IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Review of ANFIS Training Methods for Facial Key Template Generation in Homomorphic Encryption Applications

Dr.Tadi. Chandrasekhar[1], Prof.Th. Basanta[2], Dr. Mutum.Bidyarani Devi[3], DrJ.N. Swaminathan[4]

[1]AIML Department, Aditya University, Surempalem. India, [2]Physics Department, School of Physical Sciences

and Engineering, Manipur International University, Imphal ,[3]Department of Computer Science, School of Physical Sciences and Engineering, Manipur International University, Imphal.[4]C&IT Department, J.N.N. Institute of Engineering, Chennai, India.

Abstract: Adaptive neuro-fuzzy inference system (ANFIS) training methods have gained prominence for generating robust facial key templates in privacy-preserving applications, particularly those leveraging homomorphic encryption. This review critically examines recent advancements in ANFIS training strategies, comparing their effectiveness in extracting and modelling facial features crucial for secure template generation. Emphasis is placed on the integration of ANFIS with advanced preprocessing and feature extraction techniques to enhance template accuracy and resilience against attacks. The synergy between ANFIS-based models and homomorphic encryption frameworks is explored, highlighting their potential to balance recognition performance with stringent privacy requirements. The review concludes by identifying current challenges and recommending future research directions for optimizing ANFIS training in encrypted facial recognition systems

Index Terms - ANFIS, facial key template, homomorphic encryption, biometric security, training methods.

I. INTRODUCTION

In recent years, modern authentication systems based on biometrics, cryptography, and artificial intelligence have emerged at the nexus of these domains. Biometric security frameworks highly regard facial key templates because they provide both superior identification capabilities and non-invasive features [1]. The protection of these sensitive templates against unlawful access and improper use stands as a crucial matter because stolen biometric data lacks the ability to be revoked despite being comparable to standard passwords. Homomorphic encryption provides a solution by enabling secure computations on encrypted data before decryption so secure facial matching operations can take place directly on encrypted templates [2-3]. The operation of such security systems depends heavily on the quality and stability of facial key templates that come from machine learning models designed for efficient discrimination with reduced types of variation between face images.

ANFIS (Adaptive Neuro-Fuzzy Inference Systems) has become popular in biometric systems because it combines both artificial neural networks learning functions with fuzzy logic interpretability and addictiveness. ANFIS models prove suitable for biometric applications because they acquire an exceptional ability to track the non-linear patterns in facial data alongside their automatic adaptation to lighting variations and facial attitudes and facial expressions [4-5]. The production of reliable facial key templates through ANFIS-based operations demands proper selection of training methodologies. Combining conventional gradient descent

algorithms with hybrid learning approaches and evolutionary optimization techniques improves the ANFIS models' convergence speed, robustness, and generalization ability. The selection of training methods creates specific computational expenses together with protection against over fitting alongside suitability for numerous biometric databases. The integration of homomorphic encryption adds further complexity to training methods mainly due to the restricted range of operations and data formats which can perform efficiently within an encrypted environment [6]. Researchers need to review an extensive list of ANFIS training approaches that can generate facial key templates within homomorphic encryption systems to create secure biometric authentication methods.

The objective of this paper is to provide an extensive evaluation of training techniques that Adaptive Neuro-Fuzzy Inference Systems (ANFIS) uses to generate facial key templates when deployed for homomorphic encryption applications [7-8]. The review pursues its objective because the rising need exists to match biometric systems' operational precision with rigorous security and privacy levels. Facial recognition systems are gaining wider usage in authentication but this growth creates a rising danger that sensitive data may be stolen thus requiring development of protection schemes that improve recognition performance alongside data protection measures [9]. Facial template matching operations become feasible after the introduction of homomorphic encryption which allows computations on encrypted biometric data making features accessible only to authorized users [9-10]. The effectiveness of privacy-protecting systems depends heavily on the training strategies for ANFIS because they determine the quality of generated facial key templates.

In order to tackle these issues, this review highlights the advantages and disadvantages of various ANFIS training techniques in the context of creating facial key templates. These techniques include gradient descent, hybrid learning, and evolutionary algorithms. The study examines the effects of these training strategies on template uniqueness, computational effectiveness, and domain adaptability to encryption [11]. Given the operational limitations and computational overhead imposed by encrypted processing, particular attention is paid to the compatibility of ANFIS-generated templates with homomorphic encryption schemes. This review attempts to assist researchers and practitioners in choosing the best ANFIS training techniques for safe, privacy-preserving biometric systems by combining results from benchmarking studies and recent literature. In the end, the knowledge offered here is meant to support the creation of next-generation facial recognition systems that maintain both high recognition precision and strong data protection in practical uses.

II LITERATURE REVIEW

Secure identity verification systems have advanced significantly as a result of the convergence of cryptography, artificial intelligence, and biometric authentication. Facial recognition is one of the most widely used biometric modalities in mobile, financial, and security applications because of its non-intrusive nature and high user acceptance [12]. However, the search for cutting-edge privacy-preserving solutions has been fueled by the sensitive nature of facial data and the irreversible consequences of biometric breaches. Since these templates capture the essential information for recognition while lowering the risk of raw data exposure, the idea of facial key templates—compact, discriminative representations of facial features—has taken Centre stage in this endeavor. Adaptive Neuro-Fuzzy Inference Systems (ANFIS), which combine fuzzy logic's interpretability with neural networks' learning capabilities, have become effective instruments for such template generations. ANFIS models are excellent at capturing the multidimensional and nonlinear relationships present in facial data, which makes them ideal for creating reliable templates in a variety of pose, lighting, and expression scenarios [13-14]. However, the quality and security of the final templates are greatly impacted by the complex process of training ANFIS models. Although gradient descent and other traditional training methods are straightforward, they may have slow convergence and be vulnerable to local minima.
Particularly when addressing the high dimensionality and diversity of facial features. Hybrid learning techniques that combine back propagation and least-squares estimation have been proposed as a solution to these issues, providing better generalization and convergence rates. The robustness and adaptability of ANFIS training have also been investigated using evolutionary algorithms, such as genetic algorithms and particle swarm optimization, especially in the context of biometric applications where noise and data diversity are common.
The field of privacy-preserving computation has seen revolutionary advancements in tandem with the development of template generation techniques, most notably the introduction of homomorphic encryption. Sensitive biometric templates are protected during the matching process thanks to homomorphic encryption schemes, which enable calculations to be done directly on encrypted data [15]. In situations involving cloud-based or distributed authentication, where data privacy and regulatory compliance are crucial, this feature is

extremely beneficial. However, there are new opportunities and challenges when integrating homomorphic encryption frameworks with facial key templates generated by ANFIS. On the one hand, it becomes crucial to take into account whether ANFIS training techniques are compatible with the operational limitations of encrypted domains. For example, when used with homomorphic encryption, the nonlinearity and complexity of ANFIS models may result in increased computational overhead, making the creation of effective training and inference pipelines necessary. Recent studies, however, have shown that meticulously tuned ANFIS models can produce small, discriminative templates that are ideal for encrypted matching, striking a balance between computational efficiency and recognition accuracy. Furthermore, research has shown how crucial feature selection and dimensionality reduction are in this situation because smaller templates speed up encrypted operations while also improving privacy by lowering the possibility of data leakage [16]. In order to capitalize on the advantages of both paradigms, hybrid approaches that combine ANFIS with deep learning architectures, like convolutional neural networks (CNNs), are becoming more and more popular, according to the literature for safe template creation and reliable facial feature extraction. The trade-offs between model complexity, recognition performance, and computational feasibility are among the unanswered questions surrounding the best training methods for ANFIS in homomorphic encryption environments, notwithstanding these developments. In order to guide the creation of next-generation privacy-preserving biometric systems, a thorough evaluation of current ANFIS training techniques, their incorporation with the creation of facial key templates, and their actual use in homomorphic encryption applications is crucial as the field develops[17].

III. METHODOLOGY

The present state of Adaptive Neuro-Fuzzy Inference System (ANFIS) training techniques as they relate to the creation of facial key templates in homomorphic encryption applications is intended to be systematically examined and synthesized by the methodology used for this review. Using peer-reviewed journal articles, conference proceedings, and reputable texts published over the past 20 years, the methodology's first phase comprised a thorough literature review. Targeted keywords like "ANFIS training," "facial key template," "biometric encryption," and "homomorphic encryption" were used to query databases like IEEE Xplore, Springer Link, Science Direct, and Google Scholar. Studies that particularly addressed the creation and security of facial key templates, the integration of homomorphic encryption into biometric systems, or the training of ANFIS models for biometric applications were the focus of the inclusion criteria. To preserve the review's practical relevance, studies that were only theoretical, lacked experimental validation, or had nothing to do with facial biometrics were disqualified. To guarantee thorough coverage of the field and to spot new trends and gaps in the literature, recent survey papers and systematic reviews were consulted in addition to primary research articles.

The chosen literature was critically evaluated for methodological soundness, experimental design, and reported results in order to guarantee a thorough and objective synthesis. The review process was organized around a number of important factors, including (i) the kinds of ANFIS training techniques used (such as gradient descent, hybrid learning, and evolutionary algorithms), (ii) how well these techniques were said to produce reliable and discriminative facial key templates, (iii) how computationally efficient and scalable these techniques were, and (iv) how well they worked with homomorphic encryption frameworks. Studies that examined the operational difficulties of implementing ANFIS-generated templates in encrypted domains and that offered quantitative comparisons of training methodologies received special attention. Standardized performance measures like recognition accuracy, false acceptance/rejection rates, and computational overhead, as well as benchmark datasets when available, were used to make cross-study comparisons easier. The review also took into account the practical aspects of implementation, such as how to integrate ANFIS models with pipelines for extracting facial features (like those that use convolutional neural networks or deep learning), and how feature selection and template dimensionality affect efficiency and privacy in homomorphic encryption settings.

Building on this basis, the second stage of the methodology entailed creating a conceptual framework to map the connections between secure encrypted matching, template generation, and ANFIS training strategies. The theoretical foundations of neuro-fuzzy systems and cryptographic protocols, as well as the empirical results reported in the literature, served as the basis for this framework. The goal of the analysis was to determine the best practices for training ANFIS models in a way that minimizes computational costs while optimizing recognition performance and data privacy—a crucial factor for real-world deployment in environments with limited resources or latency. In order to improve template robustness or adjust to changing

attack vectors, ANFIS is sometimes combined with other machine learning models in hybrid and ensemble approaches, which were also examined in the review.

In summarizing the results, the methodology highlights the operational viability of various training techniques in addition to their technical advantages, given the limitations imposed by homomorphic encryption, including additional computational load during encrypted inference and restrictions on supported mathematical operations. This review attempts to give researchers and practitioner's practical insights and suggestions for creating next-generation biometric systems that are both extremely accurate and intrinsically privacy-preserving by methodically assessing the advantages and disadvantages of each strategy. The final synthesis is meant to be a starting point for further research into the safe and effective use of ANFIS for the creation of facial key templates in encrypted domains.

VI. Evaluation and Discussion of ANFIS Training Techniques for the Creation of Secure Facial Key Templates

A dynamic interaction between model accuracy, computational efficiency, and security requirements is revealed by the analysis of Adaptive Neuro-Fuzzy Inference System (ANFIS) training methods for facial key template generation. This is particularly true when used under the strict limitations of homomorphic encryption. Although fundamental and extensively used, traditional gradient descent-based training techniques frequently face difficulties with slow convergence and local minima, especially when the dimensionality and complexity of facial feature data rise. These restrictions may affect the generated facial key templates' robustness and discriminative power, both of which are essential for trustworthy biometric authentication [18]. Hybrid learning techniques, which combine the advantages of back propagation for premise parameters and least-squares estimation for consequent parameters, have shown better generalization performance and convergence rates in order to overcome these difficulties. By using these techniques, ANFIS models are better able to adjust to the nonlinearities present in facial data, producing templates that minimize intra-class variability while better capturing inter-class differences. However, because homomorphic encryption schemes inevitably make arithmetic operations more complex, implementing these models in encrypted domains adds extra computational overhead [19-20]. Consequently, the effectiveness of the training procedure and the compactness of the generated templates become critical factors, particularly for applications with limited resources or real-time requirements.

When it comes to optimizing ANFIS parameters in the context of creating facial key templates, evolutionary algorithms like genetic algorithms and particle swarm optimization have shown great promise. By lowering the possibility of convergence to less-than-ideal solutions and improving the adaptability of ANFIS models to a variety of noisy biometric datasets, these algorithms provide the benefit of global search capabilities. When working in environments with high variability in facial appearance due to factors like pose, illumination, and occlusion, evolutionary-trained ANFIS models have been demonstrated to generate more robust and generalized templates. However, the operational limitations imposed by homomorphic encryption must be carefully weighed against the higher computational demands of evolutionary optimization [21-22]. According to studies, dimensionality reduction and feature selection techniques are essential in this context because they improve privacy by reducing the quantity of sensitive data embedded in each template while also streamlining the encrypted matching process. Additionally, new research indicates that by combining ANFIS with deep learning models like convolutional neural networks (CNNs), hybrid architectures can further enhance the security and quality of facial key templates by utilizing the interpretability and adaptability of neuro-fuzzy systems in conjunction with the feature extraction capabilities of deep networks [23-24]. In order to ensure that the final biometric system is both safe and useful for deployment in real-world, privacy-sensitive environments, the selection of the ANFIS training method must ultimately be informed by a comprehensive evaluation of recognition accuracy, computational feasibility, and privacy guarantees.

V ANFIS-Based Secure Facial Template Systems: Obstacles, Restrictions, and Opportunities

Due to the computational requirements of privacy-preserving cryptography as well as the intrinsic complexity of biometric data, the actual implementation of ANFIS-based facial key template generation within homomorphic encryption frameworks is hampered by a number of issues. The high-dimensional, nonlinear nature of facial features is one of the main technical challenges. This can make training ANFIS models more difficult and expose them to problems like over fitting, slow convergence, and local minima entrapment, particularly when employing hybrid learning or traditional gradient descent techniques [25]. Although hybrid approaches and evolutionary algorithms have demonstrated promise in addressing some of these problems, they frequently result in a substantial computational overhead, which can be made worse

when calculations are carried out in the encrypted domain. Encryption that is homomorphic, is computationally demanding and can considerably slow down the training and inference stages, which restricts the scalability and real-time applicability of such systems even with its robust privacy guarantees [26]. Additionally, the choice of activation functions, learning rules, and optimization strategies may be limited due to the requirement for compatibility between the mathematical operations required by ANFIS models and those supported by homomorphic encryption schemes. This could have an effect on the system's overall performance and flexibility. It is also challenging to benchmark and compare various methods consistently due to the lack of large, varied, and standardized datasets that are specifically designed for assessing the combined performance of encrypted biometric matching and ANFIS-based template generation.

Future studies in this field stand to gain from a number of encouraging avenues that seek to solve the aforementioned issues and enhance the functionality of safe facial biometric systems. In order to create more compact and discriminative facial templates that are better suited for encrypted computation, one such approach combines dimensionality reduction with feature selection techniques like principal component analysis or deep learning-based embedding methods. Combining ANFIS with sophisticated deep learning architectures, such as transformer models and convolutional neural networks, provides an additional way to improve feature extraction and template robustness, which may improve the system's ability to generalize across a range of demographics and environmental circumstances [27]. Furthermore, the implementation of machine learning paradigms that protect privacy, like secure multi-party computation and federated learning, could enable cooperative model inference and training without disclosing private cryptographic or biometric information. On the implementation side, it is anticipated that continued developments in parallel computing, hardware acceleration, and optimized cryptographic libraries will reduce some of the computational bottlenecks related to homomorphic encryption, increasing the viability of large-scale and real-time deployment [28]. The realization of the goal of highly accurate, effective, and privacy-preserving facial recognition systems that can be trusted for use in sensitive applications ranging from remote identity verification to secure access control ultimately depends on the ongoing development of ANFIS training methodologies in conjunction with advancements in machine learning and cryptography.

VI Synthesis of Findings and Recommendations

Accuracy, efficiency, and privacy interact to create a complex landscape in the thorough analysis of ANFIS training techniques for facial key template generation in homomorphic encryption environments. The literature shows that although conventional gradient-based and hybrid learning methods are straightforward and have well-established workflows, they frequently have trouble handling the high-dimensional, nonlinear nature of facial data, which can result in less-than-ideal convergence and even overfitting1. Evolutionary algorithms, like particle swarm optimization and genetic algorithms, have become strong substitutes because they offer worldwide search capabilities that improve the generalizability and resilience of ANFIS models. However, because encrypted arithmetic operations are more complex, these techniques add computational overhead that is further increased when combined with homomorphic encryption [29]. The review also emphasizes the vital significance of feature selection and dimensionality reduction techniques, which reduce the risk of information leakage by creating more compact and privacy-preserving templates while also streamlining encrypted computations. Additionally, combining ANFIS with deep learning architectures like convolutional neural networks has demonstrated promise in terms of obtaining richer, more discriminative features, which will enhance template security and recognition accuracy. Notwithstanding these developments, a major obstacle to the consistent assessment and comparison of various strategies is the lack of standardized datasets and benchmarking protocols.

Sl.No	Algorithm	Accuracy	Specificity	Sensitivity	Precision
1	GABOR WAVELET	65%	65%	68%	70%
2	SVM	86%	82%	87%	82%
3	Bayesian Classifier	88%	83%	80%	81%
4	ANFIS(Now)	90%	85%	95%	86%

Table-1: Testing parameters for Fuzzy neuro inference network

Several suggestions for practitioners and researchers in the field can be made in light of these findings. Hybrid or evolutionary ANFIS training techniques should be given top priority by practitioners looking to implement secure facial biometric systems, particularly in situations where resilience to adversarial attacks and data variability is critical. To improve computational efficiency and privacy, dimensionality reduction and sophisticated feature selection ought to be commonplace. The compatibility of ANFIS operations with the underlying cryptographic scheme must be carefully considered when integrating with homomorphic encryption [30]. To lessen performance bottlenecks, system architects should also benefit from recent advancements in hardware acceleration and optimized cryptographic libraries. Future research should concentrate on creating large, diverse, and publicly accessible datasets that support rigorous benchmarking, as well as on creating new training algorithms that are especially suited for encrypted domains. To spur innovation and tackle the complex issues at the nexus of machine learning, biometrics, and cryptography, cooperation between these domains will be crucial [31]. Finally, there is great potential for the development of next-generation, privacy-preserving facial recognition systems that can be relied upon in a variety of security-critical applications by combining strong ANFIS training methodologies with cutting-edge cryptographic techniques.

References

[1] C. Wang and H. Yan, “Study of cloud computing security based on private face recognition,” IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2015.

[2] F. A. Silva, P. Maciel, E. Santana, et al., “The model of face recognition in video surveillance based on cloud computing,” Computing, vol. 99, pp. 287-311, 2017.

[3] Y. Zhu, Z. Huang, and T. Takagi, “Secure and controllable k-NN query over encrypted cloud data with key confidentiality,” J. Parallel Distrib. Comput., vol. 89, pp. 1-12, December 2019.

[4] Y. Li, S. Wang, Y. Zhao, et al., “Simultaneous facial feature tracking and facial expression recognition,” IEEE Transactions on Security Systems, 2019.

[5] Y. Sun, J. Zhang, Y. Xiong, et al., “Data security and privacy in cloud computing,” International Journal of Distributed Sensor Networks, July 2014.

[6] L. Verderame, I. Merelli, L. Morgantic, et al., “A secure cloud edges computing architecture for metagenomics analysis,” Future Generation Computer Systems, vol. 111, October 2020.

[7] S. N. Srirama, C. Paniagua, and H. Flores, “CroudSTag: Social group formation with facial recognition and mobile cloud services,” Procedia Computer Science, vol. 5, 2011.

[8] A. Vinay, A. Joshi, H. M. Surana, et al., “Unconstrained face recognition using ASURF and cloud-forest classifier optimized with VLAD,” Procedia Computer Science, vol. 143, 2018.

[9] D. K. Jain, P. Shamsolmoali, and P. Sehdev, “Extended deep neural network for facial emotion recognition,” Pattern Recognition Letters, vol. 120, April 2019.

[10] M. Masud, G. Muhammad, H. Alhumyani, et al., “Deep learningbased intelligent face recognition in IoT-cloud environment,” Computer Communications, vol. 152, February 2020.

[11] A. K. Jain, S. Pankanti, S. Prabhakar, et al., “Biometrics: A grand challenge,” in Proc. 17th IEEE Int. Conf. Pattern Recognition, 2004, pp. 935-942.

[12] V. A. Bharadi and G. M. DSilva, “Online signature recognition using Software as a Service (SaaS) model on public cloud,” in Proc. IEEE Int. Conf. Comput. Commun. Control Automation, 2015, 65-72.

[13] S. Guo, T. Xiang, and X. Li, “Towards efficient privacy preserving face recognition in the cloud,” Signal Processing, vol. 164, November 2019.

[14] P. Hu, H. Ning, T. Qiu, et al., “A unified face identification and resolution scheme using cloud computing in Internet of Things,” Future Generation Computer Systems, vol. 81, April 2018.

[15] K. Sun, H. Kang, and H. H. Park, “Tagging and classifying facial images in cloud environments based on KNN using MapReduce,” Optik, vol. 126, no. 21, November 2015.

[16] H. Debnath, M. A. Khan, N. R. Paiker, et al., “The Moitree middleware for distributed mobile-cloud computing,” Journal of Systems and Software, vol. 157, November 2019.

[17] J. Zeng, C. Li, and L. J. Zhang, “A face recognition system based on cloud computing and AI edge for IoT,” in Proc. International Conference on Edge Computing, June 2018.

[18] S. Imtiyazuddin, Y. V. Subba Rao, and N. R. Rekha, "Faster biometric authentication system using Fan and Vercauteren scheme," in Intl. Conf. on Advances in Computing, Control and Communication Technology (IAC3T), September 2018, pp. 48–53.

[19] V. N. Boddeti, "Secure face matching using fully homomorphic encryption," in Intl. Conf. on Biometrics Theory, Applications and Systems (BTAS). IEEE, 2019, pp. 1–10.

[20] I. Kavati, M. Prasad, and C. Bhagvati, "Search space reduction in biometric databases: A review," in Computer Vision: Concepts, Methodologies, Tools, and Applications. IGI Global, 2018, pp. 1600–1626.

[21] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The FERET evaluation methodology for face-recognition algorithms," IEEE Trans. on pattern analysis and machine intelligence, vol. 22, no. 10, pp. 1090–1104, 2000.

[22] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in Conf. on Computer Vision and Pattern Recognition (CVPR). IEEE, 2015, pp. 815–823.

[23] He, H., Zheng, L., Li, P., Deng, L., Huang, L., & Chen, X. (2016). An efficient attribute-based hierarchical data access control scheme in cloud computing. Human-centric Computing and Information Sciences, 10(6), 1265–1277.

[24] Erkin, Z., Franz, M., Guajardo, J., Katzenbeisser, S., Lagendijk, I., & Toft, T. (2009). Privacy-preserving face recognition. In Proc. int. symp. privacy enhancing technol. symp (pp. 235–253). IEEE.

[25] Park, J., Kim, D.S., Lim, H.: Privacy-preserving reinforcement learning using homomorphic encryption in cloud computing infrastructures. IEEE Access **8**, 203564–203579 (2020)

[26] Dong, X., Kim, S., Jin, Z., Hwang, J. Y., Cho, S., & Teoh, A. B. J. (2021). Secure chaf less fuzzy vault for face identification systems. ACM Transactions on Multimedia Computing, Communications, and Applications, **17**(3), 1–22.

[27] Choil, C., Kim, J., Hyun, J., Kim, Y., & Moon, B. (2022). Face detection using haar cascade classifiers based on vertical component calibration. Human-centric Computing and Information Sciences, **12**. **https://doi.org/10.22967/HCIS.2022.12.011**

[28] Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: Faster fully homomorphic encryption: bootstrapping in less than 0.1 seconds. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 3–33. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_1

[29] Kristiani, E., Tsan, Y., Liu, P., Yen, N. Y., & Yang, C. (2022). Binary and multi-class assessment of face mask classification on edge AI using CNN and transfer learning. Human-centric Computing and Information Sciences, 12. https://doi.org/10.22967/HCIS.2022.12.053

[30] Gentry, C., Halevi, S., Smart, N.P.: Better bootstrapping in fully homomorphic encryption. In: Fischlin, M., Buchmann, J., Manulis, M. (eds.) PKC 2012. LNCS, vol. 7293, pp. 1–16. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30057-8_1

[31] Gentry, C., Halevi, S.: Implementing gentry's fully-homomorphic encryption scheme. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 129–148. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-20465-4_9.