Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 8080 - 8091
Received 05 March 2021; Accepted 01 April 2021.

Real Time Object Detection and Tracking Using Open cv

M.Hemasri, S.Jesintha Singh Ranjith , M.Sacratees, M.Vidhyasagar, N.Shimmar Rahim

Department of Computer Science and Engineering
M.Kumarasamy College of Engineering ,Thalavapalyam, Karur, Tamilnadu,
India -639113.
hemasrim.cse@mkce.ac.in,jesinthasinghranjith@gmail.com,sacratees007be@gmail.com
vidhyasmithun007@gmail.com,shimmarrahim.8032000@gmail.com

ABSTRACT

Any calculation can be done on encrypted data with solely homomorphic encryption. In an insecure world, it's a useful tool for safe outsourced computing This essay discusses the secure external environment for homomorphic cryptography determining of the vector. We propose a stable matrix determinant outsourced computing scheme based on hypercube structure, an effective matrix coding technique that packs single substitution cipher structure. The matrix in the ciphertext region, according to simulation results, Finally, we show reader how to read Our proposed strategy is simple to set up as a dormancy sub-module. the terminal index Direct computation on encrypted data, stable external computing, a matrix determiner, and coding that appears to be fully homomorphic are all alternatives.

Keywords: homomorphic histology files, CNN image detection

Introduction

People can still have versatile, on-demand access to computing services while saving money on IT system purchases and maintenance of cloud computing [1]. Examples include Google Drive, Amazon AWS, Microsoft Azure, and other cloud storage services. One of the most important tools in the virtualization computing paradigm is outsourcing Customers with limited resources can even outsmart the system using cloud computing. The gathered data is returned to the customer after computation and storage on a linux machine. Outsourced processing takes advantage of the powerful capacities of mobile technology, significantly lowering local overhead out how much each item would cost Outsourcing computing has a number of benefits, but it also has a number of disadvantages. From [2] to [5] When it comes to outsourcing computing, consumer security is a major concern. As a product of both Outsourced computing can necessitate the use of confidential data, which can be stored in the cloud This could be a concern before the cloud service provider has direct access to the system. Data privacy, according to the Vulnerability Management Association [6, is still a major barrier to wide distribution of the cloud computing model. While the customer now has conceivable of using conventional encryption methods to encrypt data Prior to outsourcing, encryption techniques will be inaccessible, thus cloud servers will be unable to carry out any data on the data that has been encrypted, practical action is required. As a consequence, using a cloud service is perfect. Completely FHE[7] enables you to perform random calculations on encrypted data, making it perfect for secure outsourced computing in an untrustworthy setting. Purely homomorphic password-based applications have become popular in recent years. Various functions, ranging from simple matrix multiplication [8] - [11] to high-level functions, have been proposed .Machine learning implementations, for example [12] -A complex coding concern is vector useful measure calculus [15]. mathematics has a wide range of uses in science and engineering The efficiency of high-level applications would be significantly improved if the quality of determinant computation was improved.. The matrix has been expanded. Assume a consumer with limited resources needs to measure the cost of a product, the matrix's determinant. When matrix c is big, the poor customer will be tempted to make the matrix compute its cloud-based determinant. However, in the cloud computing paradigm, consumer data protection is a top priority since the cloud service provider has access to it. Be observant. As a result, we were motivated to develop an outsourced matrix-determinant system. A computing scheme that is entirely based on homomorphic encryption.

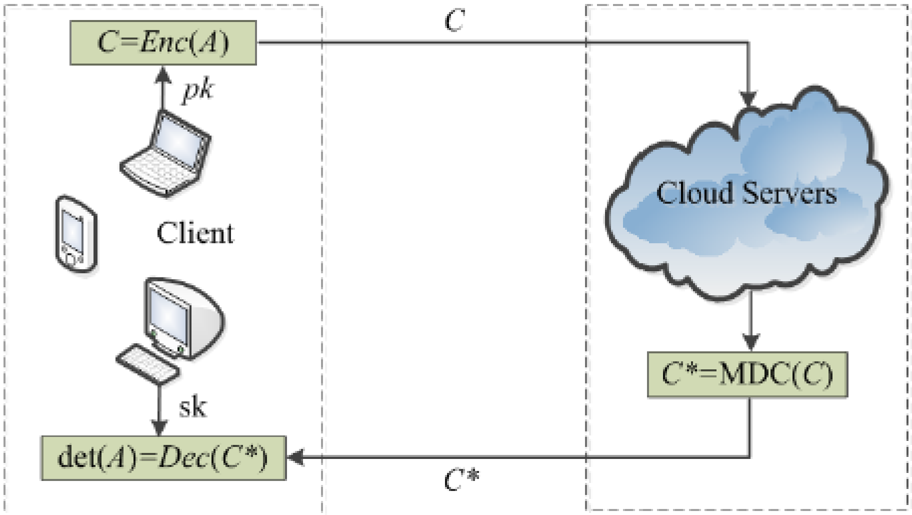

Fig. 1: Outsourced matrix determinant computing system model

Topic

ImageNet has been working on a large-scale visual recognition task for detection in depth learning since Alex Net swept the science world in 2012, far outperforming the most traditional artificial vision approaches in the literature. When it comes to image recognition, neural convolution networks stand out in artificial vision..

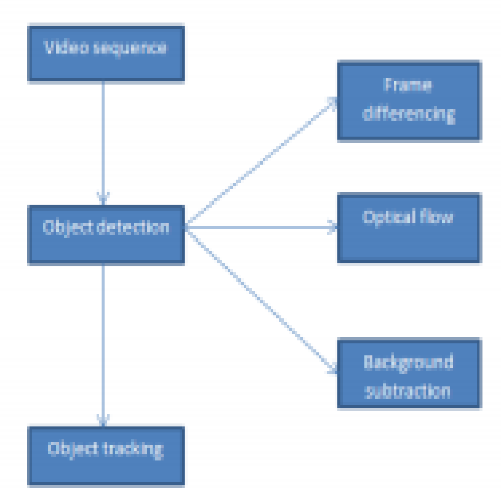

Fig. 2. Basic block diagram of detection and Tracking

Received 05 March 2021; Accepted 01 April 2021.

In this paper, detection and tracking algorithms based on SSD and portable Nets are implemented in a Python context. Object detection is the process of detecting an object's region of interest from a collection of images. Frame differencing, Optical flow, and Background subtraction are examples of different approaches. Without any prior experience of the secret key, Anyone can compute any on an epsilon element f using fully homomorphic encryption [7]. As a result, f encryption is obtained (x). Z absolutely homomorphic encryption scheme is made up of four algorithms:

- (kos) Key Gen(1): Given a bet specific surface, returns an encrypted message g and a shared secret f.
- k Enc(d, i): Generates a decrypted c C from a clear text m M and a message digest v.
- m Dec(k, co): Given a private key sk and a stream cipher c, generates a key m.
- kane, f, standard style, threonine,..., cn) Eval(pk, f, transferase, 10 mmol,..., swe) Eval(pk, f, c1, c2,... Produces a keystream c that encrypts f will use public - key cryptography pk, a fopid controllers: Mn M, and a sequence of n ciphertexts c1,..., cn C.

where + and - are M operations.

Sub topic

Methods

Network attitude represents a real security risk in the outsourcing control scheme. In this article [36], we use a non security architecture (also known as honest but curious), in which the instance is supposed to obey the protocol, but the client has the option of learning more about it.It is aware of itself. Without notice, the cloud will depart from the protocol specification, and the client will receive an error message. The quasi-honest model, on the other hand, is appropriate for the following cases.

(1) Whether a software certificate is used or built-in, it is difficult for the cloud to alter applications without being identified.

There are safeguards in place. (2) Web-based utilisations

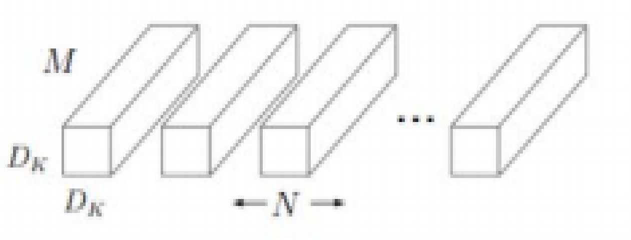

Fig. 3. Normal Convolution [2]

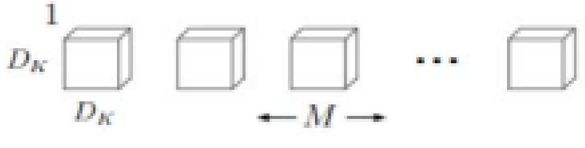

Fig. 4. Depthwise Convolution Filters [2]

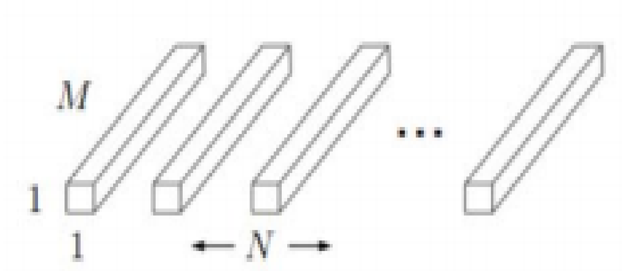

Fig. 5. Convolutional Filters called Pointwise Convolution in the context of Depthwise Separable Convolution [2].

As compared in the circuits to the set of natural distortions to the same breadth, this model uses depth wise separable convolutions, which reduces the number of parameters significantly. The development of a light weight neural network is the product of the reduction of parameters. The following formula [15] can be used to Assess the criterion of a cubic differential A denoted by the letter is the range of all iterations of a set 0 thru the (also identified as the logarithmic group on three inputs), and the sum is computed over all permutations of the set Sn. A function that rearranges the set 0 by n 1 is called a chemicals in the brain. The meaning in the I th place of the permutation is denoted by the letter I. The initial series could be reordered to for r = 3. with the number 0 p() returns a value of +1 between each permutation if the reordering given by are being achieved by sequentially interspersing entry of the original series for an even length of time, and 1 for an equal split of such intersections.

Methodology

Without knowing the private key, anyone can compute any function f in encryption x using pure homomorphic encryption [7]. As a result, the password f (x) is obtained. Four algorithms are used to construct a completely homomorphic encryption scheme: •If you're looking for a special way to express yourself (pk, sk) (1) Key Generates a public key pk and a secret key sk given a security parameter. • c Enc (pk, m): Encrypts the text c C when g is true. • m Range (sk, c): From a private key sk and an encrypted text c, generates a plain text m. •c Evaluate (pk, f, c1,..., Cn) is a function that takes a public key pk, a function f: Mn M, and a list of arguments. C generates a c-encrypted text with f's password (m1,..., cn). Addition and multiplication operations can be aided by a fully homomorphic cypher, and higher than c.M systems are + and -.Over the m-th cyclotomic polynomial ring A = Z[X]/8m, the completely homomorphic schemes BGV [37] and variants [38], [39] are described (X). The ring Ap = A/pA = Z[X]/(8m(X), p) is the plaintext space for the BGV scheme, where p is a prime. The support for single instruction multiple data (SIMD) parallel operations is a key feature of the BGV scheme and its variants [40]. The cyclotomic polynomial 8m(X) can be factorised into l distinct irreducible polynomials with degree d = (m)/l under modulo p, so that 8m(X) = Ql i=1 Fi(X)mod p. Each factor Fi(X) corresponds a plaintext slot and the following isomorphism holds. Ap ∼= Zp[X]/F1(X) × · · · × Zp[X]/Fl(X) (1 where i ∈ Z ∗ m/ < p > that rotate the underlying plaintext slots. Denote the generator) The polynomial an Ap decomposes into l-vector (a mod Fi(X))l i=1 thanks to the polynomial CRT. As a consequence, we can fit l messages into a single plaintext polynomial and perform l additions or multiplications with just one operation.As noted in [41], [42], each slot corresponds to an equivalence class of Z ∗ m/ < p > and there are automorphism mappings Ki : a(X) → a(X i) mod 8m(X)s of Z ∗ m/ < p > by {g0, g1, . . . , gd−1} where the order of gi in Z ∗ m/ < p, g1, . . . , gi−1 > is mi . If gi has the same order in Z ∗ m as in Z ∗ m/ < p, . . . >, we call i-th dimension a good dimension, otherwise it is a bad dimension. The good dimension leads to a more efficient data movement between slots. The slot-index representative set is T def = {Qd−1 i=0 g ei i mod m : ei ∈ {0, 1, . . . , mi − 1}}, which can be indexed by a vector (e0, . . . , ed−1). We get a multidimensional array called a hypercube structure from the underlying plaintext slots, with each dimension having a size of mi. The data movement operation is defined as follows for a d-dimensional hypercube structure:

- rotate1D(ct, i, k):

This method rotates the hypercube by k positions along the i'th dimension, i.e., this will move the content of slot (e0, . . . , ei, . . . , ed−1) to the slot (e0, . . . , ei + k mod mi, . . . , ed−1). It's worth noting that k can be positive or negative, and rotating by k is the same as rotating by mi k. The plaintext slots are organised into a matrix by a two-dimensional (d = 2) hypercube structure, which enables versatile data movement along rows or columns, making it an excellent tool for matrix-related operations.. Backing up each entry of the variable into stream cipher, then multiplying the matrix factor in deciding according to the type exponent, is a normal method for safe outsourced computation of matrix determinant (2). This description tool, on the other contrary, will add u! of these products will require O(n) hash-based multiplications, resulting in a substantial computational load.Further more, to represent a tuple, n 2 timestamps are needed, resulting in significant storage space costs.

Bird's division-free binary determinant estimation method, It is taken into account, as it is substantially more effective than the specification process . Despite the fact that the bracket resolution removes the first drawback, it still needs decryption to represent a loop, which requires a lot of storage space. In this part, we'll look at a bracket differential forecast method for equation A that packs the formula into a single decryption using the hexagonal lattice layout.

Consider the structure of a two-dimensional (d = 2) igg square meters cube with w - type = n and n / l >= n.

The binary A can now be packed into the concentric spheres design by padding all other positions with

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 8080 - 8091
Received 05 March 2021; Accepted 01 April 2021.

zeros. In the following, we'll assume what our method also works as well as electric motors . The client authenticates map using definitions.

$$ct_A = Enc\left(\begin{bmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,n-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,n-1} \\ \vdots & \ddots & \vdots & \\ x_{n-1,0} & x_{n-1,0} & \cdots & x_{n-1,n-1} \end{bmatrix}\right) \quad (5)$$

.

The server calculates the private key of the matrices indicator o given the cypher - text k using the formula below. This involves the three actions outlined down.

I. First, compute which accesses, as seen on the section.

Calculate g, which encrypts the and k matrix product, next.

III. Figures I and II are n times more difficult to obtain, which authenticates f in the first entry.

Given the y, let the basic eigenvalue be as follows:

Calculate h (X) from Step 1 to Step 7, which intercepts

Step 1: To get ct1, multiply the decrypted g by a mask matrix U, with all elements set to 0 in the main diagonal and below. (6) The cipher - text ct1 is as usual.

$$ct_1 = Enc\left(\begin{bmatrix} 0 & x_{0,1} & \cdots & x_{0,n-1} \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & x_{n-2,n-1} \\ 0 & \cdots & \cdots & 0 \end{bmatrix}\right) \quad (7)$$

Data Analysis

Using authentication each entry in the ciphertext and then computing the determinant of the matrix according to the specification theorem is a normal independently based approach safe calculation of the determinant of the matrix (2). On the other hand, this form of disclosure has several drawbacks. will I'm going to give you the number n!Each product requires O (n) public key products and results in there is a significant computational overhead In addition, We consider the calculating form matrix determinants without the Bird [43] section; this property is substantially better competitive than the specification method .Despite the fact that the no-partition strategy mitigates the initial disadvantage, The n2 ciphertext is still used to describe a sequence, which takes up a lot of interest the price .In this section, we'll look at how to find an undivided matrix by wrapping a matrix A in a single ciphertext using a hypercube structure. Consider the m1 m2 structure of a two-dimensional hypercube where m4 = n and m5>By filling all other positions, Matrix A can now be packaged into the matrix In addition to a large number of zeros After that, we make the call. For the sake of simplification, This source text's details can be found here. In the source text, additional translation information is needed The sides have tables. The server calculates the ciphertext of the matrix when the ciphertext c is given according to the formula below, determinant j . This is an excellent example. is made up of the three phases mentioned below.

1. First, compute the encoding as shown in the section ..
2.Calculate the encoding the and A matrix product next.
3. At the cost of increased server computational overhead will minimize communication overhead from the other direction, when the input to the comput of the matrix determinant is not freshly generated by the client but an auxiliary result from other computations, it is difficult for schemes based on the disguise scheme to provide such claude.

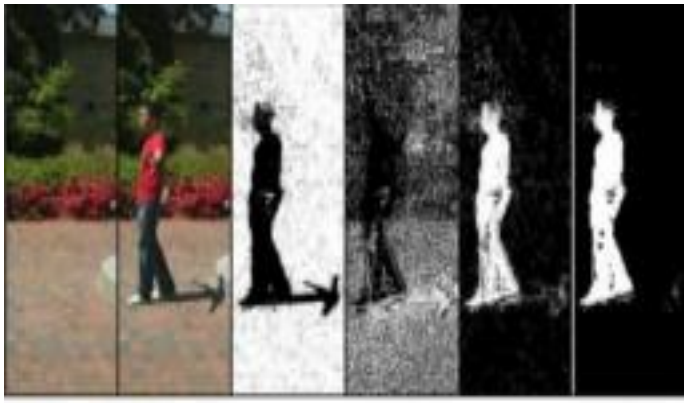

Fig.6. Detection of human from background subtraction

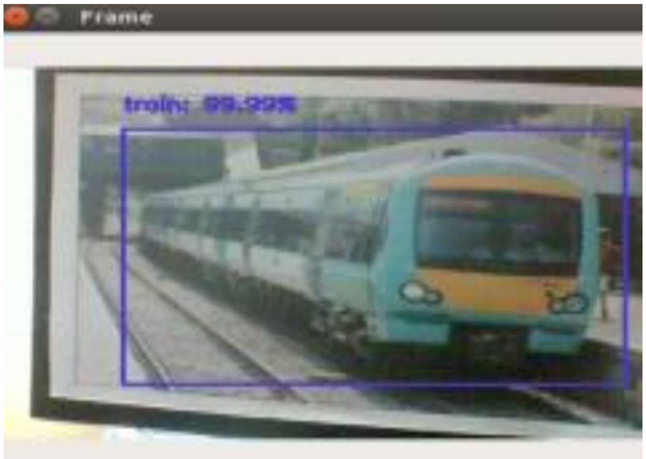

Fig. 7. Detection of Train with confidence level of 99.99%

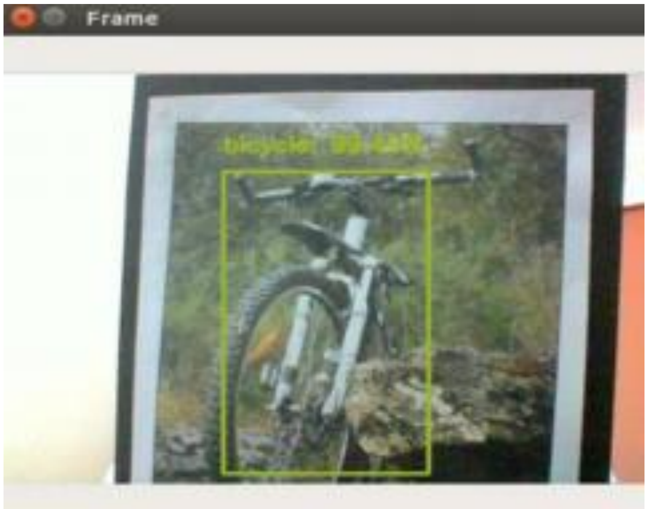

Fig.8. Detection of Bicycle with confidence level of 99.49%

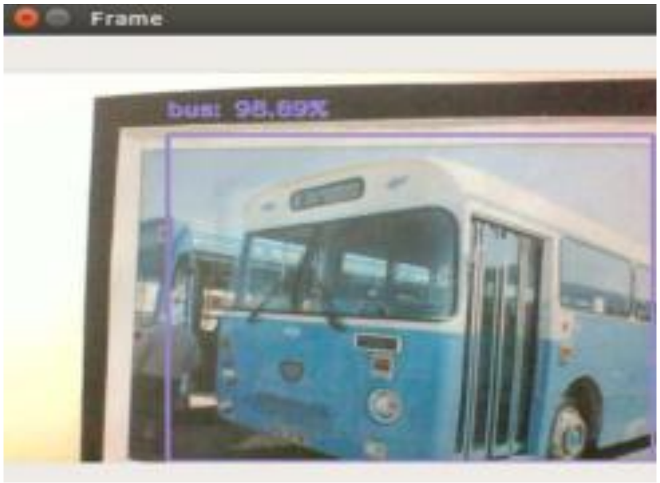

Fig.9.Detection of Bus with confidence level of 98.68%

Bicycle, bus, train, and dog identification in real time with confidence levels of 99.49 percent, 98.68 percent, 99 percent, and 97.77 percent, respectively. The model was trained to detect 21 different object classes, such as a dog, a motorcycle, a human, a boat, and a bicycle, with a 99 percent accuracy.

Results

Using purely homomorphic encryption, this paper explores the computation of stable extrinsic matrix determinants. Based on the non-divisional computation method and the structure of a hypercube, we propose an extrinsic computation scheme for the matrix determinant that is both efficient and stable. We can easily measure the determinant of the matrix in encrypted t data using our diagram. Other trustworthy outside computing applications Other stable external computing applications related to matrix operations, such as matrix factoring and linear equation solving systems based on hypercube structure, will be studied in the future

Conclusion

In real-time situations, the SSD algorithm is used to detect objects. SSD has also shown findings with a high degree of trust. The main goal of the SSD algorithm is to detect and monitor different objects in a real-time video sequence. This model performed admirably on the object trained in terms of detection and tracking, and it can be used in specific scenarios to identify, monitor, and react to goal basic camera footage objects By allowing for security, order, and benefit, this real-time ecosystem analysis can produce fantastic results for any enterprise. Extending the work to track ammunition and firearms in the event of a terrorist attack in order to alert authorities. The model can be implemented in surveillance cameras, drones, and other devices to detect attacks in places where weapons are banned, such as schools, government offices, and hospitals.

References

[1] P. Mell and T. Grance, ``The NIST de_nition of cloud computing,'' U.S. Dept. Commerce, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, Tech. Rep. SP 800-145, 2011, doi: 10.6028/NIST.SP.800 145.

[2] J. Tang, Y. Cui, Q. Li, K. Ren, J. Liu, and R. Buyya, ``Ensuring security and privacy preservation for cloud data services,'' *ACM Comput. Surv.*, vol. 49, no. 1, pp. 1_39, Jul. 2016.

[3] T. Fun and A. Samsudin, ``A survey of homomorphic encryption for outsourced big data computation,'' *KSII Trans. Internet Inf. Syst.*, vol. 10, no. 8, pp. 3826_3851, 2016, doi: 10.3837/tiis.2016.08.022.

[4] Murugesan, M., Thilagamani, S. ,” Efficient anomaly detection in surveillance videos based on multi layer perception recurrent neural network”, Journal of Microprocessors and Microsystems, Volume 79, Issue November 2020, https://doi.org/10.1016/j.micpro.2020.103303

[5] Y. Yang, X. Huang, X. Liu, H. Cheng, J. Weng, X. Luo, and V. Chang, ``A comprehensive survey on secure outsourced computation and its applications,'' *IEEE Access*, vol. 7, pp. 159426_159465, 2019, doi: 10.1109/ACCESS.2019.2949782.

[6] Thilagamani, S., Nandhakumar, C. .” Implementing green revolution for organic plant forming using KNN-classification technique”, International Journal of Advanced Science and Technology, Volume 29 , Isuue 7S, pp. 1707–1712

[7] C. Gentry, ``Fully homomorphic encryption using ideal lattices,'' in *Proc. 41st Annu. ACM Symp. Theory Comput. (STOC)*, New York, NY, USA, 2009, pp. 169_178.

[8] A. Page, O. Kocabas, S. Ames, M. Venkitasubramaniam, and T. Soyata, ``Cloud-based secure health monitoring: Optimizing fully-homomorphic encryption for streaming algorithms,'' in *Proc. IEEE Globecom Work- shops*, Austin, TX, USA, Dec. 2014, pp. 48_52, doi: 10.1109/GLO-COMW.2014.7063384.

[9] D. H. Duong, P. K. Mishra, and M. Yasuda, ``Ef_cient secure matrix multiplication over LWE-based

homomorphic encryption," *Tatra Mountains Math. Publications*, vol. 67, no. 1, pp. 69_83, Sep. 2016.

[10] X. Jiang, M. Kim, K. Lauter, and Y. Song, ``Secure outsourced matrix computation and application to neural networks," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, Oct. 2018, pp. 1209_1222.

[11] S. Wang and H. Huang, ``Secure outsourced computation of multiple matrix multiplication based on fully homomorphic encryption," *KSII Trans. Internet Inf. Syst.*, vol. 13, no. 11, pp. 5616_5630, 2019, doi:

[12] Thilagamani, S., Shanti, N.," Gaussian and gabor filter approach for object segmentation", Journal of Computing and Information Science in Engineering, 2014, 14(2), 021006, https://doi.org/10.1115/1.4026458

[13] A. Brutzkus, R. Gilad-Bachrach, and O. Elisha, ``Low latency privacy preserving inference," in *Proc. ICML*, 2019, pp. 812_821.

[14] K. Nandakumar, N. Ratha, S. Pankanti, and S. Halevi, ``Towards deep neural network training on encrypted data," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops*, Jun. 2019, pp. 1_9.

[15] Rhagini, A., Thilagamani, S. ,"Women defence system for detecting interpersonal crimes", International Journal of Advanced Science and Technology, 2020, Volume 29,Issue7S, pp. 1669–1675

.[16] M. J. Atallah, K. N. Pantazopoulos, J. R. Rice, and E. E. Spafford, ``Secure outsourcing of scienti_c computations," *Adv. Comput.*, vol. 54, pp. 215_272, Jan. 2002.

[17] K.Deepa, S.Thilagamani, "Segmentation Techniques for Overlapped Latent Fingerprint Matching", International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Volume-8 Issue-12, October 2019. DOI: 10.35940/ijitee.L2863.1081219

[18] Santhi, P., Priyanka, T.,Smart India agricultural information reterival system, International Journal of Advanced Science and Technology, 2020, 29(7 Special Issue), pp. 1169–1175.

[19] X. Lei, X. Liao, T. Huang, and H. Li, ``Cloud computing service: The case of large matrix determinant computation," *IEEE Trans. Services Comput.*, vol. 8, no. 5, pp. 688_700, Sep. 2015.

[20] Santhi, P., Lavanya, S., Prediction of diabetes using neural networks, International Journal of Advanced Science and Technology, 2020, 29(7 Special Issue), pp. 1160–1168

[21] Vijayakumar, P, Pandiaraja, P, Balamurugan, B & Karuppiah, M 2019, 'A Novel Performance enhancing Task Scheduling Algorithm for Cloud based E-Health Environment', International Journal of E-Health and Medical Communications , Vol 10,Issue 2,pp 102-117.

[22] J. Liu, J. Bi, and M. Li, ``Secure outsourcing of large matrix determinant computation," *Frontiers Comput. Sci.*, vol. 14, no. 6, Dec. 2020, Art. no. 146807.

[23] S. Zhang, C. Tian, H. Zhang, J. Yu, and F. Li, ``Practical and secure outsourcing algorithms of matrix operations based on a novel matrix encryption method," *IEEE Access*, vol. 7, pp. 53823_53838, 2019, doi:

10.1109/ACCESS.2019.2913591.

[24] P. Pandiaraja, N Deepa 2019 ," A Novel Data Privacy-Preserving Protocol for Multi-data Users by using genetic algorithm" , Journal of Soft Computing , Springer , Volume 23 ,Issue 18, Pages 8539-8553

[25] X. Hu and C. Tang, ``Secure outsourced computation of the characteristic polynomial and eigenvalues of matrix," *J. Cloud Comput.*, vol. 4, no. 1, p. 7, Dec. 2015.

[26] N Deepa , P. Pandiaraja, 2020 ," Hybrid Context Aware Recommendation System for E-Health Care by merkle hash tree from cloud using evolutionary algorithm" , Journal of Soft Computing , Springer , Volume 24 ,Issue 10, Pages 7149–7161.

[27] L. Zhou and C. Li ``Outsourcing eigen-decomposition and singular value decomposition of large matrix to a public cloud," *IEEE Access*, vol. 4, pp. 869_879, 2017.

[28] N Deepa , P. Pandiaraja, 2020 , " E health care data privacy preserving efficient file retrieval from the cloud service provider using attribute based file encryption ", Journal of Ambient Intelligence and Humanized Computing , Springer , https://doi.org/10.1007/s12652-020-01911-5.

[29] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. London, U.K.: Chapman & Hall, 2014.

[30] K Sumathi, P Pandiaraja 2019," Dynamic alternate buffer switching and congestion control in wireless multimedia sensor networks" , Journal of Peer-to-Peer Networking and Applications , Springer , Volume 13,Issue 6,Pages 2001-2010.

[31] A. C.-C.Yao, ``Howto generate and exchange secrets," in *Proc. 27th Annu. Symp. Found. Comput. Sci. (FOCS)*, Oct. 1986, pp. 162_167.

[32] Shankar, A., Pandiaraja, P., Sumathi, K., Stephan, T., Sharma, P. ," Privacy preserving E-voting cloud system based on ID based encryption " Journal of Peer-to-Peer Networking and Applications , Springer , https://doi.org/10.1007/s12083-020-00977-4.

[33] P. Paillier, ``Public-key cryptosystems based on composite degree residuosity classes," in *Advances in Cryptology_EUROCRYPT* (Lecture Notes in Computer Science), vol. 1592, J. Stern, Ed. Berlin, Germany: Springer,1999.

[34] D. Kim, Y. Son, D. Kim, A. Kim, S. Hong, and J. H. Cheon, ``Privacy- preserving approximate GWAS computation based on homomorphic encryption," *BMC Med. Genomics*, vol. 13, p. 77, Jul. 2020.

[35] C. Dwork, ``Differential privacy," in *Encyclopedia of Cryptography and Security*. Boston, MA, USA: Springer, 2011, pp. 338_340.

[36] O. Goldreich, *Foundations of Cryptography: Basic Applications*, vol. 2. New York, NY, USA: Cambridge Univ. Press, 2004.

[37] Z. Brakerski, C. Gentry, and V. Vaikuntanathan, ``(Leveled) fully homo- morphic encryption without

bootstrapping," in *Proc. 3rd Innov. Theor. Comput. Sci. Conf. (ITCS),* New York, NY, USA, 2012, pp. 309_325.

[38] C. Gentry, S. Halevi, and P. N. Smart, ``Fully homomorphic encryption with polylog overhead," in *Proc. 31st Annu. Int. Conf. Theory Appl. Cryptograph. Techn. (EUROCRYPT)*. Berlin, Germany: Springer-Verlag, 2012, pp. 465_482.

[39] C. Gentry, S. Halevi, and N. P. Smart, ``Homomorphic evaluation of the AES circuit," in *Advances in Cryptology_CRYPTO*. Berlin, Germany: Springer, 2012, pp. 850_867.

[40] N. P. Smart and F. Vercauteren, ``Fully homomorphic SIMD operations," *Des., Codes Cryptogr.*, vol. 71, no. 1, pp. 57_81, Apr. 2014.

[41] S. Halevi and V. Shoup, ``Algorithms in HElib," in *Advances in Cryptology_CRYPTO* (Lecture Notes in Computer Science), vol. 8616, J. A. Garay and R. Gennaro, Eds. Berlin, Germany: Springer, 2014.

[42] D. Rathee, P. K. Mishra, and M. Yasuda, ``Faster PCA and linear regression through hypercubes in HElib," in *Proc. Workshop Privacy Electron. Soc. (WPES)*, New York, NY, USA, Jan. 2018, pp. 42_53.

[43] R. S. Bird, ``A simple division-free algorithm for computing determi-
nants," *Inf. Process. Lett.*, vol. 111, nos. 21_22, pp. 1072_1074, Nov. 2011.

[44] G. C. Fox, S.W. Otto, and A. J. G. Hey, ``Matrix algorithms on a hypercube I: Matrix multiplication," *Parallel Comput.*, vol. 4, no. 1, pp. 17_31, Feb. 1987.

[45] Justin Lai, Sydney Maples, “Ammunition Detection: Developing a RealTime Gun Detection Classifier”, Stanford University, Feb 2017

[46] Shreyamsh Kamate, “UAV: Application of Object Detection and Tracking Techniques for Unmanned Aerial Vehicles”, Texas A&M University, 2015.

[47] Adrian Rosebrock, “Object detection with deep learning and OpenCV”, pyimagesearch.

[48] Mohana and H. V. R. Aradhya, "Elegant and efficient algorithms for real time object detection, counting and classification for video surveillance applications from single fixed camera," 2016 International Conference on Circuits, Controls, Communications and Computing (I4C), Bangalore, 2016, pp. 1-7.

[49] Akshay Mangawati, Mohana, Mohammed Leesan, H. V. Ravish Aradhya, “Object Tracking Algorithms for video surveillance applications” International conference on communication and signal processing (ICCSP), India, 2018, pp. 0676-0680.

[50] Apoorva Raghunandan, Mohana, Pakala Raghav and H. V. Ravish Aradhya, “Object Detection Algorithms for video surveillance applications” International conference on communication and signal processing (ICCSP), India, 2018, pp. 0570-0575.