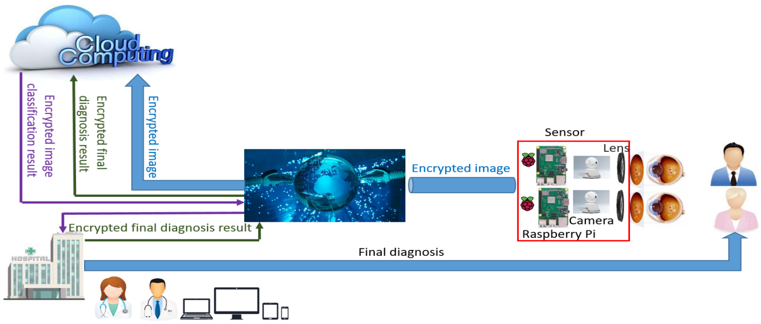

Cloud Computing
Encrypted image classification result
Encrypted final diagnosis result
Encrypted image
Encrypted image
Sensor
Lens
Camera
Raspberry Pi
Encrypted final diagnosis result
Final diagnosis
HOSPITAL

Fig. 1. System model-Homomorphic diabetes diagnosis over the encrypted retinal image of diabetic retinopathy.

Patient (P_i) **and Sensor** (S_i): P_i is a potential diabetic patient. Camera (Raspberry Pi Noir Camera V2), a handheld condensing lens and *RP* constitute a sensor (S_i), which acquires patients retinal images of *DR* [27] and encrypt them.

Cloud Server (***CS***): *CS* implements data storage, homomorphic retinal image processing and machine learning over the encrypted retinal images of *DR*. Data storage includes the encrypted retinal images of *DR*, the encrypted training dataset (the retinal images of *DR*), the intermediate and final homomorphic evaluation results about the retinal image processing of *DR* and machine learning over the encrypted training dataset, the trained machine leaning model, the classification of retinal images of *DR* and doctors final diagnostic results. Homomorphic retinal image processing of *DR* includes homomorphic feature extraction and feature points matching over the encrypted retinal images of *DR*. Homomorphic machine learning includes homomorphic machine learning model training and the retinal image classification of *DR* with the trained machine learning model.

Hospital (*H*) and Doctor (D_i): *H* has a certificate authority (*CA*) center (in hospital's server group), which issues digital certificates to certificate ownership of public key. S_i makes use of certificated public key to encrypt retinal images of *DR*. D_i makes final diagnosis based on acquired retinal images of *DR* and classification results with machine learning model by *CS*. Doctors final diagnostic results are encrypted and uploaded to *CS* by *H*. P_i receives the final diagnostic result from *H*.

B. Threat Model

Our IoT system preserves confidentiality of the retinal images of *DR* and patients privacy [28]. In our threat model, we mainly consider the following threats:

1) Threats to confidentiality of the retinal images of *DR*. Threats to confidentiality of the retinal images of *DR* mainly comes from the security of our *SIMD* homomorphic encryption scheme, encrypted data transmission, storage and processing of the encrypted retinal images of *DR* in our IoT system. Malicious attackers can use the quantum computation model (or a quantum computer) to analysis and attack the encryption scheme. In the process of encrypted data transmission, a malicious attacker can eavesdrop and obtain the encrypted data. A portable device (a sensor in our IoT system), doctors computers and a cloud server store the encrypted data and homomorphic evaluation results over the encrypted data. A cloud service provider, a portable device provider, a computer provider and a malicious attacker can obtain the encrypted data.

2) Cloud server is *honest-but-curious*. *CS* can also keep detailed record of each operation and the result of each operation performed by our schemes in our IoT system. *CS* may want to recover the plaintext of the encrypted data, and reveal content of images of *DR* and the final diagnostic results. Especially, in the *honest-but-curious* model [25], *CS* can correctly perform all the schemes in our IoT system. In the meanwhile, *CS* takes advantage of all the operating recordings and acquired encrypted data to perform analysis for the benefit of a cloud service provider.

III. Security and Privacy Requirements

In this section, we provide the security and privacy requirements of our IoT system for the data confidentiality and patients privacy. The security and privacy requirements include the following aspects:

Data Confidentiality (*DC*): In our IoT system, patients retinal images of *DR* are transmitted and stored at different devices (*CS*, S_i, *H's* servers, and doctors computers). The encrypted retinal images of *DR* for transmission and storage can not be broken by the quantum computation model (or a quantum computer), because our IoT system uses our quantum-resistant homomorphic encryption scheme. Therefore, the encrypted data stored in *CS*, *H's* servers, S_i and doctors computers can not reveal contents of retinal images of *DR* for patients.

Homomorphic retinal image processing of *DR* in our IoT system can not reveal contents of retinal images of *DR*, including the pixel value, the feature point location and the extracted feature vectors. In the meantime, homomorphic machine learning can not reveal the classification results of retinal images of *DR*. The reason of getting above results is that image processing and machine learning are implemented with homomorphic evaluation based on ideal lattice over encrypted data. The hospital internal data interaction makes use of authentic & secure channel between the *H's* servers and doctors computers [29] [30], so it can not reveal contents of retinal images of *DR*.

Because our *SIMD SHE* scheme is malleable [31] [32], tamper attacks about encrypted data transmission and storage are not considered for security in our IoT system.

Patients Privacy (*PP*): Retinal images of *DR* contain patients medical information. In our IoT system, transmission and storage of the encrypted medical images can not reveal contents of the retinal images of *DR*. During homomorphic image processing and image classification with machine learning, the *CS* and *H's* servers can not reveal any information of the retinal images of *DR* too. During the auxiliary diagnosis with a S_i, a *CS* and *H's* servers, the retinal images of *DR* stored in a S_i, a *CS* and *H's* servers are encrypted by our homomorphic encryption. Any information of the retinal images of *DR* can not be revealed by a S_i, a *CS* and *H's* servers. For doctors final diagnosis, *H's* servers and doctors computers preserve security of diagnostic result by authentic & secure channel [29] [30]. Patients privacy is protected during hospital's internal data interaction. Hence, patients privacy is protected in the whole diagnostic processing.

IV. Preliminaries and Related work

In this section, we present somewhat homomorphic encryption (*SHE*), Speed up Robust Features (*Surf*) (feature extraction of a medical image) and machine learning schemes. These schemes are basis to construct our efficient IoT system.

A. SHE Scheme

Homomorphic encryption includes partially homomorphic encryption (*PHE*), *SHE* and fully homomorphic encryption (*FHE*) schemes. *PHE* only supports multiplicative homomorphic evaluation (eg. *RSA* [31]) or additive homomorphic evaluation (eg. *Paillier* [32]). To construct a *FHE* scheme, we firstly construct a *SHE* scheme, which supports a certain number of additive and multiplicative homomorphic evaluation. When adding a bootstrapping operation to a *SHE* scheme, we can convert it into a *FHE* scheme. Based on ideal lattice, Gentry proposes the first *FHE* scheme [33] [34] in 2009. A *FHE* scheme supports any times of additive and multiplicative homomorphic evaluation simultaneously. The *FHE* scheme from ring learning with errors (*Rlwe*) [35-42] is more efficient than the *FHE* scheme from learning with errors (*Lwe*). But, a FHE scheme with bootstrapping is inefficient.

A *SHE* scheme based on *Rlwe* is more efficient than a *FHE* scheme based on *Lwe*. In the scheme [41], authors compare *SHE FV* scheme [22] with Yet Another Somewhat Homomorphic Encryption (*YASHE*) scheme [42]. In the scheme [43], a SHE scheme (*BGV*) presented by Brakerski, Gentry and Vaikuntanathan [37] is compared with *YASHE* scheme [42]. The *SHE FV* scheme has smaller ciphertexts than the *BGV* scheme. We choose *SHE FV* scheme as our basic encryption scheme. Let $\tilde{E}$ be the *SHE FV* scheme, and $m_i (i = 1, 2)$ be the plaintext. For $\mathbf{c}_1$ and $\mathbf{c}_2$ ($\mathbf{c}_1 = \tilde{E}(m_1)$ and $\mathbf{c}_2 = \tilde{E}(m_2)$), *SHE FV* scheme can get the following results: $c_{Add} = [\mathbf{c}_1 + \mathbf{c}_2]_q = \tilde{E}(m_1 + m_2)$ and $c_{Mult} = [\mathbf{c}_1 \cdot \mathbf{c}_2]_q = \tilde{E}(m_1 \cdot m_2)$. The scheme details are introduced in Supplement A.

B. Surf Scheme

Bay H, et al. [44] present *surf* scheme, which uses the Hessian matrix-based measure for the detector and a distribution based descriptor. Hessian matrix utilizing box filters simplifies computation of feature point detection. Distribution-based description of feature point also simplifies computation of descriptor. *Surf* scheme can realize real-time image feature detection, and becomes more efficient than scale invariant feature transform (*Sift*) algorithm [45] [46] [47]. The scheme details are introduced in Supplement B. The main computation steps of *surf* scheme are as follows:

Conversion from Grey Image to Integral Image: We firstly converse grey image ($\tilde{I}$) of image *I* to integral image. The integral image of $\tilde{I}$ in the pixel grid (Ω) is computed as follows: $\forall (x, y)$ (pixel of $\tilde{I}$)$\in$ Ω, the corresponding integral image pixel is:

$$\tilde{\tilde{I}}(x, y) = \sum_{0 \leq i \leq x} \sum_{0 \leq j \leq y} \tilde{I}(x, y).$$

Hessian Matrix Construction and Eigenvalue Computation: Making use of box filters (*BF*), we can complete a simplified approximate computing of Hessian matrix: The convolution of *BF* with the discrete image I can be computed with the integral image $\tilde{\tilde{I}}$: $\forall (x, y) \in \Omega$,

$$\begin{aligned} BF * I(x, y) = \tilde{\tilde{I}}(x - a, y - c) + \tilde{\tilde{I}}(x - b - 1, y - d - 1) \\ -\tilde{\tilde{I}}(x - a, y - d - 1) - \tilde{\tilde{I}}(x - b - 1, y - c). \end{aligned}$$

The first-order partial derivative computing can be approximately completed with *BF* at different scales (*L*):

$$\begin{aligned} BF_x^L &= (BF_{[-\tilde{\ell},-1]\times[-\tilde{\ell},\tilde{\ell}]} - BF_{[1,\tilde{\ell}]\times[-\tilde{\ell},\tilde{\ell}]}) * \tilde{I}, \\ BF_y^L &= (BF_{[-\tilde{\ell},\tilde{\ell}]\times[-\tilde{\ell},-1]} - BF_{[-\tilde{\ell},\tilde{\ell}]\times[1,\tilde{\ell}]}) * \tilde{I}, \end{aligned}$$

where $\tilde{\ell}(L) \in N$.

For the multi-scale computing, the second-order partial derivative computing can be approximately completed with *BF* at different *L*:

$$\begin{aligned} BF_{xx}^L &= (BF_{T_1} - 3BF_{T_2}) * \tilde{I}, \\ BF_{yy}^L &= (BF_{T_3} - 3BF_{T_4}) * \tilde{I}, \\ BF_{xy}^L &= (BF_{T_5} + BF_{T_6} - BF_{T_7} - BF_{T_8}) * \tilde{I}, \end{aligned}$$

where $T_i (i = 1, 2, \cdots, 8)$ is a rectangular domain. Finally, we get determinant approximation of Hessian matrix:

$$det(H_{approx}) = BF_{xx}BF_{yy} - (wBF_{xy})^2.$$

In general, we let $w = 0.9$.

Construction of Gaussian Pyramid and Scalar Space: We make use of Gaussian pyramid to construct the scalar space. Gaussian pyramid is divided into different octaves, which are divided into a lot of levels. Different octaves have the same image size. But, template sizes of *BF* are increased gradually. Different levels of a octave have the same filter, but fuzziness is different.

Feature Point Detection: After constructing scale space with *BF*, we can complete feature point detection as follows:

1) Filtration of feature point. In order to detect saddle points, we utilize scale-normalized determinant of Hessian matrix to complete it as follows:

$$DoH^L(\tilde{I}) = (BF_{xx}BF_{yy} - (\omega BF_{xy}^L)^2)/L^4,$$

where $L = 2^o i + 1, \omega = 0.912$, and o is the octave. Parameter L and ω are separately used for keeping scale invariance and balancing the expression of the determinant of Hessian matrix by *BF*.

2) Feature point selection. We can use 3×3 filters. There are 9 pixel points in each scalar level. With the adjacent upper and lower layers, each pixel point compares with 26 pixel points. Finally, we obtain key points of image. Surf algorithm can set the threshold t_H to eliminate noise perturbation.

3) Refinement of feature point. For a key point $X(x_0, y_0, L_0)$ in the box space, the refined result is $X = X_0 + \zeta$, where $\zeta = (\zeta_x, \zeta_y, \zeta_L)^T = -H_0^{-1} d_0$, d_0 is the discrete gradient, H_0 is the discrete Hessian matrix of $DoH^L(\tilde{I})$. d_0 and H_0 can be computed in the box space.

Feature Point Description: To extract descriptor of a feature point, a square region centred around a feature point is constructed. This region is oriented along the orientation of a feature point, and is divided into 4×4 subregions ($R_{i,j}$). There are 4 values in each subregion. Finally, a 64 dimensional vector $\mu_k = (\mu_k(i,j))_{1<i,j<4}$ is obtained. This is descriptor of a feature point.

C. Machine Learning Scheme

$S = \{(I^{(1)}, I^{(2)}, \cdots, I^{(M)}\}$ is the database for the retinal images of *DR*. $a_{I^{(i)}}^{(1)}, a_{I^{(i)}}^{(2)}, \cdots, a_{I^{(i)}}^{(N_i)}$ is the feature set for the $I^{(i)}$-th retinal image of *DR*. Because pairwise matching for retinal images of *DR* is inefficient, our application implements *multi-image matching scheme* called *multi-image matching* via density-based clustering [48] to classify the retinal images of *DR*. The core part of *multi-image matching* via density-based clustering is *Quick-Match* scheme. It is an efficient data clustering scheme with linear time complexity.

Quick-Match scheme firstly collects and puts all the feature points of retinal images of *DR* ($a_{I^{(i)}}^{(1)}, a_{I^{(i)}}^{(2)}, \cdots, a_{I^{(i)}}^{(N_i)}, i \in \{1, 2, \cdots, M\}$) into a tree. Then, the constructed tree is broken into different clusters, which represent different multi-image matching. We can define a density function DF. Based on density estimation, we can construct the feature point tree. For the given feature point $a_{I^{(s)}}^{(e)}$, the parent node from another image in the tree can be computed by $Parent$ function. Finally, we can break the constructed tree into clusters, which correspond to the multi-image matching. The algorithm is terminated until all the edges are considered. The scheme details are introduced in Supplement C.

V. System Architecture

In this section, we provide our IoT system architecture including a high level overview. Our IoT system architecture contains the following three modules as showed in Fig. 2: encryption scheme, application and management over the encrypted retinal images of *DR*.

A. High Level Overview

Our IoT system mainly performs privacy-preserving auxiliary medical diagnosis through image processing and machine leaning schemes with a cloud service. The execution process is as follows:

1) System starts and calls for the camera connected to *RP* to acquire patients retinal images of *DR*. *RP* calls for the encryption algorithm, performs encryption operation and uploads the encrypted patients retinal images of *DR*.

2) *CS* performs auxiliary medical diagnosis based on homomorphic image processing and machine learning schemes. After finishing medical diagnosis, *CS* stores encrypted diagnostic results and send them to D_i.

3) D_i makes the final medical diagnosis based on the decrypted retinal images of *DR* and classification results returned by *CS*. Then, D_i sends the final encrypted diagnostic results to *H's* servers and *CS*.

4) *H* returns each final encrypted diagnostic result to P_i.

In our IoT system, the acquired patients retinal images of *DR* are encrypted with our efficient and quantum resistant *SIMD SHE* scheme. Image processing and machine learning schemes of diagnosis both perform homomorphic evaluation. The final diagnostic results are also encrypted. No information about patients is revealed during the entire diagnostic process. System preserves data confidentiality and patients privacy.

B. System Architecture

Key Generation and Management (*KGM*): *H* has a server group to perform key generation and distribution, certification and management. *H's* servers generate public key and private key for data encryption, certification and decryption. *H's CA* centre distributes digital certificates for public key, which is used for S_i to execute our *SIMD SHE* scheme. We show this as process ① in our IoT system architecture. At the same time, *H's* servers and doctors computers build secure & authenticated channel for secure data and doctors final diagnosis transmission. We show this as process ⑥ in our IoT system architecture. Such secure & authenticated channel is easy to implement by post-quantum key exchange protocol [49] [50]. This is beyond the scope of our paper.

Medical Image Acquisition and Encryption (*MIAE*): In our IoT system, *H* utilizes S_i and lens to acquire patients retinal images of *DR*. We show this as process ② in our IoT system architecture. S_i holds the public key distributed by *H* with certificated digital certificate. The acquired retinal images are encrypted by S_i with our *SIMD SHE* scheme and the public key. Then, the encrypted retinal images are transmitted in IoT, and are uploaded to *CS*. Process ③ shows this operation.

Medical Image Processing (*MIP*) and Machine Learning: After S_i uploads data, *CS* performs homomorphic feature detection over the encrypted retinal images of *DR*. This operation is completed with our homomorphic *surf* scheme. Process ④ shows this operation. Then, *CS* performs homomorphic machine leaning with the encrypted database (data encrypted with the public key hold by S_i) and the data uploaded by S_i. Finally, *CS* implements homomorphic retinal image classification of *DR*. Process ⑤ shows this operation. The extracted feature over each retinal image of *DR* is encrypted, and the retinal image classification result of *DR* is also encrypted.

Medical Diagnosis (*MD*): The encrypted retinal images of *DR* and their classification results are stored in *CS*. D_i downloads the encrypted retinal images of *DR* and their classification results, and decrypt them. D_i makes a diagnosis with

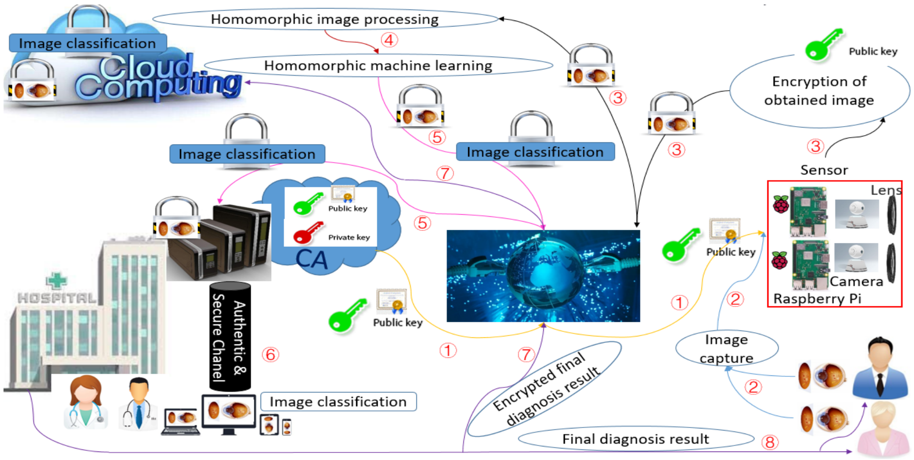


Fig. 2. System model-Homomorphic diabetes diagnosis over the encrypted diabetic retinopathy image.

decrypted retinal images of *DR*, and compare his (or her) diagnostic results with decrypted retinal image classification results of *DR*. In the end, D_i gives the final diagnostic results.

Result Feedback of Medical Diagnosis (*RFMD*): After D_i makes the final diagnosis, D_i encrypts diagnostic results and uploads them to *H's* servers. *H* uploads the final diagnostic results to *CS*, and returns each final diagnostic result to P_i. Process ⑦ and Process ⑧ show these operations.

VI. System Scheme-Privacy-preserving Services

In this section, we firstly present our encoding and *SIMD SHE* schemes. Then, our *SIMD* homomorphic comparison and division schemes are constructed through our encoding and *SIMD SHE* schemes. Ultimately, we present our *SIMD* homomorphic *surf*, *clustering* and *multi-image matching* schemes.

A. Our Encoding Scheme

Our IoT system refers to computing about fixed point real number. In general, homomorphic encryption based on *Rlwe* only supports integer and polynomial computing. In order to implement our IoT system, we need to encode fixed point real number into polynomial under certain accuracy and reliability.

We convert a fixed point real number into an unsigned integer as follows: We multiply a fix point real number with a larger factor firstly. Then, all of fixed point real numbers are converted into integers. Each integer is expressed with complement. All of integers are converted into unsigned integers. Making use of encoding in $GF(2^{\Re})$ field, it is conventional to express elements of $GF(2^{\Re})$ as binary numbers. Usually, let $GF(2^{\Re}) = GF(2^8)$ for image processing [21], we can convert unsigned integer into a polynomial, which is $\sum_{i=0}^{\ell-1} m_i x^i = (m_0, m_1, \cdots, m_{\ell-1})$, where $m_i \in GF(2)$. Finally, the fixed point real number can be represented as polynomial.

B. Our SIMD SHE FV

SIMD technology [37] can implement the same operation on ℓ inputs parasynchronously. Namely, in our *SIMD SHE* scheme, *SIMD* technology can perform homomorphic evaluation for ℓ-bits plaintext simultaneously. For $\Phi_d(x) = \Pi_i^{\ell} F_i(x)$ mod 2, we can get $Z_2[x]/(\Phi_d(X)) \cong Z_2[x]/F_i(x) \otimes Z_2[x]/F_i(x) \cdots \otimes Z_2[x]/F_{\ell-1}(x)$, and then pack ℓ independent messages $(m_0, \cdots, m_{\ell-1})$ into the unique element (one ciphertext $R_2 = Z_2[x]/(\Phi_d(X))$). This greatly improve the efficiency of homomorphic evaluation. c_1 is the ciphertext of plaintext $(m_0, \cdots, m_{\ell-1})$, and c_2 is the ciphertext of plaintext $(m'_0, \cdots, m'_{\ell-1})$. Finally, we can perform the homomorphic evaluation: $c_1 + c_2 = E(m_0 + m'_0, \cdots, m_{\ell-1} + m'_{\ell-1})$, $c_1 \cdot c_2 = E(m_0 \cdot m'_0, \cdots, m_{\ell-1} \cdot m'_{\ell-1})$. E is our *SIMD SHE FV*.

C. Our Homomorphic Comparison Scheme (HCS)

For homomorphic image processing and machine learning (feature detection and description, feature point matching, clustering algorithm, etc.), homomorphic comparison over the encrypted data is a basic operation.

We utilize a comparator in digital system to perform comparison of two numbers (x, y). The comparator is a logic circuit for comparison on two numbers (x, y). The computational results are divided into two conditions. Namely, $G(x > y)$ or $M(x < y)$. With the help of single-bit digit-comparator, we can construct parallel multi-bit digital comparator. Table I shows single-bit digit-comparator over the encrypted data.

TABLE I
Single-bit digit-comparator over the encrypted data

Input		Output	
$E(x_0)$	$E(y_0)$	$E(G_{x_0>y_0})$	$E(M_{x_0<y_0})$
$E(0)$	$E(0)$	$E(0)$	$E(0)$
$E(0)$	$E(1)$	$E(0)$	$E(1)$
$E(1)$	$E(0)$	$E(1)$	$E(0)$
$E(1)$	$E(1)$	$E(0)$	$E(0)$

According to our encoding scheme in $GF(2^{\Re})$, user encodes two one-bit integer x_0 and y_0 as polynomials. Then, x_0 and y_0 is encrypted, and uploaded to *CS*. *CS* performs homomorphic comparison with comparator: $E(G) = E[x_0(1-y_0)]$ and $E(M) = E[(1-x_0)y_0]$. Then, *CS* returns $E(G)$ or $E(M)$ to the *H's* server, which decrypts $E(G)$ or $E(M)$. The *H's* server returns $G = 1$ or $M = 1$ to *CS*. Finally, *CS* gets $x > y$ or $x < y$.

Algorithm 1 *SIMD* homomorphic comparison algorithm.

```
Input:
    $x, y$ and public key $pk$ , where $x = x_1 x_2 \cdots x_n$ and $y = y_1 y_2 \cdots y_n$.
Output:
    $x > y$ or $x < y$.
$x$ and $y$ are encrypted with $E$. Base on our encoding and packing methods, $E(x) = E(x_1, x_2, \cdots, x_n)$ and $E(y) = E(y_1, y_2, \cdots, y_n)$. $E(x)$ and $E(y)$ are uploaded to CS.
CS computes $E(M)$ and $E(G)$ by SIMD operation, where $E(G) = E[x_1(1-y_1), \cdots, x_n(1-y_n)]$ and $E(M) = E[(1-x_1)y_1, \cdots, (1-x_n)y_n]$.
CS call for $n$ single-bit digital comparators in parallelism. Then, CS return $E(M)$ or $E(G)$ to H's server.
The H's server decrypts $E(G)$ or $E(M)$.
return  $x > y$ or $x < y$.
```

Two fixed real numbers x and y are encoded as polynomials, where the coefficients of polynomials are in $GF(2)$. Based on above packing technology, we can pack $x_1, x_2, \cdots, x_n$ and $y_1, y_2, \cdots, y_n$ into $E(x)$ and $E(y)$. Using *SIMD* technology, we implement homomorphic comparison over the encrypted data. Algorithm *1* gives our detailed *SIMD* homomorphic comparison algorithm.

In our homomorphic comparison algorithm, $G = 1$ or $M = 1$ stand for $x > y$ or $x < y$, respectively. The *H's* server returns $G = 1$ or $M = 1$ to *CS*. Finally, *CS* gets $x > y$ or $x < y$.

D. Our Homomorphic Division Scheme (HDS)

For homomorphic image processing and machine learning, encrypted data division is another key computation. Homomorphic encryption does not support homomorphic division directly. We can transform division into addition and multiplication, and then perform additive and multiplicative homomorphic evaluation over the encrypted data. In the following, we provide the detailed *Repeated-squaring* and *Conversion* algorithms for *HDS*.

For two positive integers a and b, we can denote them as polynomial ($a(x)$ and $b(x)$) by above-mentioned encoding scheme. E is our *SIMD SHE FV* scheme. The corresponding ciphertexts are $E(a(x))$ and $E(b(x))$ respectively.

Based on Cook et al. scheme [51], we can compute $\frac{a}{b}$ approximatively. For two positive integers a and b, we can compute $a \cdot \frac{1}{b}$. $\frac{1}{b}$ can be computed approximatively as follows: Let $u = 1 - (\frac{b}{2^j})(u \in (0, \frac{1}{2}))$. With help of Taylor series expansion and approximation, we can get $\frac{1}{(1-u)} \approx \Sigma_{i=0}^{n-1} u^i$. Namely, $\frac{1}{b} \approx 2^{-j}(\Sigma_{i=0}^{n-1} u^i)$.

HDS $(E(\frac{a(x)}{b(x)}))$ includes the following four algorithms: *SHE.Enc*, *SHE.Add*, homomorphic *Repeated-squaring* and *Conversion* algorithms. *SHE.Enc* and *SHE.Add* algorithms are the same as in our SIMD SHE FV scheme. Algorithm *2* and algorithm *3* present homomorphic *Repeated-squaring* and *Conversion* algorithms in details.

Algorithm 2 Homomorphic *Repeated-squaring* algorithm.

```
Input:
    $E(b(x))$ and $n$.
Output:
    $[E(b(x))]^n \bmod \Phi(x)$;
Let $n = (k_{r-1} \cdots k_i \cdots k_0)_2$ be the binary representation of $n$.
Compute $E(b(x)) \bmod \Phi(x), [E(b(x))]^2 \bmod \Phi(x), \cdots, [E(b(x))]^{2^i} \bmod \Phi(x), \cdots, [E(b(x))]^{2^{\lfloor log_2 n \rfloor}} \bmod \Phi(x)$.
Compute $(E(b(x)))^{k_0} \bmod \Phi(x)$, $[E(b(x))]^{2k_1} \bmod \Phi(x)$, $\cdots$, $[E(b(x))]^{k_{\lfloor log_2 n \rfloor} 2^{\lfloor log_2 n \rfloor}} \bmod \Phi(x)$.
Compute $(E(b(x)))^{k_0} \bmod \Phi(x) \times [E(b(x))]^{2k_1} \bmod \Phi(x) \times \cdots \times [E(b(x))]^{k_{\lfloor log_2 n \rfloor} 2^{\lfloor log_2 n \rfloor}} \bmod \Phi(x)$.
return  $[E(b(x))]^n \bmod \Phi(x)$.
```

In order to computing $[E(b(x))]^n \bmod \Phi(x)$, we represent n as a sum of power of 2 with the binary representation, that is $n = (k_{\lfloor log_2 n \rfloor} \cdots k_0)_2$, where $k_i \in \{0, 1\}$. Namely, $n = \sum_{i=0}^{\lfloor log_2 n \rfloor} k_i 2^i$. Then, we perform the following computation: $[E(b(x))]^n \bmod \Phi(x) = [E(b(x))]^{k_0} \times [E(b(x))]^{2k_1} \times [E(b(x))]^{4k_2} \cdots \times [E(b(x))]^{k_{\lfloor log_2 n \rfloor} 2^{\lfloor log_2 n \rfloor}} \bmod \Phi(x)$. We can prepare a list of basics: $E(b(x)) \bmod \Phi(x), [E(b(x))]^2 \bmod \Phi(x), \cdots, [E(b(x)\ )]^{2^i} \bmod \Phi(x), \cdots, [E(b(x))]^{2^{\lfloor log_2 n \rfloor}} \bmod \Phi(x)$. The basic $([E(b(x))]^{2^i} \bmod \Phi(x))$ can be computed as $(((E(b(x)))^2)^2 \cdots)^2 \bmod \Phi(x)$. Finally, we can compute $[E(b(x))]^n \bmod \Phi(x)$ with $\lfloor log_2 n \rfloor + h(n) - 1$ multiplications, where $h(n)$ is the number of one-bit for the binary representation of n.

Based on homomorphic *Repeated-squaring* and *SHE.Add* algorithms, we can compute $E(u^i)$ and $\Sigma_{i=0}^{n-1} E(u^i)$. With the help of homomorphic *Conversion* algorithm, we can compute $E(a) \cdot E(\frac{1}{b}) = E(a \cdot \frac{1}{b})$.

Algorithm 3 Homomorphic *Conversion* algorithm.

```
Input:
    $E(a)$, $E(b)$ and $evk(= \gamma)$, where $a = a(x)$ and $b = b(x)$.
Output:
    $E(\frac{a}{b})$.
For small enough $u = (1 - \frac{b}{2^j})$, where $j$ is the number of bits in $b$.
Call for the homomorphic Repeated-squaring algorithm to compute $[E(2^j - b)]^i$, where $i = 0, \cdots, n-1$.
Compute $E(\frac{a}{b}) = E(a) \sum_{i=0}^{n-1} E^i((2^j - b))(2^j)^i$, where $i = 0, \cdots, n-1$.
Compute $E(b)E(\frac{a}{b})$.
Compare $E(b)E(\frac{a}{b})$ to $E(a)$ by HCS algorithm.
return  $E(\frac{a}{b})$.
```

E. Our Homomorphic Surf Scheme

By means of our *SIMD SHE FV*, *HCS* and *HDS* schemes, we can implement efficient homomorphic feature point detection with *surf* scheme over each encrypted retinal image of *DR*. We provide the detailed description for key steps of homomorphic *surf* scheme as follows:

Homomorphic Integral Image: Firstly, each retinal image of *DR* is partitioned into $\widetilde{\Gamma}^2$ blocks and scrambled [52]. Then, we converse a color image to a grey image and a integral image finally. We can easily get the grey image of *I* as follows: $E[Gray_1(x,y)] = E[R(x,y)]$, $E[Gray_2(x,y)] = E[G(x,y)]$ and $E[Gray_3(x,y)] = E[B(x,y)]$, where $R(x,y)$ is the red component value of $I(x,y)$, $G(x,y)$ is the green component value of $I(x,y)$, and $B(x,y)$ is the blue component value of $I(x,y)$. In the encrypted domain, we can get the encrypted grey image of *I*.

Then, we can converse the encrypted grey image to the encrypted integral image by additive and multiplicative homomorphic evaluation: $E(\tilde{\tilde{I}}(x,y)) = \sum_{0\leq i\leq x}\sum_{0\leq j\leq y} E(\tilde{I}(x,y))$.

Homomorphic evaluation of Hessian Matrix Approximation: We can get determinant approximation of Hessian matrix by additive and multiplicative homomorphic evaluation: $E(det(H_{approx})) = E(BF_{xx})E(BF_{yy}) - [E(wBF_{xy}))]^2$, where $w = 0.9$. The second-order partial derivative computing can be approximately completed as follows:

$$\begin{aligned} E(BF^L_{xx}) =& E(BF_{T_1} * \tilde{I}) - E((3BF_{T_2}) * \tilde{I}),\\ E(BF^L_{yy}) =& E(BF_{T_3} * \tilde{I}) - E((3BF_{T_4}) * \tilde{I}),\\ E(BF^L_{xy}) =& E(BF_{T_5} * \tilde{I}) + E(BF_{T_6} * \tilde{I})\\ &- E(BF_{T_7} * \tilde{I}) - E(BF_{T_8} * \tilde{I}), \end{aligned}$$

where T_i is the rectangular domain as the original surf scheme.

For a rectangular domain $\tilde{D} = [a,b] \times [c,d] \subset \Omega$ and *BF* function in two dimension space, the convolution of encrypted *BF* with the encrypted discrete image I can be computed with the encrypted integral image $E(\tilde{\tilde{I}})$: $\forall (x,y) \in \Omega$,

$$\begin{aligned} &E(BF * I(x,y))\\ &= E(\tilde{\tilde{I}}(x-a, y-c)) + E(\tilde{\tilde{I}}(x-b-1, y-d-1))\\ &- E(\tilde{\tilde{I}}(x-a, y-d-1)) - E(\tilde{\tilde{I}}(x-b-1, y-c)). \end{aligned}$$

Finally, we get determinant approximation of Hessian matrix by additive and multiplicative homomorphic evaluation.

Homomorphic feature point detection: Utilizing the different sizes *BF*, we can construct Gaussian pyramid and scalar space in the encrypted domain. After constructing scale space with *BF*, we can complete homomorphic feature point detection. The main homomorphic evaluation includes the following steps:

(1) Homomorphic filtration of feature point. We can use homomorphic scale-normalized determinant of Hessian matrix to implement it easily.

$$E[DoH^L(\tilde{I})] = (E[BF_{xx}]E[BF_{yy}] - E[(\omega BF^L_{xy})^2])/E(L^4),$$

where $\omega = 0.912$, $L (= 2^o i + 1)$ is scale, and o is octave. By homomorphic integral image, we can compute $E[DoH^L(\tilde{I})]$ with additive and multiplicative homomorphic evaluation for each point in the box space.

(2) Homomorphic feature point selection. We can use 3×3 filters. There are 9 pixel points in every scalar level. With the adjacent upper and lower layers, each pixel point compares with 26 pixel points. We can get $DoH^L(\tilde{I}) > t_H$ with our *SIMD HCS* scheme, where t_H is the pre-set threshold to eliminate noise perturbation.

(3) Homomorphic refinement of feature point. For the feature point X, the refined result is $E(X) = E(X_0) + E(\zeta)$, where $\zeta = (\zeta_x, \zeta_y, \zeta_L)^T = -H_0^{-1}d_0$, d_0 is the discrete gradient, H_0 is the discrete Hessian of $DoH^L(\tilde{I})$. Utilizing a $3\times3\times3$ centred neighborhood, $E(d_0)$ and $E(H_0)$ with scale (L_0) and location $(E[(x_0, y_0)])$ can be computed with homomorphic evaluation in the box space as follows:

$$E(d_0) = \left[\begin{array}{c} E(d_x)\\ E(d_y)\\ E(d_L) \end{array}\right],$$

$$E(H_0) = \left[\begin{array}{ccc} E(H_{xx}) & E(H_{xy}) & E(H_{xL})\\ E(H_{xy}) & E(H_{yy}) & E(H_{yL})\\ E(H_{xL}) & E(H_{yL}) & E(H_{LL}) \end{array}\right],$$

where $E[d_x(X_0)]$, $E[d_x(Y_0)]$, $E[d_L(X_0)]$, $E[H_{xx}(X_0)]$, $E[H_{xy}(X_0)]$, $E[H_{xL}(X_0)]$ and $E[H_{LL}(X_0)]$ are computed through homomorphic additive, multiplicative and division evaluation.

When $E(\zeta_x)$, $E(\zeta_y)$ and $E(\zeta_L)$ meet up with $max((\zeta_x)^2,$ $(\zeta_y)^2, \frac{(\zeta_L)^2}{2}) < p^2$, where $E(p) = E(2^{o-1})$, the refined feature point is reliable. Otherwise, the refined feature point $E(X) = E(X_0) + E(\zeta)$ is not in the neighbourhood of $E(X)$. $max((\zeta_x)^2, (\zeta_y)^2, \frac{(\zeta_L)^2}{2}) < p^2$ can be computed by our *SIMD HCS* scheme.

Feature Point Description: We can compute the encrypted weighted gradient of a feature point $E[(x,y)]$ with our *SIMD SHE FV* and *HCS* schemes as follows: $E[\phi_k(x,y)] = E[(BF^L_x, BF^L_y)^T * I(x,y)] \cdot E[G_1(\frac{x-x_k}{2\sigma_k}, \frac{y-y_k}{2\sigma_k})]$. Sum of all the weighted gradients in circular neighbourhood can be computed as follows: $E[\Phi_k(\theta)] = \sum_{(x,y)\in B_{6\sigma_k}(x_k,y_k)} E[\phi_k(x,y)]\cdot$ $E[BF(x,y)_{[\theta-\frac{\pi}{6},\theta+\frac{\pi}{6}]}(\tilde{\theta}_\phi)]$, where $\tilde{\theta}_\phi (\in [-\pi, \pi))$ denotes the angle between $\phi_k(x,y)$ and x-axis. Then, the orientation of feature point is computed as follows: $E(\theta_k) = E(\tilde{\theta}_{\Phi_k(\theta^*)})$, where $\theta^* \in argmax\|\Phi_k(\theta)\|$. $argmax\|\Phi_k(\theta)\|$ is computed via our *SIMD HCS* scheme. Finally, we get the encrypted main direction of each feature point.

The encrypted weighted gradient at point $E[(u,v)]$ can be computed as follows:

$$\left[\begin{array}{c} E[d_x(u,v)]\\ E[d_y(u,v)] \end{array}\right] := E(R_{-\theta_k}) \left[\begin{array}{c} E[BF^{L_k}_x]\\ E[BF^{L_k}_y] \end{array}\right] \times$$
$$E[\tilde{I}(X,Y)] \times E[G_1(u/3.3, v/3.3)],$$

where

$$\left[\begin{array}{c} x\\ y \end{array}\right] - \left[\begin{array}{c} x_k\\ y_k \end{array}\right] = \sigma_k R_{\theta_k} \left[\begin{array}{c} u\\ v \end{array}\right],$$

$$R_{\theta_k} = \left[\begin{array}{c} cos(\theta_k), -sin(\theta_k)\\ sin(\theta_k), cos(\theta_k) \end{array}\right].$$

We can directly compute $E[cos(\theta_k)]$ and $E[sin(\theta_k)]$ via homomorphic evaluation. In this way, there are 4 values in each subregion:

$$E[\mu_k(i,j)] = \left[\begin{array}{c} \sum_{(u,v)\in R_{i,j}} E[d_x(u,v)]\\ \sum_{(u,v)\in R_{i,j}} E[d_y(u,v)]\\ \sum_{(u,v)\in R_{i,j}} E[|d_x(u,v)|]\\ \sum_{(u,v)\in R_{i,j}} E[|d_y(u,v)|] \end{array}\right].$$

Finally, the encrypted vector $E(\mu_k) = E[(\mu_k(i,j))_{1<i,j<4}]$ is obtained. This is the descriptor of a feature point.

F. Homomorphic Diabetic Retinopathy Detection

For surf-based diabetic retinopathy (DR) detection schemes [53] [54], the training of retinal lesion detectors is the critical factors. All the existing schemes are to take full advantage of the following schemes: *surf*, *clustering* (k-means) (or hard-assignment coding/sum pooling (*HARD-SUM*) and soft-assignment coding/max pooling (*SOFT-MAX*)), bag-of-visual-words (*BoVW*) and two-class classifier (Support Vector Machine (*SVM*)) schemes. The key ideas of the existing schemes are to use *surf* scheme to detect the low-level points of interest (*PoIs*) with a region of interest (*RoI*) containing specific lesions indicated by experts for *DR*. Then, utilizing *clustering* (k-means) (or *HARD-SUM* and *SOFT-MAX*) to create *BoVW* (or *max-pooling*) for training two-class classifier (*SVM*) of the lesion detectors. Finally, a trained two-class classifier is utilized for the final classification about the individual lesion detectors.

But, the above methods need complex *clustering* (k-means) process (or *HARD-SUM* and *SOFT-MAX*) to create *BoVW* (or *max-pooling*) for training two-class classifier (*SVM*) of the lesion detectors, and a trained two-class classifier for the final classification about the individual lesion detectors.

In this section, we use homomorphic fast *multi-retina-image matching* to simplify the whole process of lesions detection and *DR* detection simultaneously. With the help of the encrypted *RoIs* containing specific lesions indicated by expert, we can implement the parameters modification of homomorphic *surf* and fast *multi-retina-image matching* schemes based on the feedback matching results of the encrypted *multi-retina-image matching*. Finally, homomorphic *surf* and fast *multi-retina-image matching* schemes confirm a suitable number of feature points in specific lesions. A good specific lesions matching is implemented. Then, based on the modified homomorphic *surf* and fast *multi-retina-image matching* schemes with right parameters, the lesions and *DR* detection can be implemented for a new encrypted retinal image of *DR*. With the help of homomorphic *multi-retina-image matching* scheme, our scheme can directly implement homomorphic lesions detection and classification for many encrypted retinal images of *DR*. Algorithm *4* presents the detailed homomorphic *multi-retina-image matching* algorithm, which includes the following operations:

1) For feature points $(E(a^{(1)}_{I^{(i)}}), E(a^{(2)}_{I^{(i)}}), \cdots, E(a^{(N_i)}_{I^{(i)}}), i \in \{1, 2, \cdots, M\})$ of retinal images of *DR*, we firstly construct the following encrypted density function:

$$E(DF) = \sum_{i=1}^{M}\sum_{k=1}^{N_i} E[a(D^{(e)}_{I^{(s)}})]E[\tilde{h}(x, a^{(e)}_{I^{(s)}}; \rho_{den} D^{(e)}_{I^{(s)}})],$$

where $\tilde{h}(x, a^{(e)}_{I^{(s)}}; \sigma) = exp(-\frac{\|x - a^{(e)}_{I^{(s)}}\|^2}{2\sigma^2})$ with bandwidth $\rho_{den} D^{(e)}_{I^{(1)}}$, $\rho_{den} = 0.25$, $a(D^{(e)}_{I^{(s)}}) = log(1 + D^{(e)}_{I^{(s)}})$, $D^{(e)}_{I^{(s)}} = D^{(2)}_{I^{(1)}}$, and $\sigma = \rho_{den} D^{(2)}_{I^{(1)}}$. Based on e^{-x} defined by the following power series: $e^{-x} = 1 + (-x) + \frac{x^2}{2!} + \frac{(-x)^3}{3!} + \cdots + \frac{(-x)^n}{n!} + \cdots$, we can approximately compute $E[\tilde{h}(x, a^{(e)}_{I^{(s)}}; \sigma)] \approx E[1] + E[(-z)] + E[\frac{z^2}{2!}] + E[\frac{(-z)^3}{3!}] + \cdots + E[\frac{(-z)^n}{n!}]$, where z equals $-\frac{\|x - a^{(e)}_{I^{(s)}}\|^2}{2\sigma^2}$, $\| x - a^{(e)}_{I^{(s)}} \|^2$ is Euclidean distance. We can compute $E[(x - a^{(e)}_{I^{(s)}})^2]$ instead of $E[\| x - a^{(e)}_{I^{(s)}} \|^2]$ with our *SIMD* homomorphic addition and multiplication. Then, via our *HDS* scheme, we compute $E[\frac{-(x - a^{(e)}_{I^{(s)}})^2}{2\sigma^2}]$ instead of $E[-\frac{\|x - a^{(e)}_{I^{(s)}}\|^2}{2\sigma^2}]$. Finally, we get an approximation of $E[\tilde{h}(x, a^{(e)}_{I^{(s)}}; \sigma)]$.

Algorithm 4 Homomorphic *multi-image matching* algorithm.

```
Input:
    Encrypted data set: Feature points of retinal images of DR
    $(E[a^{(1)}_{I^{(i)}}], E[a^{(2)}_{I^{(i)}}], \cdots, E[a^{(N_i)}_{I^{(i)}}], i \in \{1, 2, \cdots, M\})$.
Output:
    Encrypted clusters EC with encrypted multi-image matching;
For all encrypted pairs $(E[a^{(e)}_{I^{(s)}}], E[a^{(v)}_{I^{(t)}}])$, CS compute
    $E[DF] = \sum_{i=1}^{M}\sum_{k=1}^{N_i} E[a(D^{(e)}_{I^{(s)}})]E[\tilde{h}(x, a^{(e)}_{I^{(s)}}; \rho_{den} D^{(e)}_{I^{(s)}})]$,
    where $\tilde{h}$ is the density kernel function with bandwidth $\rho_{den} D^{(e)}_{I^{(1)}}$, $\rho_{den}$ is the user-defined ration $(0 < \rho_{den} < 1)$,
    $a$ is an arbitrary adaptive amplification factor that depends on $D^{(e)}_{I^{(s)}}$, which is the distance between $a^{(e)}_{I^{(s)}}$ and the
    closet descriptor from the same image.
To build the homomorphic tree, CS computes:
    $E[Parent(a^{(e)}_{I^{(s)}})] = E[argmin_{(v, I^{(t)}) \in J} D(a^{(e)}_{I^{(s)}}, a^{(v)}_{I^{(t)}})]$,
    where $J = \{(v, I^{(t)}) : I^{(s)} \neq I^{(t)}, D^{(v)}_{I^{(t)}} > D^{(e)}_{I^{(s)}}\}$, $D(\cdot, \cdot)$ is the distance for the feature point space.
To break the built homomorphic tree and merge $E[C_M]$ and $E[C_{M'}]$, CS computes:
    $E[MD(C_{Mat})] = E[min_{(e, I^{(s)}) : a^{(e)}_{I^{(s)}} \in C_M} D^{(e)}_{I^{(s)}}]$,
    $E[D(a^{(e)}_{I^{(s)}}, a^{(v)}_{I^{(t)}}) \leq \rho_{edge} min\{MD(C_M), MD(C_{M'})\}]$,
    and $E[MD(C_M) \cap MD(C_{M'}) = \emptyset]$.
return Encrypted clusters EC with encrypted multi-image matches.
```

2) Through the encrypted density estimation, we construct an encrypted feature point tree. For the given encrypted feature point $E[a^{(e)}_{I^{(s)}}]$, we can implement the following computing with our *SIMD SHE FV* and *HCS* schemes:

$E[Parent(a^{(e)}_{I^{(s)}})] = E[argmin_{(v, I^{(t)}) \in J} D(a^{(e)}_{I^{(s)}}, a^{(v)}_{I^{(t)}})]$, where $J = \{(v, I^{(t)}) : I^{(s)} \neq I^{(t)}, D^{(v)}_{I^{(t)}} > D^{(e)}_{I^{(s)}}\}$, $D(\cdot, \cdot)$ is the distance for the feature point space. We can compute $E[D(a^{(e)}_{I^{(s)}}, a^{(v)}_{I^{(t)}})]$ with homomorphic addition, and compute $D^{(v)}_{I^{(t)}} > D^{(e)}_{I^{(s)}}$ via our *HCS* scheme for $E[D(a^{(e)}_{I^{(s)}}]$ and $E[D(a^{(v)}_{I^{(t)}})]$.

3) Finally, for the previous constructed tree, we implement homomorphic break to form different clusters, which correspond to the encrypted *multi-retina-image matching* results of *DR*. Namely, we complete the lesions detection. By our *HCS* scheme, we can compute:

$E[MatchDis(C_{Mat})] = E[min_{(e,I^{(s)}):a^{(e)}_{I^{(s)}} \in C_{Mat}} D^{(e)}_{I^{(s)}}]$. We cluster for each encrypted node (feature point) with the bottom-up procedure. Then, we compute $E[D(a^{(e)}_{I^{(s)}}, a^{(v)}_{I^{(t)}}) \leq \rho_{edge} min\{MatchDis(C_{Mat}), MatchDis(C_{Mat'})\}]$ and $E[MatchDis(C_{Mat}) \cap MatchDis(C_{Mat'}) = \emptyset]$, which can be implement with our *HCS* scheme directly. We can decide the valid edge and merge $E[C_{Mat}]$ and $E[C_{Mat'}]$ until all the edges are considered.

To modified the parameters of homomorphic *surf* (*PoIs* in the *RoI*) and fast *multi-retina-image matching* schemes (the lesions detection), we utilize encrypted *RoIs* containing specific lesions indicated by expert with the database. After a certain number of running tests, we can hold the parameters of homomorphic *surf* (*PoIs* in the *RoI*) and fast *multi-retina-image matching* schemes (the lesions detection). Based on the determined parameters of homomorphic *surf* (*PoIs* in the *RoI*) and fast *multi-retina-image matching* schemes (the lesions detection), we can implement the lesions detection for any new encrypted retinal image. From the results of the lesions detection, we can achieve *DR* detection.

VII. System Security and Privacy Analysis

For the security of our IoT system, we mainly consider our *SIMD SHE FV*, *HCS*, *HDS*, homomorphic *surf* and *clustering* schemes according to our threat model.

Based on our threat model, confidentiality of the retinal images of *DR* mainly relies on the security of our *SIMD SHE FV* scheme, transmission, storage and processing of the encrypted retinal images of *DR* in our IoT system. Our *SIMD SHE FV* scheme is quantum-resistant encryption scheme based on lattice. The data is encrypted during the transmission process. The processing over the encrypted retinal images of *DR* in our IoT system is homomorphic evaluation. Therefore, confidentiality of the retinal images of *DR* in our IoT system is guaranteed even in the era of quantum computation.

According to our threat model, *CS* is *honest-but-curious*. When *CS* implements *HCS*, *HDS*, homomorphic *surf* and *clustering* schemes, *CS* wants to get the encryption parameters g_1 and g_2 or e_1 and e_2 for revealing x or y. Finally, *CS* wants to obtain the content about the retinal images of *DR* and their classification results. We mainly consider *KPA* and *COA* attacks. Under *KPA* and *COA* attacks, for our IoT system, any information about each retinal image of *DR* and its classification is not revealed by *CS*. Patients privacy can be preserved in our IoT system.

Definition 1 (Ring-Learning with Error Problem [36])**.** *Ring-Learning with Error Problem is the problem to distinguish with non-negligible probability between independent samples* $(a_i, [a_i s + e_i]_q)$ *from the Ring-LWE distribution and the same number of independent samples* (a_i, b_i) *from the uniform distribution on* $R_q \times R_q$.

Definition 2 ($\alpha - BDD$ Problem [55])**.** *Let a lattice* L *and a vector* y *(within distance* $\alpha \cdot \lambda_1(L)$*),* $\alpha - BDD$ *problem is to find a lattice point* $x \in L$ *within distance* $\alpha \cdot \lambda_1(L)$ *from the target.*

Theorem 1 (Security of *HCS* scheme)**.** *Homomorphic comparison scheme HCS is COA and KPA security.*

Proof. For homomorphic comparison scheme *HCS*, we can prove it is *COA* and *KPA* security. When *CS* obtains $x > y$ or $x < y$, *CS* wants to derive x or y. *CS* selects a threshold $\hbar$, where $\hbar < x$ or $\hbar > y$. *CS* encrypted $\hbar$ with parameters $\tilde{a}$, $\tilde{b}$, g_3, e''_1 and e''_2. *CS* can computes $c_1 - c_3 = ([\triangle([x]_t - [\hbar]_t) + \tilde{b}(g_1 - g_3) + (e_1 - e''_1)]_q, [\tilde{a}(g_1 - g_3) + (e_2 - e''_2)]_q)$ or $c_3 - c_2 = ([\triangle([\hbar]_t - [y]_t) + \tilde{b}(g_3 - g_2) + (e''_1 - e'_1)]_q, [\tilde{a}(g_3 - g_2) + (e''_2 - e'_2)]_q)$. Based on *Rlwe* assumption (Definition *1*) and $\alpha - BDD$ problem (Definition *2*), *CS* can not get x or y.

Theorem 2 (Security of homomorphic *surf* and multi-image clustering schemes)**.** *Security of our homomorphic surf and multi-image clustering schemes are COA and KPA security.*

Proof. We can prove our homomorphic *surf* and multi-image clustering schemes are *COA* and *KPA* security. Our *SIMD SHE FV* scheme (E) is *IND-CPA* security, which is based on *Rlwe* assumption (Definition *1*).

E and *HDS* schemes are all *IND-CPA* security. Due to theorem *1*, *HCS* is *KPA* and *COA* security. When *CS* performs feature point detection, it can not get encrypted parameters e, s, x, y and $I(x, y)$. Our homomorphic *surf* scheme also can not reveal any content about each retinal image of *DR* in the encrypted domain. Each retinal image of *DR* is partitioned into $\widetilde{\Gamma}^2$ blocks and scrambled before performing encryption operation [52]. Scramble makes one of the sub-images has $\widetilde{\Gamma}^2$ possible location. The joint image has $\widetilde{\Gamma}^2!$ possible combination. When $\widetilde{\Gamma} \geq 5$, probability of *CS* to get the original partitioned image is negligible. Hence, our homomorphic *surf* scheme is *COA* and *KPA* security.

When *CS* performs homomorphic multi-image clustering, it employs *HCS* and *HDS* schemes. Based on security of our *HCS*, *HD* and homomorphic *surf*, homomorphic multi-image clustering scheme is *COA* and *KPA* security.

VIII. System Performance Evaluation

In this section, we provide the detailed performance evaluation about our *SIMD SHE FV*, *HCS*, *HDS*, homomorphic *surf* and *clustering* schemes for the *DR* diagnosis. Our IoT system use Camera (Raspberry Pi Noir Camera V2), a hand held condensing lens and Raspberry Pi 2 Model B [24] to constitute a sensor (S_i) to acquire the patients retinal images of *DR*, and perform image splitting and encryption. Then, the encrypted retinal image processing of *DR* and machine learning-based diagnosis are implemented by a cloud server (*CS*) with an Intel Xeon E5-1630 v4 CPU and 256 GB memory. The retinal image databases of *DR* are *DR*1 [56], RetiDB database [57] and Messidor database [58].

A. Efficiency Analysis of SIMD SHE FV and SIMD SHE FV-based Schemes

In this section, we provide efficiency analysis of our *SIMD SHE FV*, *HDS* and *HCS* schemes.

For the retinal image processing of *DR*, the pixel value of a grey image is in the range $[0, 256]$. Making use of our encoding

TABLE II
OUR SIMD SHE FV EFFICIENCY WITH SELECTED PARAMETERS

Scheme	Parameters	PK		SK		Ciphertext	Enc	Dec	Add	Mult
		Size(kb)	Time(ms)	Size(kb)	Time(ms)	Size(kb)	Time(ms)	Time(ms)	Time(ms)	Time(ms)
Our SIMD SHE FV	$\lambda = 80$, $n = 8192$, $t = 2^8$	3276.81	94.01	300	2.1	600	160.03	98.04	2.4	865.06
BGV SHE [35]		3281.69	1256.06	306.98	46.18	612	1842.12	567.25	6.23	1081.02

method, each value of the pixel can be encoded as a polynomial in the finite filed $GF(2^8)$. Security parameter $\lambda = 80$ for *Rlwe*-based *SHE* is quantum resistant [41] [42] [43]. Our *SIMD SHE FV* scheme chooses the following parameters: $\lambda = 80$ and $R_{2^8} = Z_{2^8}[X]/(X^{8192}+1)$. Such parameters meet up with security and application requirements of our IoT system.

Table II shows that our *SIMD SHE FV* scheme have smaller (public and private) key and ciphertext size than *BGV SHE* scheme [37]. The times for key generation and homomorphic evaluation (homomorphic addition and multiplication) are much shorter than *BGV SHE* scheme. For the retinal images of *DR* acquired by camera, sensor takes average 524*ms* to encrypt each acquired image. The ciphertext size of each retinal image of *DR* is about 68.52*MB*.

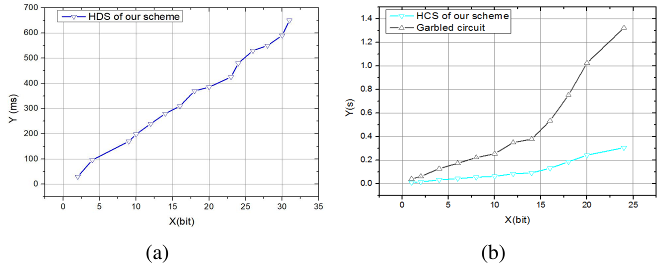


Fig. 3. (a) Efficiency of our *HDS* scheme. (b) Efficiency of our *HCS* scheme.

Fig. 3 (a) shows efficiency analysis of our *HDS* scheme. By means of our *Repeated-squaring* and *Conversion* algorithms, *CS* can efficiently perform homomorphic division evaluation by *HDS* scheme. For a 8 or 32 bit number, *CS* can implement homomorphic division evaluation in 150*ms* or 650*ms*.

Fig. 3 (b) presents efficiency analysis of our *HCS* scheme. We compare our *HCS* scheme with secure comparison protocol based on garbled circuit [59]. The result shows that our *HCS* scheme is more efficient than secure comparison protocol based on garbled circuit. It is because our *HCS* scheme just computes $E(M)$ and $E(G)$ once by *SIMD* operation, which greatly reduces the interaction number and the bit number of two different numbers to compare between the *CS* and the *H's* server.

B. *Efficiency Analysis of Our Homomorphic Surf Scheme*

In this section, we provide efficiency analysis of our homomorphic *surf* scheme for feature detection about each retinal image of *DR*. Synchronously, we compare communication cost about the feature detection via our *HCS* scheme with secure comparison protocol based on garbled circuit between the *CS* and the *H's* server. The retinal image databases of *DR* (*DR*1 [56], RetiDB database [57] and Messidor database [58]) include five abnormal findings in the eye fundus caused by the *DR*: (1) microaneuryms (*MAs*); (2) hemorrhages (*HMs*); (3) hard exudates (*HEs*); (4) soft exudate (*SEs*); (5) neovascularization (*NV*). Red lesions include *MAs* and *HMs*. Bright lesions include *HEs* and *SEs* [60]. We mainly consider the retinal image of *DR* (containing *MAs*, *HMs*, *HEs*, *SEs* and *NV*) for feature detection with the original *surf* and our homomorphic *surf* schemes.

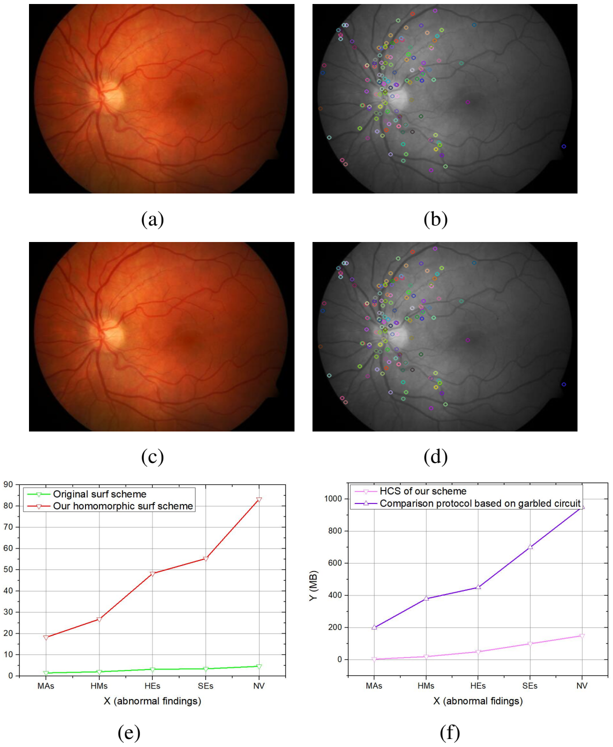


Fig. 4. (a)(c) Original retinal image of *DR*-1. (b) Feature detection of grey retinal image of *DR*-1 with original *surf* scheme. (d) Feature detection of grey retinal image of *DR*-1 with our homomorphic *surf* scheme. (e) Efficiency comparison of feature detection between the original *surf* and our homomorphic *surf* schemes. (f) Average communication cost comparison of feature detection about retinal images of *DR* between our homomorphic *surf* scheme with *HCS* and garbled circuit.

Fig. 4(a)(c) show the same retinal image of *DR*. Fig. 4(b) holds up feature detection of a grey retinal image of *DR* with original *surf* scheme. Fig. 4(d) shows the result of the feature detection (with our homomorphic *surf* scheme) for a grey retinal image of *DR* in the encrypted domain (the detection results recover from encrypted data to decrypted data). The results of feature point detection showed in Fig. 4(b)(d) demonstrate our homomorphic *surf* scheme can efficiently detect the feature points over the encrypted retinal images of *DR* as the original *surf* scheme [44].

In order to detect different abnormal findings in the eye fundus caused by *DR*, such as *MAs*, *HMs*, *HEs*, *SEs* and *NV*, we choose different parameters for our homomorphic *surf* scheme. The parameters modification is based on a certain

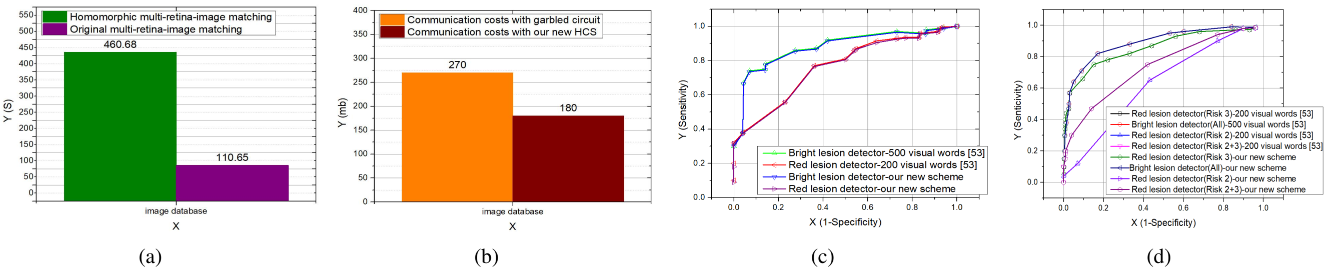


Fig. 5. (a) Efficiency comparison of lesions detection between the original *multi-retina-image matching* and our homomorphic *multi-retina-image matching* schemes. (b) Communication cost comparison of lesions detection about retinal images of *DR* between our homomorphic *surf* scheme with *HCS* and garbled circuit. (c) Comprehensive measure comparison between the scheme [53] and our scheme for bright and red lesions detection. Training/Parameters modification with *DR*1 database and testing over the RetiDB database. (d) Comprehensive measure comparison between the scheme [53] and our scheme for bright and red lesions detection. Training/Parameters modification with *DR*1 database and testing over the Messidor database.

number of running testing results about homomorphic *surf* and fast *multi-retina-image matching* schemes for *PoIs* in the *RoI* and the lesions detection. In this way, according to the feature points detecting results of the encrypted retinal images of *DR*, we can implement the lesions detection about different abnormal findings in the eye fundus caused by the *DR* for our efficient homomorphic fast *multi-retina-image matching* scheme.

Fig. 4(e) shows the efficiency comparison of feature point detection between the original *surf* scheme [44] and our homomorphic *surf* scheme. It is about *ten minutes* that our homomorphic *surf* scheme can finished the feature point detection over the encrypted retinal images of *DR*. Fig. 4(f) shows communication cost comparison between our *HCS* scheme and secure comparison protocol based on garbled circuit [59] during the homomorphic feature point detection. The result proves that our *HCS* scheme greatly reduces the communication cost. Our *HCS* scheme used for homomorphic feature point detection is more efficient than secure compare protocol based on garbled circuit [59].

C. Homomorphic Lesions Detection and Medical Diagnosis

In this section, with the aid of our homomorphic *surf* and fast *multi-retina-image matching* schemes, we provide experiments about homomorphic lesions detection of the *DR* and privacy-preserving remote *DR* diagnosis.

Fig. 5(a) shows the efficiency comparison of lesions detection between the original *multi-retina-image matching* and our homomorphic *multi-retina-image matching* schemes. Utilizing our homomorphic *multi-retina-image matching* scheme, a doctor can obtain the results of lesions detection and diagnosis in *seven minutes*. It is more efficient than manual work in hospital, and greatly reduces doctors workloads. Fig. 5(b) shows the communication cost comparison of lesions detection about retinal images of *DR* between our homomorphic *surf* scheme with *HCS* and garbled circuit schemes. The results proves that our *HCS* scheme greatly reduces communication cost between *CS* and the hospital's server.

For the automatic detection of *DR*, we utilize receiver operator characteristic (*ROC*) curves as the comprehensive measure of system performance [60] [53] [54]. *ROC* is created by the sensitivity/specificity pairs for every retinal image of *DR*. Fig. 5(c) shows comprehensive measure comparison between the scheme [53] and our scheme for bright and red lesions detection. The scheme [53] utilizes the *DR*1 database to train its system and test the trained system over the RetiDB database. But, our homomorphic system utilizes *DR*1 database to modify parameters about our homomorphic *surf* and fast *multi-retina-image matching* schemes for *PoIs* in the *RoI* and the lesions detection. Then, our system utilizes the RetiDB database for testing. For the bright lesions detection, our system results in an $AUC = 88.1\%$ as the scheme [53] with 500 words over the RetiDB database. For the red lesions detection, our system results in an $AUC = 76.4\%$ as the scheme [53] with 200 words over the RetiDB database.

Fig. 5(d) shows the comprehensive measure comparison between the scheme [53] and our scheme for bright and red lesions detection. The scheme [53] utilizes the *DR*1 database to train his system and test the trained system over the Messidor database. But, our homomorphic system utilizes the *DR*1 database to modify parameters about our homomorphic *surf* and fast *multi-retina-image matching* schemes for *PoIs* in the *RoI* and the lesions detection. Then, our system utilizes the Messidor database for testing. For the bright lesions detection, our system results in an $AUC = 89.3\%$ (for 90% sensitivity and 64%) as the scheme [53] with 500 words over the Messidor database. For the red lesions detection, our system results in $AUC = 86.2\%$ of $Risk_3$, $AUC = 63.3\%$ of $Risk_2$ and $AUC = 86.2\%$ of $Risk_{2+3}$ as the scheme [53] with 200 words (combined Risk) over the Messidor database.

According to the result, our scheme can efficiently performs classification of the encrypted image of *DR*.

IX. Conclusion

The world is changed by feat of IoT. Taking advantage of IoT and somewhat homomorphic encryption, we implement privacy-preserving diabetic retinopathy detection early. In this paper, we provide a *SIMD SHE FV* scheme. Based on *SIMD SHE FV* scheme, we realize efficient homomorphic comparison and division schemes. With the help of above our findings, we provide the privacy-preserving homomorphic *surf* and fast *multi-retina-image matching* schemes, which can perform efficient feature point detection and image matching for retinal images of diabetic retinopathy. Finally, by means of homomorphic fast *multi-retina-image matching*, we implement an efficient privacy-preserving remote diagnosis for diabetes. Computation of diagnostic process is homomorphic evaluation in our IoT system. Hence, patients privacy is protected. At the same time, our encryption scheme based on lattice, which is quantum-resistant, can preserves data confidentiality even in the era of quantum computation.

ACKNOWLEDGMENT

This work is supported by the Open Important Project of Guangxi Key Laboratory of Cryptography and Information Security (Grant No. GCIS201703), the Opening Project of GuangDong Province Key Laboratory of Information Security Technology (Grant No. 2017B030314131-12), the National Natural Science Foundation of China (Grant No. 61962013) and European Unions Horizon 2020 research and innovation programme under grant agreement No. 779391 (FutureTPM).

REFERENCES

[1] Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. IEEE communications surveys & tutorials, 17(4), 2347-2376.

[2] Zanella, A., Bui, N., Castellani, A., Vangelista, L., & Zorzi, M. (2014). Internet of things for smart cities. IEEE Internet of Things journal, 1(1), 22-32.

[3] Da Xu, L., He, W., & Li, S. (2014). Internet of things in industries: A survey. IEEE Transactions on industrial informatics, 10(4), 2233-2243.

[4] Guan, K., He, D., Ai, B., Matolak, D. W., Wang, Q., Zhong, Z., & Krner, T. (2019). 5-GHz obstructed vehicle-to-vehicle channel characterization for internet of intelligent vehicles. IEEE Internet of Things Journal, 6(1), 100-110.

[5] Zhang, H., Li, J., Wen, B., Xun, Y., & Liu, J. (2018). Connecting intelligent things in smart hospitals using NB-IoT. IEEE Internet of Things Journal, 5(3), 1550-1560.

[6] Reddy, S. R. N., & Kumar, D. (2018). Review of Smart Health Monitoring Approaches with Survey Analysis and Proposed Framework. IEEE Internet of Things Journal.

[7] Jara, A. J., Zamora-Izquierdo, M. A., & Skarmeta, A. F. (2013). Interconnection framework for mHealth and remote monitoring based on the internet of things. IEEE Journal on Selected Areas in Communications, 31(9), 47-65.

[8] Stachel, J. R., Sejdić, E., Ogirala, A., & Mickle, M. H. (2013, May). The impact of the internet of Things on implanted medical devices including pacemakers, and ICDs. In 2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC) (pp. 839-844). IEEE.

[9] Al-Taee, M. A., Al-Nuaimy, W., Muhsin, Z. J., & Al-Ataby, A. (2017). Robot assistant in management of diabetes in children based on the Internet of things. IEEE Internet of Things Journal, 4(2), 437-445.

[10] Zhou, J., Cao, Z., Dong, X., & Vasilakos, A. V. (2017). Security and privacy for cloud-based IoT: Challenges. IEEE Communications Magazine, 55(1), 26-33.

[11] Frustaci, M., Pace, P., Aloi, G., & Fortino, G. (2018). Evaluating critical security issues of the IoT world: Present and Future challenges. IEEE Internet of Things Journal, 5(4), 2483-2495.

[12] Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015, September). On the security and privacy of Internet of Things architectures and systems. In 2015 International Workshop on Secure Internet of Things (SIoT) (pp. 49-57). IEEE.

[13] https://twitter.com/leehsienloong

[14] Kocabas, O., Soyata, T., & Aktas, M. K. (2016). Emerging security mechanisms for medical cyber physical systems. IEEE/ACM transactions on computational biology and bioinformatics, 13(3), 401-416.

[15] National Institute of Standards and Technology, U.S. Department of Commerce, ”Advanced Encryption Standard”, Federal Information Processing Standards Publication 197, Washington, DC, November 2001.

[16] Standard, DES Encryption. ”National Bureau of Standards (US).” Federal Information Processing Standards Publication 46 (1997).

[17] Shoup, V. (2001). A proposal for an ISO standard for public key encryption (version 2.1). IACR e-Print Archive, 112.

[18] Mosca, M. (2018). Cybersecurity in an era with quantum computers: will we be ready?. IEEE Security & Privacy, 16(5), 38-41.

[19] Andrushkevych, A., Kuznetsova, T., Bilozertsev, I., & Bohucharskyi, S. (2016, October). The block symmetric ciphers in the post-quantum period. In 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T) (pp. 43-46). IEEE.

[20] Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In Post-quantum cryptography (pp. 1-14). Springer, Berlin, Heidelberg.

[21] Perlner, R. A., & Cooper, D. A. (2009, April). Quantum resistant public key cryptography: a survey. In Proceedings of the 8th Symposium on Identity and Trust on the Internet (pp. 85-93). ACM.

[22] Fan, J., & Vercauteren, F. (2012). Somewhat Practical Fully Homomorphic Encryption. IACR Cryptology ePrint Archive, 2012, 144.

[23] Duclos, P., Boeri, F., Auguin, M., & Giraudon, G. (1988, November). Image processing on a SIMD/SPMD architecture: OPSILA. In [1988 Proceedings] 9th International Conference on Pattern Recognition (pp. 430-433). IEEE.

[24] Bray, Jonathan. ”Raspberry Pi 2 Model B.” Pc Pro (2015).

[25] Smart, N. P. (2003). Cryptography: an introduction (Vol. 3). New York: McGraw-Hill.

[26] Biryukov, A., & Kushilevitz, E. (1998, August). From differential cryptanalysis to ciphertext-only attacks. In Annual International Cryptology Conference (pp. 72-88). Springer, Berlin, Heidelberg.

[27] Shen, B. Y., & Mukai, S. (2017). A portable, inexpensive, nonmydriatic fundus camera based on the Raspberry Pi? Computer. Journal of ophthalmology, 2017.

[28] Birkett, J., & Dent, A. W. (2014). Security models and proof strategies for plaintext-aware encryption. Journal of cryptology, 27(1), 139-180.

[29] Nagao, W., Manabe, Y., & Okamoto, T. (2005, February). A universally composable secure channel based on the KEM-DEM framework. In Theory of Cryptography Conference (pp. 426-444). Springer, Berlin, Heidelberg.

[30] Herranz, J., Hofheinz, D., & Kiltz, E. (2006). KEM/DEM: Necessary and sufficient conditions for secure hybrid encryption. Manuscript in preparation.

[31] Rivest, R. L., Adleman, L., & Dertouzos, M. L. (1978). On data banks and privacy homomorphisms. Foundations of secure computation, 4(11), 169-180.

[32] Paillier, P. (1999, May). Public-key cryptosystems based on composite degree residuosity classes. In International Conference on the Theory and Applications of Cryptographic Techniques (pp. 223-238). Springer, Berlin, Heidelberg.

[33] Gentry, C. (2010). Computing arbitrary functions of encrypted data. Communications of the ACM, 53(3), 97-105.

[34] Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In Stoc (Vol. 9, No. 2009, pp. 169-178).

[35] Alperin-Sheriff, J., & Peikert, C. (2014, August). Faster bootstrapping with polynomial error. In Annual Cryptology Conference (pp. 297-314). Springer, Berlin, Heidelberg.

[36] Lyubashevsky, V., Peikert, C., & Regev, O. (2010, May). On ideal lattices and learning with errors over rings. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 1-23). Springer, Berlin, Heidelberg.

[37] Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). (Leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory (TOCT), 6(3), 13.

[38] Smart, N. P., & Vercauteren, F. (2010, May). Fully homomorphic encryption with relatively small key and ciphertext sizes. In International Workshop on Public Key Cryptography (pp. 420-443). Springer, Berlin, Heidelberg.

[39] Smart, N. P., & Vercauteren, F. (2014). Fully homomorphic SIMD operations. Designs, codes and cryptography, 71(1), 57-81.

[40] Gentry, C., Halevi, S., & Smart, N. P. (2012, April). Fully homomorphic encryption with polylog overhead. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 465-482). Springer, Berlin, Heidelberg.

[41] Lepoint, T., & Naehrig, M. (2014, May). A comparison of the homomorphic encryption schemes FV and YASHE. In International Conference on Cryptology in Africa (pp. 318-335). Springer, Cham.

[42] Bos, J. W., Lauter, K., Loftus, J., & Naehrig, M. (2013, December). Improved security for a ring-based fully homomorphic encryption scheme. In IMA International Conference on Cryptography and Coding (pp. 45-64). Springer, Berlin, Heidelberg.

[43] Costache, A., & Smart, N. P. (2016, February). Which ring based somewhat homomorphic encryption scheme is best?. In Cryptographers Track at the RSA Conference (pp. 325-340). Springer, Cham.

[44] Bay, H., Ess, A., Tuytelaars, T., & Van Gool, L. (2008). Speeded-up robust features (SURF). Computer vision and image understanding, 110(3), 346-359.

[45] Lowe, D. G. (1999, September). Object recognition from local scale-invariant features. In iccv (Vol. 99, No. 2, pp. 1150-1157).

[46] Lowe, D. G. (2004). Distinctive image features from scale-invariant keypoints. International journal of computer vision, 60(2), 91-110.

[47] Juan, L., & Gwon, L. (2007). A comparison of sift, pca-sift and surf. International Journal of Signal Processing, Image Processing and Pattern Recognition, 8(3), 169-176.

[48] Tron, R., Zhou, X., Esteves, C., & Daniilidis, K. (2017). Fast multi-image matching via density-based clustering. In Proceedings of the IEEE International Conference on Computer Vision (pp. 4057-4066).

[49] Alkim, E., Ducas, L., P?ppelmann, T., & Schwabe, P. (2016). Post-quantum key exchangeła new hope. In 25th USENIX Security Symposium (USENIX Security 16) (pp. 327-343).

[50] Bos, J. W., Costello, C., Naehrig, M., & Stebila, D. (2015, May). Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In 2015 IEEE Symposium on Security and Privacy (pp. 553-570). IEEE.

[51] Coyne, D. T. (2010). Restructuring Proposal for the Criminal Division of the Circuit Court of Cook County.

[52] Wu, Y., Zhou, Y., Noonan, J. P., Panetta, K., & Agaian, S. (2010, April). Image encryption using the sudoku matrix. In Mobile Multimedia/Image Processing, Security, and Applications 2010 (Vol. 7708, p. 77080P). International Society for Optics and Photonics.

[53] Rocha, A., Carvalho, T., Jelinek, H. F., Goldenstein, S., & Wainer, J. (2012). Points of interest and visual dictionaries for automatic retinal lesion detection. IEEE transactions on biomedical engineering, 59(8), 2244-2253.

[54] Pires, R., Jelinek, H. F., Wainer, J., Goldenstein, S., Valle, E., & Rocha, A. (2013). Assessing the need for referral in automatic diabetic retinopathy detection. IEEE Transactions on Biomedical Engineering, 60(12), 3391-3398.

[55] Jiang, L., Xu, C., Wang, X., & Lin, C. (2017). Statistical learning based fully homomorphic encryption on encrypted data. Soft Computing, 21(24), 7473-7483.

[56] Diabetic Retinopathy Datasets (DR1), in 2010. [Online]. Available: https://recodbr.wordpress.com/code-n-data/retinopathy.

[57] Diabetic Retinopathy Datasets (RetiDB), in 2007. [Online]. Available: http://www.it.lut.fi/project/imageret/.

[58] Diabetic Retinopathy Datasets (Messidor), in 2014. [Online]. Available: http://www.adcis.net/en/Download-Third-Party/Messidor.html.

[59] Huang, Y., Evans, D., Katz, J., & Malka, L. (2011, August). Faster secure two-party computation using garbled circuits. In USENIX Security Symposium (Vol. 201, No. 1, pp. 331-335).

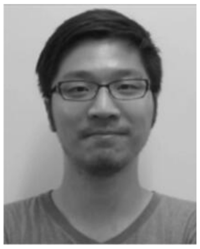
[60] Abrmoff, M. D., Niemeijer, M., Suttorp-Schulten, M. S., Viergever, M. A., Russell, S. R., & Van Ginneken, B. (2008). Evaluation of a system for automatic detection of diabetic retinopathy from color fundus photographs in a large population of patients with diabetes. Diabetes care, 31(2), 193-198.

Linzhi Jiang is a scientific researcher at Guilin University of Electronic Technology in China. He is also the Research Fellow at University of Surrey, United Kingdom. He received his Ph.D. from University of Electronic Science and Technology of China. His research interests include Fully Homomorphic Encryption, IoT Security, Trusted Computing, Quantum-Resistant Cryptography, Big Data and Cloud Computing Security. E-mail: linzjiang@hotmail.com, linzhi.jiang@surrey.ac.uk.

Liqun Chen is a professor in Surrey Centre for Cyber Security, University of Surrey, United Kingdom. Prior to this appointment, she was a principal research scientist at Hewlett-Packard Laboratories (HP Labs) in Bristol, United Kingdom. She has developed several cryptographic schemes adopted by the International Standards and some of them have been implemented in Trusted Platform Modules. She has an extensive publication record and holds a large number of granted patents in cryptography and information security.

Thanassis Giannetsos earned his Ph.D. degree from University of Allaborg, Denmark in 2012. Prior to his appointment as an Associate Professor within the Cyber Security Section, Technical University of Denmark, he was a Senior Researcher at the Networked Systems Security group with KTH, Sweden and then an Assistant Professor at the Department of Computer Science with University of Surrey, UK. His research interests span from applied cryptography to security and privacy in information technology. He has expertise in the design and implementation of secure and privacy-preserving protocols and risk management.

Bo Luo received the BE degree from the University of Sciences and Technology of China in 2001, the MPhil degree from the Chinese University of Hong Kong in 2003, and the PhD degree from The Pennsylvania State University in 2008. He is currently an assistant professor with Electrical Engineering and Computer Science Department at the University of Kansas. He is interested in information retrieval, information security, and privacy. He is a member of the IEEE Computer Society.



Kaitai Liang is an assistant professor in Surrey Centre for Cyber Security, University of Surrey, United Kingdom. He received the Ph.D. degree of Computer Science from City University of Hong Kong in 2014. His research interests include applied cryptography and information security, in particular, data encryption, user privacy, blockchain security, post-quantum secure solutions, trusted computing, privacy-enhancing technologies and light-weight secure systems. He has published over 60 research works in high-tier security conference and journals.

Jinguang Han received his Ph.D from University of Wollongong, Australia, in 2013. He currently is a lecturer in the Centre for Secure Information Technologies (CSIT), Institute of Electronics, Communications and Information Technology (ECIT), Queens University, UK. His main research interests include cryptography, access control, blockchain and privacy-preserving systems. He has served as a program co-chair of ProvSec 2016 and a program committee member of over 60 international conferences. He is a senior member of the IEEE.