CryptoImg: Privacy Preserving Processing Over Encrypted Images

M. Tarek Ibn Ziad*, Amr Alanwar†, Moustafa Alzantot†, and Mani Srivastava†
*Ain Shams University, Cairo, Egypt
†University of California, Los Angeles, Los Angeles, California, USA
Email: mohamed.tarek@eng.asu.edu.eg, {alanwar, malzantot, mbs}@ucla.edu

***Abstract*—Cloud computing services provide a scalable solution for the storage and processing of images and multimedia files. However, concerns about privacy risks prevent users from sharing their personal images with third-party services. In this paper, we describe the design and implementation of *CryptoImg*, an open source library[1] of modular privacy preserving image processing operations over encrypted images. By using homomorphic encryption, *CryptoImg* allows the users to delegate their image processing operations to remote servers without any privacy concerns. Currently, *CryptoImg* supports a subset of the most frequently used image processing operations such as image adjustment, spatial filtering, edge sharpening, histogram equalization and others. We implemented our library as an extension to the popular computer vision library `OpenCV`. *CryptoImg* can be used from either mobile or desktop clients. Our experimental results demonstrate that *CryptoImg* is efficient while performing operations over encrypted images with negligible error and reasonable time overheads on the supported platforms.**

I. Introduction

Cloud computing is one of the fastest growing technologies. Gartner research selected cloud computing among the top 10 strategic technology trends in 2015. Software-as-a-Service (SaaS) is a class of cloud computing that allows thin clients, such as mobile devices or web browsers, to make use of centrally hosted software services on demand. During the past few years, there has been a proliferation of commercial SaaS solutions for various application domains including image editing. For example, services like Adobe Creative Cloud [1], and Pixlr [2] allow the user to upload pictures from her personal computer or mobile device in order to apply different image enhancements online.

However, image processing in the cloud presents a serious threat to the user's privacy. A malicious service provider can look into the user private photos in order to discover sensitive information such as identity, friends, visited places, etc. As privacy is a crucial issue for end users, mitigating privacy concerns is necessary to increase the adoption of online image processing services.

In this paper, we present ***CryptoImg***, a library of modular image processing operations over encrypted images. We implemented our operations by extending the `OpenCV` library and employing the Paillier cryptosystem [6]. The major enhancement, which ***CryptoImg*** introduces as compared to previous work in the field, is that ***CryptoImg*** can efficiently perform the needed computations with minimal overhead, while guaranteeing the secrecy of private images. ***CryptoImg*** omits the need for multiple non-collided servers [3]. Also, ***CryptoImg*** supports different operations including image adjustment, spatial filtering, edge sharpening, edge detection, morphological operations, and histogram equalization over encrypted images. To the best of our knowledge, we are the first to support secure morphological operations besides other image processing operations in one package.

Recently, Lathey and Atrey [3] introduced a privacy-preserving method for image processing based on Shamir's Secret Sharing (**SSS**) scheme [4]. This method distributes the image enhancement task among multiple servers to ensure privacy. Their solution supports a number of low-level image processing tasks carried out on encrypted images, such as spatial filtering, anti-aliasing, edge enhancement, and dehazing. Although this approach allows performing both addition and multiplication operations over encrypted data, the security of this model is guaranteed only if the computation is distributed over n (>1) entities with no more than k among them are colluding. This model is impractical, as it requires non colluding servers and thus provides only weak security guarantees. Moreover, they employed different pre-processing for each secure operation. Therefore, a sequence of secure operations can not be done without decryption and re-encoding.

The rest of the paper is organized as follows: Section II defines the problem and threat model. Section III provides a brief background about Paillier cryptosystem and floating-point (FP) encoding technique. It also summarizes the related work. Section IV describes our proposed secure operations in details. Section V provides our experimental evaluation results. Finally, Section VI concludes the paper.

II. Problem Statement And System Architecture

In this section, first we define the problem statement and threat model. Later, we describe the system architecture of

[1]Source at https://github.com/TarekIbnZiad/CryptoImg

This research is funded in part by the National Science Foundation under awards CNS-1136174 and CNS-1329755, and by the Center for Excellence for Mobile Sensor Data-to-Knowledge under National Institutes of Health grant #1U54EB020404. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of NSF, NIH, or the U.S. Government.

CryptoImg.

A. Problem Statement

We study the problem of protecting the confidentiality of private images against third-party services performing image processing. Our threat model assumes that the clients trust their own hardware and locally-running software programs, but they do not trust third-party remote servers. Although the pressure of market competition forces service providers to perform the requested image enhancement operations correctly, these servers might threaten the user's privacy by abusing the given images to uncover private information for their own business interest. By giving the server access to nothing more than encrypted images, our system is secure under the "honest-but-curious" adversary model.

We rely on the Paillier cryptosystem which is provably secure using the hardness of *decisional composite residuosity assumption* [6]. This means that it is infeasible for any attacker to break the encryption unless he has an efficient algorithm that can solve a family of problems that are computationally intractable. Compared to previous work in image processing over encrypted images, our solution provides better security guarantees than the model adopted by [3], [8], which requires more than one server and becomes insecure against colluding servers.

B. System Architecture

As shown in Fig. 1, ***CryptoImg*** consists of two parties: client and server. The client represents either an individual personal computer (PC) or mobile device (Mob), while the server is a powerful system offering processing and storage services over the cloud. The client owns private image data and desires to make use of the server image processing services, while keeping the confidentiality of the submitted image against unauthorized access. To achieve this goal, the client encrypts the image before submitting it to the server. Using the homomorphic encryption (HE) properties of Paillier cryptosystem, the server can perform operations over the encrypted image without revealing the source plain-image. The output encrypted image is sent back to the client to decrypt and display the processed image.

III. Preliminaries and Related Work

This section provides a brief background about Paillier cryptosystem, discusses the used encoding scheme, and summarizes the related work.

A. Paillier Cryptosystem

HE is a form of encryption which permits secure computations over encrypted data. We denote the encryption of message m using the public key pk as $[\![m]\!]$. Paillier cryptosystem is an additive HE scheme as it provides a public-key operation $\oplus_z$ over two encrypted integers which is equivalent to their plaintext addition, as shown in (1). It also supports a self-blinding

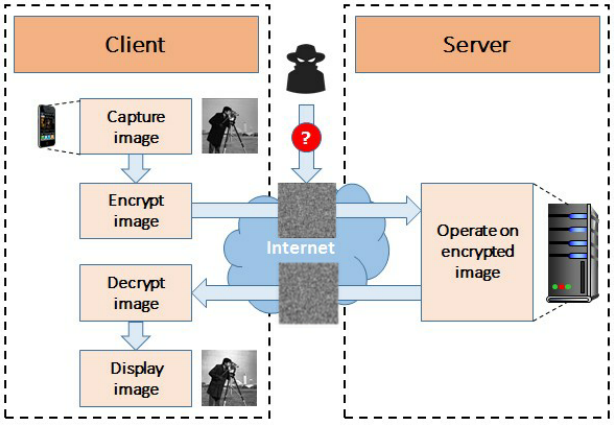

Fig. 1: System Architecture of ***CryptoImg***.

operation $\otimes_z$ which allows multiplication of encrypted integer by a plaintext scalar d, as shown in (2) $\forall m_1, m_2 \in \mathbb{Z}_n$.

$$\begin{aligned} \texttt{DEC}([\![m_1]\!] \oplus_z [\![m_2]\!]) &= \texttt{DEC}(([\![m_1]\!] \times [\![m_2]\!]) mod\, n^2) \\ &= (m_1 + m_2)\, mod\, n \end{aligned} \tag{1}$$

$$\begin{aligned} \texttt{DEC}([\![m_1]\!] \otimes_z d) &= \texttt{DEC}([\![m_1]\!]^d\, mod\, n^2) \\ &= (m \times d)\, mod\, n \end{aligned} \tag{2}$$

B. From Integers to Floating Point (FP) Numbers

Paillier cryptosystem is defined over a group of positive integers $\mathbb{Z}_n$, while in practice many operations should happen over real numbers. Therefore, an encoding function $\mathbb{EN}$ with minimal quantization error is needed in order to perform secure computation over FP numbers. We define ϕ_{add} and ϕ_{mul} as the error introduced due to addition and multiplication operation, as shown in (3) and (4), respectively. Optimal encoding mechanism should have $\phi_{mul} = \phi_{add} = 0$. Prior work over encrypted data represents FP numbers through multiplying by a large scaling factor as done in [5]. However, this representation has ϕ_{mul} equals the scale factor after each multiplication operation. Thus, it can not be used with arbitrary number of multiplication operations over FP numbers.

$$\phi_{add} := abs(\,\mathbb{EN}(m_1 + m_2) - (\mathbb{EN}(m_1) + \mathbb{EN}(m_2))\,) \tag{3}$$

$$\phi_{mul} := abs(\,\mathbb{EN}(m_1 \times m_2) - (\mathbb{EN}(m_1) \times \mathbb{EN}(m_2))\,) \tag{4}$$

Therefore, we have chosen to use the same approach developed by Google's Encrypted BigQuery Client [9], which represents FP number by a mantissa m and a non-positive exponent e. A FP number in plaintext is represented by pair (m, e). In encrypted domain, FP number is represented by a pair of an encrypted mantissa using paillier cryptosystem and an unencrypted exponent ($[\![m]\!]$, e). Self blinding and additive homomorphic over floats are denoted by $\otimes$ and $\oplus$, respectively. By using the addition and multiplication primitives ($\oplus_z$, $\otimes_z$) of the Paillier cryptosystem, we can perform FP numbers addition and multiplication, as shown in Protocol 1. Also, signed numbers are handled by assigning the ranges $[0, n/3]$ and $[n/3, 2n/3]$ for positive and negative numbers, respectively, Whereas the remaining range $(2n/3, n)$ is used

for overflow detection. Subtraction accordingly over encrypted floats is denoted by $\ominus$.

Protocol 1 Secure FP Numbers Processing.

Multiplication: $[\![c]\!] = a \otimes [\![b]\!]$
$[\![m_c]\!] = m_a \otimes_z [\![m_b]\!]$
$e_c = e_a + e_b$
Addition: $[\![c]\!] = [\![a]\!] \oplus [\![b]\!]$
if $e_a \leq e_b$
$[\![m_c]\!] = [\![m_a]\!] \oplus_z (Base^{e_b - e_a} \otimes_z [\![m_b]\!])$, $e_c = e_a$
if $e_a > e_b$
$[\![m_c]\!] = [\![m_b]\!] \oplus_z (Base^{e_a - e_b} \otimes_z [\![m_a]\!])$, $e_c = e_b$

C. Related Work

Recently, various privacy preserving algorithms using HE have emerged in different domains including: information retrieval, data mining, and image processing. Shortell and Shokoufandeh addressed the problem of privacy-preserving image processing by using fully homomorphic encryption (FHE) to process the data while encrypted [5]. They used their solution to implement brightness/contrast filter. Also, they extended FHE to support FP numbers via multiplying each value by a factor of 10^d, where d depends upon the precision of the desired decimal digits up to which we want to process the FP numbers. However, the reported execution time was 15 minutes on a scaled down image and three hours on the original image.

Hu *et al.* [10] proposed a double-cipher method to implement nonlocal means (NLM) denoising over encrypted images. As the NLM operation includes exponentiation, which is a non linear operation, the authors encrypted the plain image with two different cryptosystems before sending to the cloud. The first one was the Paillier scheme, in order to enable the mean filter, and the other was obtained by a distance-preserving transform, in order to enable the nonlocal search. However, their proposed method had higher communication overhead, due to outsourcing two different ciphers for every image. They also enabled only a single type of image processing operations.

Moreover, secure multi-party computation (SMC) has been utilized to protect privacy of outsourced images. Hu *et al.* implemented two secure linear filtering protocols [8]. The first one relied on a combination of rank reduction and random permutation, whereas the second one is based on random perturbation with the help of a third party entity. In the context of secure image retrieval, Zhang *et al.* proposed a secure image retrieval method for cloud computing, which is implemented based on content-based image retrieval (CBIR) framework [13].

Hsu *et al.* proposed a privacy-preserving realization of the scale-invariant feature transform (SIFT) method based on Paillier cryptosystem [14]. However, their proposed method introduced errors due to the rounding operation in their Gaussian filter coefficients, which were adjusted as integers because their Paillier cryptosystem can only operate in the integer domain. We handle this issue by using appropriate encoding technique.

IV. Secure Operations In Encrypted Domain

The following subsections give details about the supported image processing operations by ***CryptoImg***.

A. Secure Image Adjustment

Image enhancement is done by applying transformation T on an image I, which produces the resultant image R. We denote the individual pixels values in images I and R by i and r, respectively. Therefore, the relationship between input pixels i and output pixels r can be represented by $r = T(i)$.

CryptoImg supports *brightness control* and *image negation*. For *brightness control*, the client requests to adjust the brightness of his image by adding value v, encrypting it along with the image pixels using his public key, pk, and sends both the encrypted value $[\![v]\!]$ and encrypted image $[\![I]\!]$ to the server. The server computes the encrypted values of output pixels for all pixels in the image using $[\![r]\!] = [\![i]\!] \oplus [\![v]\!]$. Then, the server sends the encrypted image back to the client who will decrypt using its secret key sk.

Furthermore, ***CryptoImg*** supports secure *Image negation* where the server computes the encrypted output pixel according to $[\![r]\!] = [\![L-1]\!] \ominus [\![i]\!]$, for all pixels in input image with grey levels in the range $[0, L-1]$.

B. Secure Noise Reduction

Noise reduction and anti-aliasing operations are essential for many applications like medical, and remote sensing images processing. Smoothing filter in spatial domain is very common operation for anti-aliasing and noise removal, which is equivalent to a low pass filter (LPF) applied in the frequency domain. We denote the output image by I_{spt} whose individual pixels (u,v) are computed by performing average filter represented in (5). The filter $f(u,v)$ is applied first to $m \times n$ patch around (u,v) pixel, then the intensity values of this patch are averaged.

$$[\![I_{spt}(u,v)]\!] = \frac{1}{m \times n} \otimes \sum_{u=1,v=1}^{m,n} f(u,v) \otimes [\![I(u,v)]\!] \qquad (5)$$

The challenging part in mapping the average filtering operation to encrypted domain (ED) is how to map the division operation, which may result in a non integer result. As the original Paillier cryptosystem supports only operations over integers, we used our encoding technique, described in sub section III-B. It enables us to multiply by the FP term $1/(m \times n)$. Furthermore, arbitrary spatial filter masks can be applied in (5), as we do not restrict the filter value to be positive integers. On the other hand, authors in [5] did not support negative value in the filter mask.

C. Secure Edge Detection And Sharpening

Edge detection is an extremely important step facilitating high-level image analysis [15]. Edges are pixels where image brightness changes abruptly, therefore gradient operators are commonly used to discover such pixels in the image. ***CryptoImg*** supports different kind of edge detection operators as Prewitt, Sobel, Robinson, and Kirsh, which are able to detect edges in different directions. Those operators approximates the first derivative. Client sends the encrypted image to the server associated with the required operator ID. Horizontal kernel h_1 and vertical kernel h_2 are convoluted with the encrypted image to find encrypted horizontal $[\![G_x]\!]$ and vertical $[\![G_y]\!]$ gradient components as shown in (6) and (7). The client decrypts the resultant to find the gradient magnitude $G = \sqrt{{G_x}^2 + {G_y}^2}$ and gradient's direction $\Theta = \text{atan2}(G_y, G_x)$.

$$[\![G_x(u,v)]\!] = \sum_{u=1,v=1}^{m,n} h_1(u,v) \otimes [\![I(u,v)]\!] \tag{6}$$

$$[\![G_y(u,v)]\!] = \sum_{u=1,v=1}^{m,n} h_2(u,v) \otimes [\![I(u,v)]\!] \tag{7}$$

Additionally, edge sharpening operation in [5] can be reformulated, as shown in (8) in order to decrease the number of operation in the encrypted domain. Subtracting the blurred image I_{LPF} from the original one removes the low pass frequency component and yields the edge representation of the original image I. A positive constant, k, is used to control the amount of sharpening. For high-boost filtering, k is greater than one, while it equals one in case of unsharp masking. $[\![I_{LPF}]\!]$ can be obtained using (5) using the appreciate mask.

$$[\![I_{shrp}(u,v)]\!] = ((k+1) \otimes [\![I(u,v)]\!]) \ominus (k \otimes [\![I_{LPF}(u,v)]\!]) \tag{8}$$

D. Secure Morphological Operations

Morphological operations represent a relatively separate part of image processing. They are widely used in many applications, such as document analysis, character recognition, industrial inspection, and the analysis of microscopic images in fields like geology, biology, and material science. The basic idea in binary morphological operations, studied in this work, is to probe an image I with a pre-defined shape, called the structuring element B with size $m \times n$. The main two operations in binary morphology are erosion and dilation. Based on these two operations, more complex morphological operations can be computed, such as opening, closing, and shape decomposition. Protocol 2 describes the secure erosion and dilation operations. The erosion threshold value T equals the number of ones in B. Conversely, the threshold value T is equal to 1 to perform dilation.

E. Secure Histogram Equalization

Histogram equalization is a commonly used operation for contrast enhancement. It aims to create an image with equally distributed brightness levels over the whole brightness scale. As shown in Protocol 3, this goal is performed by calculating the cumulative image histogram H_c for the input image. Then, a monotonic pixel brightness transformation $T(p)$ is applied such that the desired output histogram is almost uniform over the whole brightness scale. Original image histogram is denoted by H and its size is G. Image size is $w \times \ell$. Intensity level is denoted by p.

Protocol 2 Secure Morphological Operations.

1: Client sends $[\![I]\!]$ to the server associated with the requested structuring element B.
2: Server performs $[\![L(u,v)]\!] = \sum_{u=1,v=1}^{m,n} [\![I(u,v)]\!]$.
3: Server sends $[\![L]\!]$ to the client.
4: Client decrypts $[\![L]\!]$ using his private key. Then, Image thresholding is applied on L using threshold value T.

Protocol 3 Secure Histogram Equalization.

1: Client sends encrypted image histogram H.
2: Server computes the brightness transformation $T(p)$ as following:
$[\![H_c(0)]\!] = [\![H(0)]\!]$
$[\![H_c(p)]\!] = [\![H_c(p-1)]\!] \oplus [\![H(p)]\!], where\ p = 1, 2, \cdots G-1$
$[\![T(p)]\!] = (G-1)/(w \times \ell) \otimes [\![H_c(p)]\!]$.
3: Server sends $[\![T]\!]$.
4: Client decrypts and applies $T(p)$ on each image pixel.

V. Evaluation

CryptoImg is implemented in C++ using GMP and NTL as an extension to the popular computer vision library `OpenCV`. We also developed an Android client application, which is implemented in Java. Our implementation of Paillier cryptosystem extends the work of [16] to introduce the FP support described earlier in SubSection III-B. For our experiments, we used a Intel Xeon(R) desktop machine with 8 cores at 2.20 GHz running Ubuntu 64-bit operating system. Our Android client application is installed on Nexus 5 (NX) mobile device, with Quad-core 2.30 GHz Krait 400 CPU.

The rest of this section provides our ***CryptoImg*** evaluation in terms of the introduced error, computation time on both client and server, and communication overhead.

A. Visual Output Evaluation

We performed a number of experiments to evaluate the performance of different operations supported by ***CryptoImg***. We applied the operations to a number of gray level images from the public CVG-UGR gray level image database [17]; The dimensions of every image is 512×512 pixels and every pixel is represented by 8 bits. In case of morphological operations, selected binary images from another database [18].

Fig. 2 shows the result of the proposed methods using a precision of 10^{-8}. The precision determines the exponent of the encoded FP number using $\lfloor \log_{Base} precision \rfloor$. Due to space limit, we only show one output for each method. Fig. 2-a represents the original images, which is encrypted using user Paillier public key and submitted to the server to obtain

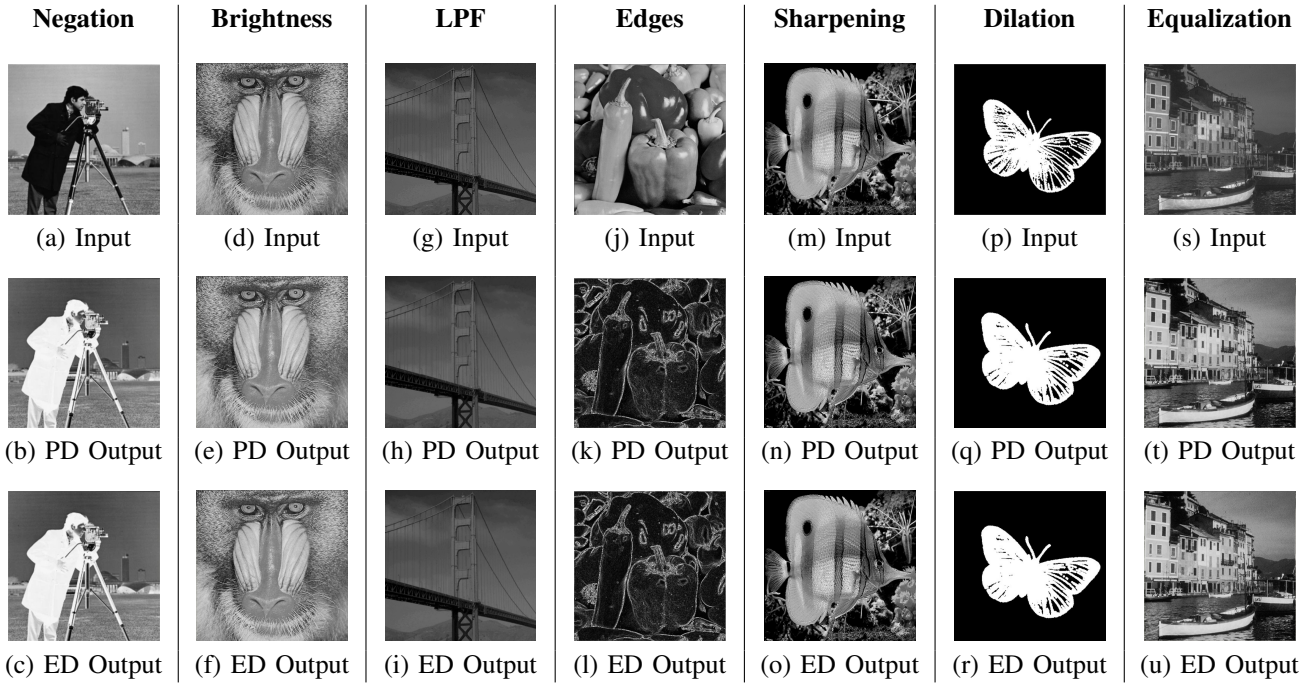

Fig. 2: Visual output evaluation for operations applied in PD and ED using 10^{-8} precision level.

image negation. Fig. 2-c shows the output after applying image negation in encrypted domain (ED). On the other hand, Fig. 2-b shows the output of image negation in the plaintext domain (PD) using normal `OpenCV` APIs. Fig. 2-d through Fig. 2-f show the same for brightness adjust. Additionally, Fig. 2-i shows the decrypted output after applying secure averaging operation on Fig. 2-g using a 3×3 filter. The visual effect of secure blurring and noise removal is compared with Fig. 2-h which is the normal average filter in the PD.

For the sake of testing edge detection techniques, a simple Sobel filter is used to detect edges in Fig. 2-j the outputs of the ED and PD are shown in Fig. 2-l and Fig. 2-k, respectively. On the other hand, edge sharpening with $k = 1.0$ is applied on Fig. 2-m. Edge sharpening in ED and PD are shown in Fig. 2-o and Fig. 2-n, respectively. Also, an example for the morphological operations is represented by applying a dilation operation on Fig. 2-p. The output in PD and ED are shown in Fig. 2-q and Fig. 2-r, respectively. Finally, Protocol 3 is applied on Fig. 2-s to perform histogram equalization in ED. The result is shown in Fig. 2-u which is compared with PD outputs in Fig. 2-t.

By comparing the output of operations in both encrypted and plain domains, we find that all our secure methods introduce zero error except LPF and edge sharpening, which introduce a low error at higher precision. Table I shows the effect of choosing the precision level in the secure LPF and edge sharpening operations. The error is calculated by comparing the output in PD and ED. Based on that, we choose 10^{-8} as a reasonable precision.

B. Computation Time

We used two different implementation for Paillier cryptosystem for PC and Mob. Table II shows the computation time that ***CryptoImg*** takes to encrypt/decrypt images using different key sizes. The encryption/decryption process is done pixel by pixel. Therefore, if the original image size is $n \times n \times 8$ bits and a k bit key is used, the size of the encrypted image would equal approximately $2k \times n \times n$ bits. That represents approximately a $k/4$ expansion factor. Histogram equalization operation does not require the encryption of all pixels. Only the histogram is encrypted, as explained in Protocol 3.

Table III shows timing results of running our protocols using a PC or Mob clients with the configuration given in Section II-B. For obtaining a high level of security, we set the Paillier key length to of 1024-bits and 2048-bits in all scenarios. Edge sharpening is the most expensive operation, as it needs successive computations. The relatively high cost of the encryption process could be amortized by storing an encrypted version of the image on a cloud storage. The image is encrypted once and could be used as an input for many secure image processing operations.

TABLE I: Precision effect on the introduced error.

Precision	Average Error		Standard Deviation	
	LPF	Sharpening	LPF	Sharpening
10^{-2}	0.768	0.644	0.471	0.485
10^{-8}	0.145	0.012	0.352	0.112
10^{-10}	0.145	0.012	0.352	0.116

TABLE II: Execution Time (sec) of the Paillier encryption/decryption of image using different key sizes on both personal computer (PC) and mobile device (Mob) clients. We used 512×512 image for PC and 256×256 image for Mob.

Key Size	256	512	1024	2048
Encrypt-PC	23.9164	156.905	1154.29	7670.49
Decrypt-PC	1.39223	1.93554	4.06813	9.62313
Encrypt-Mob	13	73	575	3701
Decrypt-Mob	10	48	325	2268

TABLE III: Execution Time (sec) of the proposed operations using 1024-bit and 2048-bit keys on both personal computer (PC) and mobile device (Mob) clients. The server is modeled as the personal computer. We used 512×512 image.

Operation	PD	ED					
		Pre-processing		Server		Post-processing	
		PC	Mob	1024-bit	2048-bit	PC	Mob
Negation	0.00122	0	0	42.4737	137.925	0	0
Brightness	0.00108	0	0	0.81994	2.39777	0	0
LPF	0.00763	0	0	180.508	609.199	0	0
Sobel filter	0.00642	0	0	147.567	482.195	0.0012	0.0940
Sharpening	0.00977	0	0	238.257	807.528	0	0
Erosion	0.00009	0	0	4.04937	10.8085	0.0006	0.0198
Dilation	0.00008	0	0	4.04937	10.8085	0.0005	0.0198
Equalization	0.00174	0.00182	0.177	0.01446	0.04835	0.0007	0.0290

C. Discussion

Based on our results, we conclude that performing operations over encrypted images adds more cost in terms of computation time, communication, and storage. The added cost increases as the length of encryption key increases. However, our protocols add minimal computation overhead, which is orders of magnitude less than prior work (e.g. [5]) and also minimal communication overhead, only one round between the client and server.

Also, it is worth mentioning that not all image processing operations can be directly implemented in ***CryptoImg***. For instance, operations that require sorting/comparison, such as median filtering [19], would require more communication rounds between the client and server. Some gray-scale transformations, such as contrast manipulation, would not be feasible in ED as they rely on the knowledge of the original intensity value of the pixel to be able to map this value to another intensity value. More complicated algorithms, such as SIFT, could be supported in ED at the cost of adding more communication rounds between the client and server, a similar approach was used by [14].

VI. Conclusion

In this paper, we introduced ***CryptoImg***, a library of modular privacy preserving image processing operations over encrypted images based on the homomorphic properties of Paillier cryptosystem. Secure operations, such as image adjustment, spatial filtering, edge sharpening, edge detection, morphological operations, and histogram equalization, are safely outsourced to third-party servers with no privacy issues.

We presented how this operations can be implemented with much less time overhead, and single communication round. Moreover, ***CryptoImg*** can be used from either mobile or desktop clients with low client-side overheads. Experiments show the efficiency of our proposed library. In the future, it will be interesting to explore the feasibility of using the current secure operations as building blocks to support more complex algorithms.

References

[1] "Adobe creative cloud," http://www.adobe.com/creativecloud.html, [online; accessed July 3, 2016].

[2] "Pixlr: Photo Editor Online," https://pixlr.com/web, [Online; accessed July 3, 2016].

[3] A. Lathey and P. K. Atrey, "Image enhancement in encrypted domain over cloud," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 11, no. 3, pp. 38:1–38:24, Feb. 2015.

[4] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[5] T. Shortell and A. Shokoufandeh, "Secure signal processing using fully homomorphic encryption," in *Advanced Concepts for Intelligent Vision Systems*, ser. Lecture Notes in Computer Science. Springer International Publishing, 2015, vol. 9386, pp. 93–104.

[6] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in *Proceedings of the 17th International Conference on Theory and Application of Cryptographic Techniques*, ser. EUROCRYPT'99, New York, NY, USA, 1999, pp. 223–238.

[7] C. Gentry, "A Fully Homomorphic Encryption Scheme," Ph.D. dissertation, Stanford University, 2009.

[8] N. Hu, S. S. Cheung, and T. Nguyen, "Secure image filtering," in *2006 IEEE International Conference on Image Processing*, Atlanta, Ga, USA, Oct. 2006, pp. 1553–1556.

[9] "Google encrypted bigquery client," https://github.com/google/encrypted-bigquery-client, [Online; accessed July 3, 2016].

[10] X. Hu, W. Zhang, K. Li, H. Hu, and N. Yu, "Secure nonlocal denoising in outsourced images," *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 12, no. 3, pp. 40:1–40:23, Mar. 2016.

[11] A. Buades, B. Coll, and J. M. Morel, "A review of image denoising algorithms, with a new one," *Multiscale Modeling & Simulation*, vol. 4, no. 2, pp. 490–530, 2005.

[12] M. Gomathisankaran, X. Yuan, and P. Kamongi, "Ensure privacy and security in the process of medical image analysis," in *2013 IEEE International Conference on Granular Computing (GrC)*, Beijing, China, Dec 2013, pp. 120–125.

[13] Y. Zhang, L. Zhuo, Y. Peng, and J. Zhang, "A secure image retrieval method based on homomorphic encryption for cloud computing," in *19th International Conference on Digital Signal Processing (DSP)*, Aug. 2014, pp. 269–274.

[14] C. Y. Hsu, C. S. Lu, and S. C. Pei, "Image feature extraction in encrypted domain with privacy-Preserving SIFT," *Image Processing, IEEE Transactions on*, vol. 21, no. 11, pp. 4593–4607, Nov 2012.

[15] M. Sonka, V. Hlavac, and R. Boyle, "Image pre-processing," in *Image Processing, Analysis and Machine Vision*. Springer US, 1993.

[16] S. T. R. Bost, R. A. Popa and S. Goldwasser, "Machine learning classification over encrypted data," August 9, 2015, https://github.com/rbost/ciphermed/tree/master/src/crypto.

[17] "CVG-UGR image database," http://decsai.ugr.es/cvg/dbimagenes/, [Online; accessed July 3, 2016].

[18] "MPEG7 CE Shape-1 Part B image database," http://www.imageprocessingplace.com/downloads_V3/root_downloads/image_databases/, [Online; accessed July 3, 2016].

[19] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*. Pearson, 2007.