

A Practical Exercise in Adapting SIFT Using FHE Primitives

Ishwar B Balappanawar*, Bhargav Srinivas Kommireddy*
{ishwar.balappanawar, bhargav.srinivas}@students.iiit.ac.in
IIIT Hyderabad

* These authors contributed equally to this work.

Abstract—An exercise in implementing Scale Invariant Feature Transform using CKKS Fully Homomorphic encryption quickly reveals some glaring limitations in the current FHE paradigm. These limitations include the lack of a standard comparison operator and certain operations that depend on it (like array max, histogram binning etc). We also observe that the existing solutions are either too low level or do not have proper abstractions to implement algorithms like SIFT.

In this work, we demonstrate:

- Methods of adapting regular code to the FHE setting.
- Alternate implementations of standard algorithms (like array max, histogram binning, etc.) to reduce the multiplicative depth.
- A novel method of using deferred computations to avoid performing expensive operations such as comparisons in the encrypted domain.

Through this exercise, we hope this work acts as a practical guide on how one can adapt algorithms to FHE.

I. INTRODUCTION

How good is the current Fully Homomorphic Encryption (FHE) paradigm at performing common everyday algorithms? To explore this question, we started working on adapting a common image processing algorithm, Scale Invariant Feature Transform (SIFT) [1]. Fully Homomorphic Encryption (FHE) schemes have been increasingly utilized for secure computations [2, 3], but adapting algorithms like SIFT comes with unique challenges. While frameworks like Microsoft SEAL, HELib, and TenSEAL [4–6] provide strong primitives, their abstractions often fall short for complex algorithms.

In the context of FHE, this task involves two main parties: - a) the client who has the raw image and is the entity that encrypts the image. b) The server which executes the algorithm that needs to take an encrypted image, i.e., a 2-dimensional array of encrypted pixel values and produce the encrypted version of the output. The goal is to ensure accurate execution of the algorithm without revealing the image or intermediate results (like SIFT keypoints) to the processing entity.

There is existing work on implementing SIFT using homomorphic encryption schemes, but most of the approaches involve revealing some information either about the image or the SIFT points.[7] [8] We wanted to avoid revealing any kind of information to the processing entity. We also avoid utilizing the internals of the FHE scheme and only use the primitives provided by libraries. This is a deliberate choice made to assess the quality of abstractions that are available. First we will discuss the SIFT algorithm itself and isolate the parts of it that are challenging/interesting to adapt to the FHE domain. In the subsequent sections we will talk about the deficiencies of the state of the art and propose some new ways to deal with the challenges using deferred computations.

II. THE SIFT ALGORITHM

The SIFT algorithm involves the following steps[9]:

- Scale-space Extrema Detection

- Keypoint Localization
- Orientation Assignment
- Keypoint Descriptor Generation

Our goal was to implement all these computational tasks using the primitives provided to us for a FHE scheme. Some of the tasks involve computing gradients and Hessians which warrant the use of floating point numbers. For this reason we chose to use the CKKS encoding scheme[10]. We used the tencal python library, as it is a well supported wrapper around the popular Microsoft SEAL library. The primitives that we utilize are addition and multiplication. So we implemented all the necessary computational tasks using addition and multiplication. There is the further constraint of multiplicative depth, which prevents us from performing a long chain of multiplications on an encrypted number. This is one of the most significant hurdles with adapting any algorithm to the FHE setting.

Some of the tasks, such as convolution and matrix multiplication, were trivial to implement using addition and multiplication.[11] However there were multiple tasks that were far from trivial, we will discuss these in the next section.

III. THE HARD TASKS

A. Comparison

The computation of scale-space extrema in a Fully Homomorphic Encryption (FHE) setting requires comparing encrypted values, a challenging task due to the complexity of implementing comparison functions. Integer domain comparisons can leverage Fermat’s Little Theorem for exact results, while approximate methods exist for floating-point numbers [12]. However, both approaches are resource-intensive, requiring significant multiplication depth, which is costly in FHE.

A practical solution involves an interactive approach where the server sends the two numbers to the client for comparison, and the client returns an encrypted boolean result with minimal noise [?]. While this method introduces interactivity and potential algorithm exposure (as the client sees the values being compared), the risk can be mitigated by sending spurious comparison requests alongside the real ones. This approach balances practicality with security, leveraging modern communication speeds to maintain efficiency.

B. Division

Integer division is surprisingly hard to perform using FHE primitives, it often requires the use comparison function which itself is expensive. Floating point division is a bit simpler; approximations such as Taylor or Chebyshev series are commonly used in FHE computations [13]. To get a good approximation we still need to use excessive multiplicative depth.

$$\frac{1}{x} \approx \frac{1}{a} - \frac{(x-a)}{a^2} + \frac{(x-a)^2}{a^3} - \frac{(x-a)^3}{a^4} + \dots$$

To avoid this, we store the numerator and denominator of the division separately and modify the subsequent uses of the algorithm

to use the numerator and denominator separately. For example, if $c = \frac{a}{b}$ and later we use it for, say, comparison, $c < d$, we modify this comparison to $a < d \cdot b$. This allows us to avoid calculating the inverse of b , which would have been expensive.

C. Other Functions Requiring Approximation

There are steps in SIFT which require the computation of the magnitude of vectors. This involves computing the square root of a number. Again there are polynomial approximations of this using Chebyshev polynomials (used by openFHE). Any sort of polynomial approximation would require a lot of multiplicative depth to get a good approximate value, so we do the same that we did in comparison and delegate this calculation to the client.

D. Conditional Blocks

The result of a comparison is often used to decide which code block to execute. In algorithms implemented with FHE primitives, we do not have a luxury to choose. If the boolean value of an if else condition is encrypted then we need to execute both the if-block and the else-block and mask the effects of the block by multiplying with the boolean value.

This is branchless coding and there has already been a lot of research done in converting regular algorithms to their branchless version [14, 15]. A big reason for this is that to take advantage of the min-maxed parallelism of GPUs, one needs to reduce the number of branches. We believe this field is worth consulting before one starts implementing their algorithms.

Some optimizations that help in regular algorithms can become unnecessary when using FHE, because we execute both if and else block anyway. So early stopping strategies like breaking in loops is pointless. This allowed us to skip a very large chunk of code in SIFT. One should greedily look for such blocks to eliminate while adapting their algorithms.

E. Histograms and Binning

In one of the steps we need to calculate the magnitude and angle of gradients in a neighborhood. A histogram of these angles need to be calculated weighted by their magnitudes. An efficient representation of the histogram bins is critical. This kind of optimization has been explored in privacy-preserving image processing [16]. Typically, we would implement this by creating an array with $360 / \text{num_bins}$ entries. For a given angle, one would calculate the index of the array that needs to be incremented. In the FHE setting we cannot choose which element of the array to increment, we need to update every element but multiplied with a mask so that only the correct element is incremented. The mask is generated by comparing the candidate element with the limits of each of the bins. $a_i < \theta < a_{i+1}$. for all i . This means that indices in FHE space are one-hot vectors.

Before we start calculating the histogram, we need to calculate the angles of the gradient according to the following equation.

$$\theta = \arctan\left(\frac{dy}{dx}\right)$$

We have the values for dx and dy but using approximations to calculate inverse of dx and \arctan is just too expensive, so we modify the condition we use to calculate the mask.

$$\tan(a_i) \cdot dx < dy < \tan(b_i) \cdot dx$$

Now we have the bins in terms of multiplications and additions. There is still a \tan to calculate but that is over an unencrypted value, so can do it regularly. Would a simple compiler pass of the regular

histogram binning code be able to do an optimization like this? Probably not. Is it impossible to come up with an automated way of doing this? Probably not. The conversion here needed knowledge of the properties of \arctan and \tan , but nothing more. This opens up new directions to look into in terms of automatic conversion of regular algorithms to code that works well using FHE primitives.

F. Finding Max in an Array

In the step of orientation calculation, one needs to find the maximum element in the histogram. The usual method of doing this would be maintaining a running maximum of the elements and comparing that running maximum with subsequent elements. Update the running maximum according to the boolean result of the comparison.

Algorithm 1 Find Maximum in Array

```

1:  $max \leftarrow 0$ 
2: for each element in array do
3:    $b \leftarrow (element > max)$ 
4:    $max \leftarrow b \cdot element + (1 - b) \cdot max$ 
5: end for
```

If we analyze the multiplicative depth of this algorithm, it would be $O(N)$, where N is size of array, ignoring the requirement for comparison.

Since length of arrays can be large, we instead use a different way of calculating max, where we compare adjacent elements of the array and remove the smaller values. This would cut down the array size in half. We perform this step till only one element is left. The multiplicative depth of this algorithm ignoring comparison is $O(\log N)$.

Algorithm 2 Max Function

```

1: function MAX( $a, b$ )
2:    $cond \leftarrow (a > b)$ 
3:   return  $cond \cdot a + (1 - cond) \cdot b$ 
```

Algorithm 3 Vector Maximum (VECMAX)

```

1: function VECMAX( $ls$ )
2:    $l \leftarrow \text{length of } ls$ 
3:   if  $l = 1$  then
4:     return  $ls[0]$ 
5:   else if  $l = 2$  then
6:     return MAX( $ls[0], ls[1]$ )
7:   else
8:     return MAX(VECMAX( $ls[:l//2]$ ), VECMAX( $ls[l//2:]$ ))
```

IV. DEFERRED COMPUTATION

In order to delegate expensive operations, such as comparison and square root, to the client in a non-interactive manner, we propose a novel method of **deferring computation**. The deferred computation technique is inspired by concepts from dynamic computation graphs and secure function evaluation, as used in frameworks like TensorFlow for privacy-preserving tasks [17]. In this method, the server sends a single response to the client. The client can then perform the requisite computation to extract the result from the response.

A. How It Works

The server assumes it does not know the boolean value and treats it as a variable. As operations are performed on this boolean variable, a function is constructed with the variable as a parameter. The server sends the following to the client:

- The comparison required to compute the boolean value.
- A function that uses this boolean value as a parameter.

The client performs the necessary comparison and substitutes the resulting values into the function to compute the final result.

B. Construction of the Function

To construct this function, a **dynamic computation graph** is created, which tracks how the comparison results are manipulated. This graph contains comparison nodes and represents the structure of the computation. Post-processing may be applied to simplify the graph and produce a more compact function.

C. Example

Consider the following expression:

$$a = (x > y) \cdot c + (z > w) \cdot d + (y \geq x) \cdot e$$

The server will return to the client:

$$f(c_1, c_2) = c_1 \cdot (c - e) + c_2 \cdot d + e$$

where:

$$c_1 = (x > y), \quad c_2 = (z > w)$$

D. Downside of the Approach

One potential downside of this approach is that, in the worst case, the client could extract the exact algorithm used by the server. For example, if the entire algorithm depends on a single initial comparison, the computation graph will store all the subsequent computations. Thus, the complexity of the function depends heavily on the algorithm itself. However, in most cases, the resulting function is likely to be simpler.

V. FINAL THOUGHTS

Through this exercise we see that there is an absence of a framework that can be used to implement general algorithms [15]. While execution time might be a problem, applications such as CNNs and Neural Networks are trivial to implement given the primitives. The vast majority of libraries observed either provide only basic primitives or attempt automatic code translation with limited success [2] [18]. Frameworks like SEAL, HELib, and OpenFHE [4, 5, 19] are excellent for secure computations but lack intermediate abstractions for algorithm adaptation. The former is not friendly to beginners who are trying to use the technology but don't want to know the details of the field while the latter is inconsistent in how it works.

There needs to be an intermediate framework which abstracts what can trivially be abstracted away but still make it explicit where the user needs to be careful, so that the user knows the tradeoffs of using a particular feature. If we want practicality, then we need to embrace the limitations of the current FHE scene.

REFERENCES

- [1] T. Lindeberg, *Scale Invariant Feature Transform*, 05 2012, vol. 7.
- [2] M. Naehrig, K. Lauter, and V. Vaikuntanathan, "Can homomorphic encryption be practical?" *Proceedings of the 3rd ACM Workshop on Cloud Computing Security*, pp. 113–124, 2010.
- [3] S. Chhabra and et al., "A survey on fully homomorphic encryption: An engineering perspective," *IEEE Access*, vol. 8, pp. 217 050–217 073, 2020.
- [4] Microsoft, "Seal (simple encrypted arithmetic library)," 2017. [Online]. Available: <https://github.com/microsoft/SEAL>
- [5] S. Halevi and V. Shoup, "Helib," 2014. [Online]. Available: <https://github.com/homenc/HELlib>
- [6] T. Contributors, "Tenseal: A library for encrypted tensor computation," 2020. [Online]. Available: <https://github.com/OpenMined/TenSEAL>
- [7] C.-Y. Hsu, C.-S. Lu, and S.-C. Pei, "Image feature extraction in encrypted domain with privacy-preserving sift," *IEEE transactions on image processing : a publication of the IEEE Signal Processing Society*, vol. 21, pp. 4593–607, 06 2012.
- [8] X. Liu, X. Zhao, Z. Xia, Q. Feng, P. Yu, and J. Weng, "Secure outsourced sift: Accurate and efficient privacy-preserving image sift feature extraction," *IEEE Transactions on Image Processing*, vol. 32, pp. 4635–4648, 2023.
- [9] I. Rey Otero and M. Delbracio, "Anatomy of the SIFT Method," *Image Processing On Line*, vol. 4, pp. 370–396, 2014, <https://doi.org/10.5201/ipol.2014.82>.
- [10] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," in *Advances in Cryptology – ASIACRYPT 2017*, T. Takagi and T. Peyrin, Eds. Cham: Springer International Publishing, 2017, pp. 409–437.
- [11] W. Fu, R. Lin, and D. Inge, "Fully homomorphic image processing," 10 2018.
- [12] J. H. Cheon, A. Kim et al., "Comparison algorithms for homomorphic encryption," *Cryptology ePrint Archive*, vol. 2017, p. 1164, 2017. [Online]. Available: <https://eprint.iacr.org/2017/1164>
- [13] D. Bootland, I. Iliashenko, and C. Martindale, "Optimal polynomial approximations for modular exponentiation," *Cryptology ePrint Archive*, vol. 2020, p. 1213, 2020.
- [14] G. S. Brodal, "Cache-oblivious algorithms and data structures," *Lecture Notes in Computer Science*, vol. 2497, pp. 268–286, 2001.
- [15] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, A. Ravi, and J. McMahan, "Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy," *International Conference on Machine Learning*, pp. 201–210, 2016.
- [16] H. Qin and et al., "Privacy-preserving sift: A secure framework for image feature extraction," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2068–2084, 2018.
- [17] M. Abadi and et al., "Tensorflow: A system for large-scale machine learning," *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pp. 265–283, 2016.
- [18] C. Marcolla, V. Sucasas, M. Manzano, R. Bassoli, F. H. Fitzek, and N. Aaraj, "Survey on fully homomorphic encryption, theory, and applications," *Cryptology ePrint Archive*, Paper 2022/1602, 2022. [Online]. Available: <https://eprint.iacr.org/2022/1602>
- [19] O. D. Team, "Openfhe library," 2021. [Online]. Available: <https://github.com/openfheorg/openfhe-development>