Fully Homomorphic Encryption Operators for Score and Decision Fusion in Biometric Identification

Tilak Sharma
University at Buffalo
Buffalo, NY, USA
tilaksha@buffalo.edu

Mahika Wason
University at Buffalo
Buffalo, NY, USA
mahikawa@buffalo.edu

Vishnu Boddeti
Michigan State University
East Lansing, MI, USA
vishnu@msu.edu

Arun Ross
Michigan State University
East Lansing, MI, USA
rossarun@msu.edu

Nalini Ratha
University at Buffalo
Buffalo, USA
nratha@buffalo.edu

***Abstract*—The principle of biometric fusion, which entails combining multiple biometric matchers, is often used to (a) improve recognition accuracy and (b) increase the security of biometric systems. However, fusion can expose information generated by individual biometric matchers that an adversary can exploit. This paper explores the possibility of performing score-level and decision-level fusion by utilizing fully homomorphic encryption (FHE) for enhanced security and privacy. In the context of decision-level and score-level fusion, we appropriate a comparison algorithm that can operate on fully homomorphically encrypted inputs. Furthermore, for score-level fusion, we perform score normalization in the encrypted domain, thereby enhancing the privacy and security of the score data. Experiments on the NIST BSSR1 dataset suggest that FHE can provide a viable solution for securing biometric scores and decision data while retaining their utility in fusion. The contributions of this paper are as follows: (a) leveraging and implementing FHE-compatible operations in a biometric identification framework; and (b) evaluating the performance of such a framework on a real-world dataset.**

I. Introduction

Biometric systems use a person's physical or behavioral characteristics, such as fingerprints, face, and iris, to establish their identity. Unimodal biometric systems, which rely on a single biometric trait, have several limitations. For one, such systems can be more easily compromised. For instance, fingerprint systems can be tricked using fake or lifted fingerprints, face systems can be fooled using a high-quality facial photograph or mask, and iris systems can be bypassed using textured contact lenses. Further, a single biometric trait may not offer the desired recognition accuracy in some large-scale applications [25]. In this context, using multi-biometric systems has gained traction [27], [28]. Biometric fusion combines multiple biometric modalities (e.g., face and gait or fingerprint and iris) to enhance the accuracy and reliability of biometric systems. Fusion can be accomplished at different levels, such as feature-level, score-level, or decision-level (other levels include data-level and rank-level). Feature-level fusion combines the features of different modalities to create a new feature set; score-level fusion combines the comparison scores produced by different matchers/modalities in order to render the final decision; and decision-level fusion combines the output of the decision by individual modalities to generate the final decision. Individual decisions in identity verification systems typically take on a binary form indicating a match or a non-match.

In addition to securing features, securing biometric scores is equally important. Biometric scores represent the degree of similarity or dissimilarity between the biometric samples of an individual and the enrolled template in a biometric database. If biometric scores are not securely stored and transmitted, they can be vulnerable to attacks, such as spoofing [24], replay attacks, or injection attacks [30]. Spoofing involves presenting fake or altered biometric samples to the biometric system, while a replay attack involves capturing and replaying legitimate biometric samples to bypass the authentication process. If these attacks are successful, they can compromise the security and privacy of individuals and organizations by allowing unauthorized access to sensitive information and resources. Therefore, it is crucial to secure biometric scores by using strong encryption, secure transmission protocols, and secure storage techniques to prevent unauthorized access, modification, or theft of biometric data.

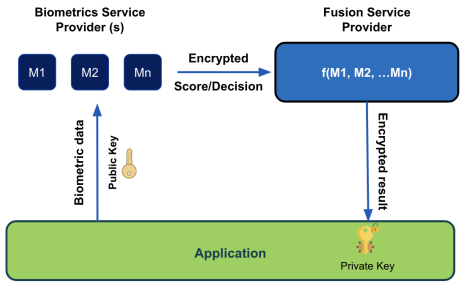


Fig. 1. A cloud service scenario with the need for encrypted processing and the associated threat model.

With cloud services being a popular method for biometrics deployment, arriving at a final biometric authentication decision is critical. In such a scenario, one can imagine three parties being involved, as shown in Figure 1. First, the query is generated by the *application interface*, which sends data to the *biometric service providers* (e.g., biometric matchers). Next, we add the *fusion layer service* that processes the output of the biometric service providers and sends the results back to the application interface. The comparison scores and individual decisions rendered by each biometric service provider can reveal the final decision before it is made. Hence, it is necessary to encrypt the decisions and scores the biometric

service providers produce. The final recommendation to the application interface should be made after the fusion engine fuses the intermediate scores or decisions in their encrypted form. The only party to be able to view the final results should be the application interface with the private key.

We propose encrypted score/decision-level fusion for biometrics in such a scenario. To the best of our knowledge, this is the first work to address secure score/decision level fusion using non-interactive homomorphic encryption to facilitate biometric cloud services while mitigating concerns about the scores or decisions being exploited by an adversary.

In the above scenario, the **threat model** is as follows. The application layer sends biometric data AND the public key to the biometric service provider. Each biometric service (e.g., face, fingerprint, etc.) provider will perform matching and generate a score/decision. They will encrypt the score/decision and send it to the fusion layer where the encrypted fusion will happen. The result is sent to the application layer which will decrypt with the secret key. We assume that the biometrics service providers will always follow protocol to encrypt the scores/decisions and send them to the fusion service provider. Lastly, we assume that the biometric service provider is not malicious. While this paper focuses on securing the *fusion service*, the *biometric matching service*, and thus the end-to-end biometric fusion system, can also be secured by encrypting the query and gallery performing the matching [9], [15] in the encrypted domain.

II. Encryption and FHE schemes

Encryption is vital in securing sensitive data from unauthorized access or modification. It involves transforming plaintext data into ciphertext using a cryptographic algorithm and a secret key. Only authorized parties with the private key can decipher the ciphertext back into plaintext. In this paper, we focus on a fully homomorphic encryption (FHE) scheme, which allows computation on encrypted data without the need for decryption. It is important to note that there are several types of homomorphic encryption, including, Partially Homomorphic Encryption (PHE), which allows addition or multiplication; Somewhat Homomorphic Encryption (SHE), which allows limited computation on ciphertexts; Leveled Homomorphic Encryption (LHE) which allows computation on ciphertexts of limited depth with an option to increase the depth by using multiple levels of encryption and Fully Homomorphic Encryption (FHE) which allows computation on ciphertexts of any depth and complexity.

Our work uses the CKKS encryption scheme that allows operations over encrypted vectors of complex numbers [11]. Over the other available FHE schemes (e.g., BGV [10], BFV [18]), CKKS offers operations on floating point numbers. CKKS also offers post-quantum security for an appropriate choice of encryption parameters [3].

Three keys are involved in the CKKS scheme: a secret key sk, a public key pk, and an evaluation key evk. The details of the scheme's functions are as follows: **Key Generation:** Generates all the three keys described above: a secret key for decryption sk, a public key for encryption pk, and an evaluation key for homomorphic multiplication evk; **Encryption:** The plaintext polynomial is encrypted to generate the ciphertext using the secret key into a set of two polynomials; **Decryption:** Given a ciphertext comprised of two polynomials, apply the secret key and retrieve a plaintext polynomial. The two basic operations that are part of the scheme include: **Addition:** A simple sum of the ciphertexts translates to homomorphic addition; **Multiplication:** Multiplication of ciphertexts is polynomial multiplication that results in three polynomials.

One of the challenges in an FHE scheme is the accumulation of noise as the computation depth increases. A process known as $bootstrap$ is needed to refresh the ciphertext and reduce the noise in the ciphertext. This process is computationally expensive but the only way to evaluate deeper circuits. There are several publicly available open-source versions of the CKKS scheme, including HEAAN [11], SEAL [1], and HELib [21]. We have opted for HEAAN since it supports *bootstrap*. The user in the HEAAN [11] has to handle relineralization to restrict the size of resultant ciphertexts.

III. Prior Work

The protection of biometric templates' privacy has been addressed using cryptographic tools such as oblivious transfer, homomorphic encryption, secret sharing, and garbled circuits. These tools are commonly employed in the semi-honest threat model to achieve security. Operating protocols in the encrypted domain present challenges due to their high complexity, necessitating optimization at various levels. In the encrypted domain, efficient implementations are crucial, favoring algorithms with lower complexity, even if they sacrifice some accuracy.

Higher security guarantees are essential to meet the requirements imposed by the General Data Protection Regulation (GDPR) and safeguard against malicious attackers. SEMBA [6] presents a comprehensive review of existing works addressing security concerns in biometric authentication. Previous proposals by Kantarcioglu and Kardes [23], Abidin [2], Pathak and Raj [26], and others have explored various techniques, such as dot product and equality checks, homomorphic encryption, and garbled circuit techniques, to protect biometric data against malicious attacks. However, practical implementation details were lacking in some cases, while other approaches required decryption of the final result, potentially introducing security vulnerabilities. SEMBA [6] focuses on a multi-biometric authentication protocol that preserves privacy by utilizing face and iris recognition. It primarily focuses on the SPDZ framework, a two- or multi-party computation protocol designed to provide secure computations against adversaries. It utilizes somewhat homomorphic encryption and secret-sharing techniques. The paper uses the well-known sum rule for fusing face and iris templates. It should be noted that this protocol solely handles integers. The SEMBA protocol entails communication between the client and the server, including the transmission of encrypted data. This communication over-

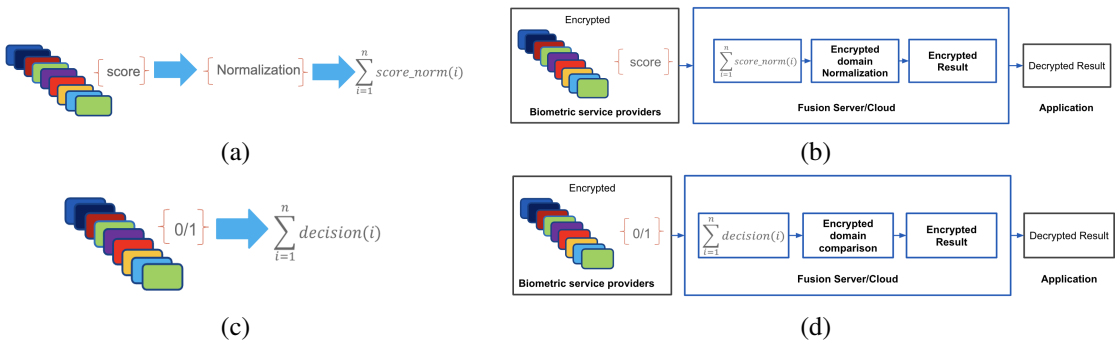


Fig. 2. (a) and (b) Score level fusion (Unencrypted and encrypted), (c) and (d) Decision level fusion (Unencrypted and encrypted).

head may introduce additional latency and potential security vulnerabilities if not managed effectively.

Early biometric systems driven by HE were based on partially homomorphic encryption (PHE) schemes applied to numerous biometric modalities such as face, iris, and fingerprints [4], [5], [8], [19], [31], [32]. More recently, Gomez-Barrero et al. [20] developed a general framework for template-level fusion based on homomorphic encryption. FHE-based work has been reported by Boddeti [9], which demonstrated the ability to match face templates in the encrypted domain. Engelsma et al. [16] proposed an efficient way to search encrypted templates by combining a novel encoding scheme with feature compression. Drozdowski et al. [14] proposed an indexing scheme by using a tree search structure created by fusing similar templates. Bassit et al. [7] introduced a homomorphic encryption-based biometric matching scheme to eliminate costly homomorphic multiplication operations. Most recently, Sperling et al. [29] proposed a biometric template fusion method in FHE. In contrast to this body of work, we leverage fully homomorphic encryption for score/decision-level fusion in this paper.

IV. Proposed Encrypted Fusion Algorithm

Since fully homomorphic encryption (FHE) can compute any arbitrary function directly on encrypted data, it is an attractive option for privacy-preserving biometrics applications. Therefore, the results of the computations are only available to one with access to the private key used in setting up the cryptosystem for FHE.

In order to model the biometric fusion system, we assume the availability of m biometric classifiers for fusion, each of which provides a score/decision in encrypted form. Our objective is to design (i) a customized decision-level fusion in FHE and, (ii) a score-level fusion algorithm as shown in Figure 2. Additionally, we aim to perform encrypted score-level fusion using encrypted score normalization functions. In both cases of decision or score fusion, the last stage of the fusion process requires a comparison to a threshold. When a weighted fusion scheme is needed, the threshold is adjusted accordingly.

A. Comparison Algorithms

While in theory CKKS can compute any arbitrary function, in practice, they support homomorphic addition and multiplication. Beyond that, many functions need to be estimated using polynomial approximations of the intended function. A compare function can be defined as comp(a,b) = 0 if a<b; 1 if a>b; and 0.5 otherwise. A compare function requires a non-arithmetic operation not supported by the FHE. So a polynomial approximation is necessary. The usual polynomial approximation methods, such as minimax [17], find approximate polynomials with a minimal degree on a target function for a certain error bound. However, considering that the CKKS scheme can only support a limited computation depth, the computational complexity to evaluate high-degree polynomials makes it highly impractical and inefficient to obtain approximate results. Recently, to resolve this problem, Cheon et al. [12] defined a new iterative definition: $comp(a,b) = \lim_{k\to\infty} \frac{a^k}{(a^k+b^k)}$ achieving a $\Theta(\alpha \log(\alpha))$ computational complexity to obtain approximate values within an error rate $2^{-\alpha}$.

Later Cheon et al. [12] proposed a new comparison method by approximating the sign function using a composite polynomial. In the same work, they also showed that faster convergence is possible by using a mixed composition ($g(x)$ and $f(x)$ in Table I and II) of polynomials. Both these functions have a common theme of iteratively computing the results. This helps us decide the resolution and computational depth needed in an application. Additionally, they also show how to systematically devise polynomials f and g. Using these functions consumes significant multiplicative circuit depth. Hence, one has to limit the number of iterations without impacting the result expected in the application at hand such as the biometrics fusion.

The two algorithms based on [13] definition are shown in algorithms 1 and 2. We evaluate the performance of the `comp` and `compG` algorithms in Table I and II (Interchanged as `compA` and `compB` respectively) on encrypted biometric data. While `compA` has two parameters - (n and d), `compB` has three parameters - (n, d_g and d_f): n for the degree of the polynomial, d and d_f for the number of iterations for the function $f(x)$, and d_g for the number of iterations for the

1: **function** COMPA(a, b, n, d)
2: $x \leftarrow a - b$
3: **for** $i \leftarrow 1$ to d **do**
4: $x \leftarrow f(n, x)$
5: **end for**
6: **return** $(x + 1)/2$
7: **end function**

$$f_1(x) = -\frac{1}{2}x^3 + \frac{3}{2}x$$
$$f_2(x) = \frac{3}{8}x^5 - \frac{10}{8}x^3 + \frac{15}{8}x$$
$$f_3(x) = -\frac{5}{16}x^7 + \frac{21}{16}x^5 - \frac{35}{16}x^3 + \frac{35}{16}x$$
$$f_4(x) = \frac{35}{128}x^9 - \frac{180}{128}x^7 + \frac{378}{128}x^5 - \frac{420}{128}x^3 + \frac{315}{128}x$$

TABLE I
ALGORITHM COMPA [12] AND ITS ASSOCIATED POLYNOMIAL f_n.

function $g(x)$ in `compB`. The first algorithm, `compA(a, b, n, d)`, takes four inputs: a, b, n, and d. It computes the value x = a - b and then applies the function $f(n, x)$ to x, d times. Finally, it returns the value (x+1)/2.

The second algorithm, `compB(a, b, n,` d_g`,` d_f`)`, takes five inputs: a, b, n, d_g, and d_f. It computes the value x = a - b and then applies the function g(n, x) to x for d_g iterations, followed by applying the function f(n, x) to x another d_f times. Finally, it returns the value (x+1)/2. The second algorithm performs better than the first because it applies two different functions, g(n, x) and f(n, x), to x in sequence, whereas the first algorithm applies only f(n, x). Using g(n, x) likely introduces more variation in the values of x than using only f(n, x), allowing for more diverse computation and potentially better performance. Additionally, using two different functions may allow for more effective cancellation of errors that might be introduced during the computation.

1: **function** COMPB(a, b, n, d_g, d_f)
2: $x \leftarrow a - b$
3: **for** $i \leftarrow 1$ to d_g **do**
4: $x \leftarrow g(n, x)$
5: **end for**
6: **for** $i \leftarrow 1$ to d_f **do**
7: $x \leftarrow f(n, x)$
8: **end for**
9: **return** $(x + 1)/2$
10: **end function**

$$g_1(x) = -\frac{1359}{2^{10}}x^3 + \frac{2126}{2^{10}}x$$
$$g_2(x) = \frac{3796}{2^{10}}x^5 - \frac{6108}{2^{10}}x^3 + \frac{3334}{2^{10}}x$$
$$g_3(x) = -\frac{12860}{2^{10}}x^7 + \frac{25614}{2^{10}}x^5 - \frac{16577}{2^{10}}x^3 + \frac{4589}{2^{10}}x$$
$$g_4(x) = \frac{46623}{2^{10}}x^9 - \frac{113492}{2^{10}}x^7 + \frac{97015}{2^{10}}x^5 - \frac{34974}{2^{10}}x^3 + \frac{5850}{2^{10}}x$$

TABLE II
ALGORITHM COMPB [12] AND ITS ASSOCIATED POLYNOMIAL g_n. THE POLYNOMIAL f_n IS THE SAME AS IN THE COMPA ALGORITHM.

We conducted experiments using different combinations of values for n ranging from 1 to 4, d from 1 to 4, d_g + d_f from 2 to 4, and the difference between the two comparison numbers, i.e., $a - b$ from -0.5 to 0.5. It can be observed that higher polynomial degrees (n) and a larger number of iterations (d) yield better approximations and hence better comparison results. However, FHE-aware comparators become less accurate if the two numbers being compared are closer. Finally, it is to be noted that `CompB` outperforms `CompA` in terms of accuracy and speed for close cases. In the context of a multimodal system with m=9 different biometric models for fusion, the extreme cases are pretty quickly handled, as shown in Figures 4.

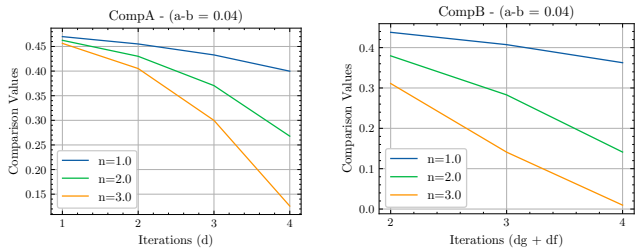


Fig. 3. `CompA` and `CompB` for close numbers as a function of the polynomial degree and the number of iterations. With four iterations, and n=3, the convergence is the fastest.

In homomorphic encryption, the multiplicative depth refers to the maximum number of times two ciphertexts can be multiplied together before the result must be decrypted. This poses a challenge to homomorphic encryption schemes as there is a trade-off between the level of computation that the scheme can support, represented by the maximum multiplicative depth, and the size of the ciphertexts and the noise that accumulates during the computation.

Considering the effect of the number of iterations and polynomial degrees on the multiplicative depth in FHE is crucial. The multiplicative depth increases linearly 5 with the number of iterations and exponentially with the degree of the polynomial due to the power computation involved. Therefore, when selecting the parameters of comparison algorithms, it is essential to account for the potential increase in multiplicative depth to ensure that the computation remains within the limit of the encryption scheme.

B. Score Normalization

Score normalization is a critical step in multimodal biometric systems to ensure that the scores obtained from different biometric modalities are on a common scale and can be combined effectively. Extending the conclusions from [22], applying min–max, z-score, and tanh normalization schemes followed by a simple sum of scores fusion method results in better recognition performance compared to other methods.

Min-max and sum rule normalization are popular score normalization methods, particularly in multimodal biometric systems. Min-max normalization maps the scores from different modalities to a common range (typically 0 to 1), allowing easy comparison. The sum rule is a straightforward and efficient approach to normalizing scores in biometric recognition systems. It has the added benefit of ensuring that the scores are consistent and can be compared across different recognition experiments, making it an essential tool for achieving optimal performance.

Our study employs a multimodal biometric system that utilizes encrypted scores and unencrypted min-max ranges

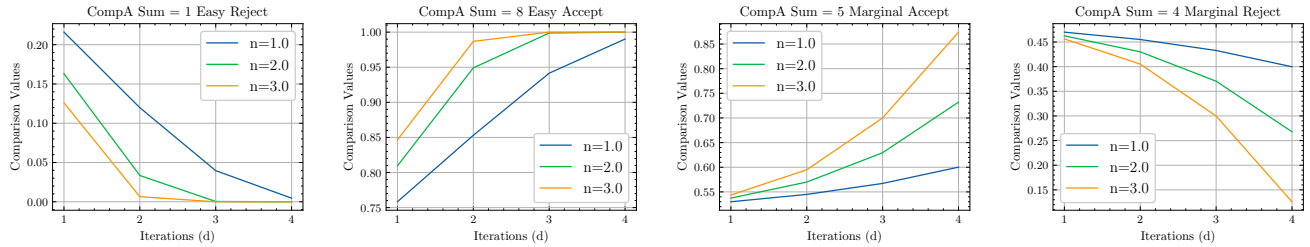


Fig. 4. CompA results for extreme cases, defined as the numbers being compared being too close in contrast to the easy cases where the numbers are far apart. The results are best for n=3 and d=4.

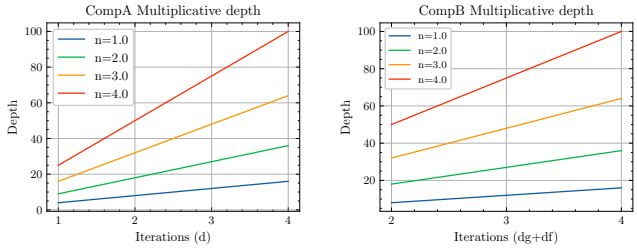


Fig. 5. CompA and CompB Multiplicative depth. As the degree and iterations grow, the multiplication depth increases linearly. We need to pay attention to the multiplicative depth so as not to hit the bootstrap threshold.

for score normalization. Using the min-max normalization method, we normalize the encrypted scores by mapping them to a common range. These normalized scores are then combined or fused by computing their average. The fused score is assessed by comparing it to a predefined threshold using the $compB$ algorithm. Notably, the results in the encrypted domain align with those in the plaintext, indicating a consistent outcome since the division is performed using a plaintext constant.

C. NIST BSSR score dataset

In addition to the simulated data, we also tested our algorithm on NIST BSSR1 - a publicly available multi-modal score dataset involving face and fingerprint matcher scores from multiple vendors with a total of 517 identities. This dataset allowed us to evaluate biometric fusion in both verification and identification scenarios, providing a rich set of mated and non-mated pairs for analysis.

We first normalized each of the four modalities and then applied a threshold to the fused scores for performance evaluation. Notably, the identification scenario was of particular interest in the Fully Homomorphic Encryption (FHE) setting due to its ability to parallelly process a large number of records in the database. By processing 2^{14} or $16,384$ scores at once, we obtained the identification results efficiently.

Result Analysis: After comparing the two algorithms with varying parameters, we found that $compB$ is much faster with a small number of iterations. Although its error rate increases as the iterations decrease, it still outperforms $compA$ as the error is still significantly below $compA$. The comparison results obtained using $compB$ are within an acceptable error range relative to $compA$, with a nearly twice speedup. Fine-tuning the parameters of the algorithms makes it possible to strike a balance between accuracy and computation time, depending on the required level of accuracy and the trade-off with computation time.

Table III displays the computation time for two comparison algorithms using the same degree of the polynomial and the total number of iterations. Algorithm $compB$ matches the accuracy achieved by $compA$ while requiring fewer iterations to converge, rendering it a faster alternative as can be seen in Figures 3 6. This finding indicates that choosing the appropriate comparison algorithm can significantly impact the overall performance of homomorphic encryption schemes. Such optimization is crucial, especially when dealing with large-scale computations, as it can reduce computation time and improve the system's efficiency.

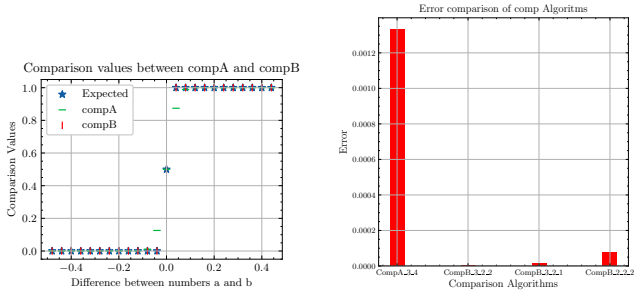
n	d	d_g	d_f	compA (s)	compB (s)
3	4	2	2	34.45	34.47
3	4	2	1	35.21	29.21

TABLE III
COMPA AND COMPB COMPUTATION TIMES IN (S) FOR DIFFERENT PARAMETER SETUP.

NIST BSSR Results: For the identification scenario, we selected a threshold value of 0.386, determined from the ROC of the unencrypted evaluation of 517x517 score entries. This threshold yielded promising results, with 499 True Positives, 18 False Negatives, and $266,772$ True Negatives. Out of the 517 true identities present in the dataset, 515 identities exhibited top comparison score matches (rank one score), indicating the effectiveness of our approach in correctly identifying individuals.

Furthermore, we measured the practicality of our approach by evaluating the time taken for each batch of 16,384 comparisons. The results showed that each batch required $34s$ of execution time and only $10s$ of execution time upon using multithreading, which is equivalent to about 2.07 and 0.61 msec/comparison, respectively, demonstrating the efficiency and real-world applicability of our biometric fusion technique.

FHE-based algorithms are widely recognized to exhibit considerably higher execution times compared to cleartext



(a) (b)

Fig. 6. (a) Comparison of algorithms for $n = 3$ and 4 iterations (d, $d_g + d_f$). Most of the time, the comparison output matches with the cleartext algorithm; (b) Errors of comp algorithms with different combinations of n, d, d_g, and d_f. The smallest error is achieved with CompB with $n = 3$, $d = 2$, $d_g = 2$, and $d_f = 2$.

computations. On average, the comparison operation takes approximately 32 seconds to complete. However, it is noteworthy that by employing multithreading, the elapsed time significantly decreases to approximately 10 seconds on average.

V. Conclusions

In this paper, we proposed the first non-interactive end-to-end homomorphically encrypted multimodal decision-level and feature-level fusion and matching system. From an inference perspective, we carefully analyzed different ways to compute a comparator function based on polynomial approximation schemes suitable for score and decision-level fusion. Experimental results show that our approach can handle fusion due to approximations induced by FHE constraints while being practically feasible, taking about 32s of single-threaded execution time and 10s in a multithreaded setup using 8 threads, to fuse encrypted scores and decision vectors of size up to 2^{14}. We presented results on the NIST BSSR-1 dataset in the context of an identification scenario where our method demonstrated nearly identical matches to the unencrypted domain with minimal errors, affirming its practicality for real-world applications.

Acknowledgement: This material is based upon work supported by the Center for Identification Technology Research and the National Science Foundation under Grant Nos. 1822190 and 1841517.

References

[1] Microsoft SEAL (release 4.0). https://github.com/Microsoft/SEAL, 2022.

[2] A. Abidin. On privacy-preserving biometric authentication. 05 2016.

[3] M. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, K. Lauter, et al. Homomorphic encryption standard. In *Protecting Privacy through Homomorphic Encryption*. 2021.

[4] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. D. Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri, A. Piva, et al. A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates. In *IEEE International Conference on Biometrics: Theory, Applications, and Systems (BTAS)*, 2010.

[5] M. Barni, G. Droandi, and R. Lazzeretti. Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing. *IEEE Signal Processing Magazine*, 32(5):66–76, 2015.

[6] M. Barni, G. Droandi, R. Lazzeretti, and T. Pignata. SEMBA:secure multi-biometric authentication. *IET Biometrics*, 8, 11 2019.

[7] A. Bassit, F. Hahn, R. Veldhuis, and A. Peter. Multiplication-free biometric recognition for faster processing under encryption. In *IEEE International Joint Conference on Biometrics (IJCB)*, 2022.

[8] M. Blanton and P. Gasti. Secure and efficient protocols for iris and fingerprint identification. In V. Atluri and C. Diaz, editors, *Computer Security – ESORICS 2011*, pages 190–209, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[9] V. N. Boddeti. Secure face matching using fully homomorphic encryption. *CoRR*, abs/1805.00577, 2018.

[10] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. (leveled) fully homomorphic encryption without bootstrapping. *ACM Trans. Comput. Theory*, 6(3), jul 2014.

[11] J. H. Cheon, A. Kim, M. Kim, and Y. Song. Homomorphic encryption for arithmetic of approximate numbers. In T. Takagi and T. Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 409–437, Cham, 2017. Springer International Publishing.

[12] J. H. Cheon, D. Kim, and D. Kim. Efficient homomorphic comparison methods with optimal complexity. Cryptology ePrint Archive, Paper 2019/1234, 2019. https://eprint.iacr.org/2019/1234.

[13] J. H. Cheon, D. Kim, D. Kim, H. H. Lee, and K. Lee. Numerical method for comparison on homomorphically encrypted numbers. In *International Conference on the Theory and Application of Cryptology and Information Security*, 2019.

[14] P. Drozdowski, F. Stockhardt, C. Rathgeb, D. Osorio-Roig, and C. Busch. Feature fusion methods for indexing and retrieval of biometric data: Application to face recognition with privacy protection. *IEEE Access*, 9:139361–139378, 2021.

[15] J. J. Engelsma, K. Cao, and A. K. Jain. Learning a fixed-length fingerprint representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 43(6):1981–1997, 2019.

[16] J. J. Engelsma, A. K. Jain, and V. N. Boddeti. HERS: Homomorphically encrypted representation search. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, 4(3):349–360, 2022.

[17] A. Eremenko and P. Yuditskii. Uniform approximation of sgn(x) by polynomials and entire functions, 2006.

[18] J. Fan and F. Vercauteren. Somewhat practical fully homomorphic encryption. Cryptology ePrint Archive, Paper 2012/144, 2012. https://eprint.iacr.org/2012/144.

[19] O. Goldreich. *Foundations of cryptography: volume 2, basic applications*. Cambridge University Press, 2009.

[20] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez. Multi-biometric template protection based on homomorphic encryption. *Pattern Recognition*, 67:149–163, 2017.

[21] S. Halevi and V. Shoup. Algorithms in helib. In *Annual Cryptology Conference*. Springer, 2014.

[22] A. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 38(12):2270–2285, 2005.

[23] M. Kantarcioglu. Privacy-preserving data mining in malicious model. 01 2008.

[24] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia. An evaluation of indirect attacks and countermeasures in fingerprint verification systems. *Pattern Recognition Letters*, 32(12):1643–1651, 2011.

[25] M. L. Ngan, P. J. Grother, and K. Hanaoka. Face recognition vendor test (frvt) part 4a: Morph - utility of 1:n face recognition algorithms for morph detection, 2022-07-29 04:07:00 2022.

[26] M. Pathak and B. Raj. Privacy-preserving speaker verification and identification using gaussian mixture models. *Audio, Speech, and Language Processing, IEEE Transactions on*, 21:397–406, 02 2013.

[27] A. Ross and A. K. Jain. Multimodal biometrics: An overview. In *12th European Signal Processing Conference*, pages 1221–1224, 2004.

[28] M. Singh, R. Singh, and A. Ross. A comprehensive overview of biometric fusion. *Information Fusion*, 52:187–205, 2019.

[29] L. Sperling, N. Ratha, A. Ross, and V. N. Boddeti. Heft: Homomorphically encrypted fusion of biometric templates. In *IEEE International Joint Conference on Biometrics (IJCB)*, 2022.

[30] T. Swearingen and A. Ross. Synthesizing face images from match scores. In *IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW)*, pages 292–300, 2022.

[31] J. R. Troncoso-Pastoriza, D. Gonzalez-Jimenez, and F. Perez-Gonzalez. Fully private noninteractive face verification. *IEEE Transactions on Information Forensics and Security*, 8(7):1101–1114, 2013.

[32] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. Jawahar. Blind authentication: a secure crypto-biometric verification protocol. *IEEE Transactions Information Forensics and Security*, 5(2):255–268, 2010.