ASEAN Engineering Journal

Full Paper

MODELING OF OPTIMAL MULTI KEY HOMOMORPHIC ENCRYPTION WITH DEEP LEARNING BIOMETRIC BASED AUTHENTICATION SYSTEM FOR CLOUD COMPUTING

D.Prabhu*, S.Vijay Bhanu, S.Suthir

Department of Computer Science and Engineering, Annamalai University, Annamalai Nagar, Chidambaram, Tamil Nadu, India

Article history
Received
04 April 2023
Received in revised form
19 July 2023
Accepted
27 July 2023
Published online
30 November 2023

*Corresponding author
prabhu@lit.edu.in

Graphical abstract

Abstract

More recently, cloud computing (CC) has gained considerable attention among research communities and business people. Inspite of the advantages of CC, security, and privacy remains a challenging problem. Therefore, biometric authentication systems have been employed and fingerprint is considered as widely employed to attain security. In addition, image encryption techniques can be used to encrypt the fingerprint biometric image to add an extra level of security. Based on these motivation, this study designs an optimal multikey homomorphic encryption (OMHE) with stacked autoencoder (SAE) based biometric authentication system for CC environment. The proposed OMHE-SAE model aims to encrypt the biometrics using OMHE technique and then verification takes place using SAE model. In addition, the OMHE technique involves the optimal key generation process using sandpiper optimization (SPO) algorithm to effectively choose the keys for encryption and decryption. Furthermore, the verification of decrypted biometrics takes place by the use of SAE model. A wide range of simulation analyses take place on benchmark datasets and the experimental outcomes portrayed the betterment of the OMHE-SAE More than cutting edge technology.

Keywords: biometrics, Authentication, cloud computing, Image encryption, Security, Optimal key generation

1.0 INTRODUCTION

Cloud computing (CC) is a technology that provides flexibilities like software as a service Platform as a Service [1], Infrastructure as a Service, Cloud Web Computing, Utilities, Managed Services, etc. This generated information could be saved on memory unit given by cloud system provider. A key benefit of the cloud is that any organization of employees/users/company can access it whenever they need to access this data authentication as before [2]. But, it also contains certain shortcomings like vulnerable to attack, restricted control, cost, vendor lock-in, limited flexibility, and more significantly privacy and security [3]. Authentication like conventional approaches could be implemented by PINs and passwords, however, their disadvantage is that users have to keep in mind. To alleviate in remembering multiple passwords, it can be often employ a similar password anywhere which isn't troublesome works for an attacker. These days, multifactor authentication is also taken advantage of by mobile phones and cloud services, however, cost imbalance is made together with IT onerous [4]. Using mobile devices as tablets and smartphones now being almost ubiquitous, increased interest has been provided to safety precautions performed in this device [5]. More and more people are seeing it as central to their digital lifestyles, with tablets, smartphones and the increasing amount of data being uploaded to the cloud (which is always very private). With a lot of personal data at risk, a higher level of

security is required [6]. Conventionally, measures like tokens, passwords, or PINs have been used, but lately, biometric discovery often replaces or complements it, providing greater accessibility and user-friendliness.

Biometrics is a branch of computer science which handles automated identity detection and is largely employed in access control [7]. Biometric system depends on behavioral properties (for example, voice, handwritten signature, EEG, gait) or anatomical properties (handprint, fingerprint, face geometry, iris, ear geometry, hand geometry, and so on.). The modality utilized in biometric solution must be described as having higher discriminative data volume and be hard to recreate with spoof artifacts [8]. Longer term resistance and stability to disease variations are also crucial, along with wide user acceptance. The universality of a biometrics technique is limited on the repeatability of observation, low sensor cost, and ease of technical implementation [9].

Joseph et al. [10] proposed a multi-factor authentication method by fusing iris, palm print, and fingerprint features. All features have been subjected to successive processes of image processing techniques such as feature extraction, preprocessing, and normalization. In the extracted function, a dedicated secret key was created by combining the characteristics in two steps. False Rejection Rate (FRR) and False Acceptance Rate (FAR) matrices are employed for measuring the strength of the scheme. Kumar et al. [11] proposed an individual authentication system appropriate to cloud platforms with EEG signals. EEG signal is recorded from mobile devices whereas the participant listens to music. The recorded signal is later transmitted to a cloud server with REST web services, while valuable feature is extracted. Individual verification and identification procedures are performed by 2 familiar classifications such as SVM and HMM models.

In Venkatachalam et al. [12], cryptographic techniques are employed by the service provider to produce the biometric key for verification that would be available only for the authorized user. XOR operation with Gabor filters using distributed security and cryptography. is utilized for generating the presented biometric key (bio-key) and evade information de-duplication in the cloud, ensure evasion of information security and redundancy. Ilankumaran and Deisy [13] developed a new C2 code derived by magnitude and orientation data extracted from iris images and finger veins for improving the validating scheme. The C2 code eliminates FS operators decreasing the complicated process since it integrates the magnitude and orientation data from iris image and finger vein inputs. This method could be performed in a cloud computing platform based biometric authorization scheme because of its reduced data management complication.

Bartuzi and Trokielewicz [14] presented a proof-of-concept biometrics authorization system with hand images gathered in distinct light spectrum. Analyses of comparison among Vascular patterns extracted from thermal and near-infrared images and evaluation of the correlations among single biometric feature included in all image types are also implemented. Ali et al. [15], developed a multi-modal authentication method with encrypted biometrics for the edge centric cloud platform. The private portable device is used to encrypt biometrics in the presented model that enhances the utilization of resource and tackle other limitations of the cloud platform. Biometric is encrypted by a novel methodology. In the presented model, the edge transmits the encrypted face and speech to the cloud processing.

This study introduces an optimal multikey homomorphic encryption (OMHE) with stacked autoencoder (SAE) based biometric authentication system for CC environment. The proposed OMHE-SAE model involves the OMHE based encryption technique with sandpiper optimization (SPO) algorithm based key generation process to effectually choose a key for encryption and decryption. Finally, we perform verification of the decrypted biometric data using the SAE model. To report the superiority of the OMHE-SAE model, we perform a comprehensive analysis of the simulations and validate the results against various metrics.

2.0 THE PROPOSED BIOMETRIC AUTHENTICATION MODEL

This study uses a novel OMHE-SAE model for biometric authentication in a CC environment. The proposed OMHE-SAE model includes various sub-processes such as miniaturization, MHE-based encryption, SPO-based key generation, and SAE-based recognition. A typical workflow for the OMHE-SAE model is shown in Figure 1 a detailed description of the operation of these modules is provided in the following section.

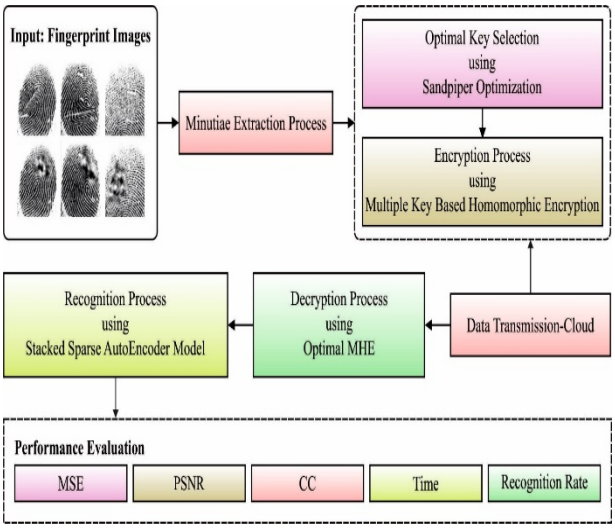


Figure 1 Overall block diagram of OMHE-SAE model

2.1. Miniature Extraction Process

Q-learning is used to extract fine details from fingerprint images. It is an active hardening technology that creates and enforces an agent's policy on the fly. They place agents on fingerprint images. This agent selects a state from the reward structure by following the ridge along the gray scale values. To obtain the compensation structure, we take the fingerprint image and use image downscaling to make it a single pixel value. Scan the image using grayscale and a 3x3 filter. One intermediate neighbor is considered an end point, and the two central neighbors are considered branching points. After scanning the entire image, the entire end point and branch point are reached. Then we estimate the Euclidean distance from that point and use that distance as the compensation structure R. The state is also

selected. They take a row option from the reward structure and choose an initial state**.** Here they find a non-negative integer value in R and take a variant of this non-negative value. This non-negative value is stored as an action [16]. So we choose the action with the highest non-negative value and evaluate Q [action, state]. The selected task will be in a new state and repeat the process until the process is complete.

2.2 Optimal MHE based Encryption Process

During the image encryption, the OMHE technique gets encrypted by the use of optimal keys produced by SPO algorithm. Semantically secure homomorphic public-key cryptography approaches are key cryptographic devices for many secure multiparty evaluation problems. Homomorphic properties are very useful for creating protected methods with higher security data recovery strategies. This cryptographic structure is used to perform operations using encrypted information without knowledge of the secret key (without decryption). That is, the user is the primary owner of the secret key. The homomorphic computational approach considered an image of a polynomial cipher, i.e. an image encrypted with N keys, provides an encrypted image along with its computed key. Multi-encryption is the sure way towards changing over exclusive messages to a confused shape by implementing encryptions several times, whether by performing the distinctive or same processes. It is presented as cascade encryption, multiple encryption, and cascade encryption. From the procedure of examination, decryption and encryption have been implemented using multiple keys [17]. The presented MHE considered three steps: encryption/decryption method, multi-key generation, and optimal key determination.

A key is used for encrypting/decrypting whatever data is being decrypted or encrypted. A method is under the usage of decoding and encoding keys and the correlated Image with symmetric key; Security and Privacy. A relative public key (pu_k) and the private key (pr_k) from multiple keys are utilized. Key matching is used with asymmetric keys. Now some keys, $K = \{K_1, K_2, \dots K_n\}$ are made for MHE. In some cases, keys are randomly generated by a random number generator and optimization algorithms are taken into account to select the optimal key from multiple keys. The inspiration for manual optimization is to enhance the privacy of key selection in image decryption and encryption procedures. Eventually, the optimal encryption frame is selected as the final encryption frame. The SPO model was used to refine public and private keys across multiple key sets. Transformation methods were then used to improve the encryption process, which was to be expected. Finally, the optimal encrypted content is selected as the final encrypted content.

The SPO algorithm depends on the wader's moving and attacking behavior. The mathematical processes of migration as well as attack performances are explained below.

2.2.1 Migration behavior (Exploration)

This technique examines the set of sandpipers that transfer from one place to another under the migration. Currently, the sandpiper fulfills the subsequent 3 three criteria's:

Collision avoidance: A more variable C_A has been utilized in the calculation of a novel search agent place for avoiding collision avoidance amongst its neighboring sandpiper.

$$\overrightarrow{C_{sp}} = C_A \times \overrightarrow{P_{sp}}(z) \quad (1)$$

where $\overrightarrow{C_{sp}}$ refers the place of search agent that doesn't collide with another search agent, $\overrightarrow{P_{s\rho}}$ stands for the present place of search agents, z stands for the present iteration, and C_A demonstrates the movement of search agent during the search space.

$$C_A = C_f - \left(z \times \left(C_f / \mathrm{Max}_{iterations}\right)\right)$$

Where,

$$z = 0, 1, 2, \dots, \mathrm{Max}_{iterations} \quad (2)$$

Where C_f implies the control frequency for adjusting the variables C_A that has linearly reduced in $C_f\ to\ 0$. For sample, when the parameter C_f is fixed to 2, the variable C_A has been continuously reduced in [2-0]. The value of C_f is fixed to 2.

Converge in the direction of best neighbor's: Then collision avoidance, the search agent converges (for instance, move) near the way of optimum neighbor [18].

$$\overrightarrow{M_{sp}} = C_B \times \left(\overrightarrow{P_{bst}}(z) - \overrightarrow{P_{sp}}(z)\right) \quad (3)$$

Where $\overrightarrow{M_{sp}}$ states the places of search agent $\overrightarrow{P_{sp}}$ nearby the optimum fittest search agents $\overrightarrow{P_{bst}}$ (for instance, whose fitness value has been minimum). C_B Represents the arbitrary variables that are responsible for an optimum exploration. C_B Has been calculated as:

$$C_B = 0.5 \times R_{and} \quad (4)$$

Here, it means a random number between 0 and1.

Best search agent update: Eventually, Search agents/warders are updated to the optimal level of search agents.

$$\overrightarrow{D_{sp}} = \overrightarrow{C_{sp}} + \overrightarrow{M_{sp}} \quad (5)$$

where $\overrightarrow{D_{sp}}$ demonstrates the gap amongst the search agent as well as Optimal Search Agent.

2.2.2 Attack Action (Wear)

In the migration, sandpiper is modify its speed as well as angle of attack continuously. It can be utilized its wings for increasing its altitudes. The sandpipers create the spiral performance but attack the prey during the air. This performance in 3-D plane has been explained as follows.

$$x' = R_{adius} \times sin(i) \quad (6)$$
$$y' = R_{adius} \times cos(i) \quad (7)$$
$$z' = R_{adius} \times i \quad (8)$$
$$r = u \times e^{kv} \quad (9)$$

where R_{adius} indicates The radius of all turns of a helix is a variable in the range, a constant that determines the shape of the helix, and is the base of the natural logarithm. It is noticeable that we leave the value of the constant as 1. If more than one value of this constant is equal, the shape of the spiral becomes more

complex. So, the upgraded place of search agent has been calculated utilizing in Eqs. (6)–(9).

$$\overrightarrow{P_{sp}}(z) = \left(\overrightarrow{D_{sp}} \times (x' + y' + z')\right) \times \overrightarrow{P_{bst}}(z) \quad (10)$$

where $\overrightarrow{P_{sp}}(z)_{\text{updates}}$ Deploy different search agents and save the best optimal solution..

The SPO-based multi-key optimization method processes the fitness function with PSNR, which restores video quality. This method is suitable for amplifying many nonlinear and linear problems. I couldn't tell the size of the distorted image matrix from the size of the correct image matrix**.** The presented key optimization algorithm, consider as PSNR, can be determined in the following:

$$F_i = \text{Max}(PSNR). \quad (11)$$

2.2.3 Encryption

Homomorphic encryption provides encryption that treats encrypted and plain images as equivalent logarithmic functions. Homomorphic encryption allows servers to act on encrypted information without knowing the original plain image. The client encrypts the original image using the private key and sends the encrypted image to the server along with the public key**.** $pu_k = (k, i)$ and $K = (p, q)Enc(I, pr_k)$ for picking arbitrary parameters.$\because r \in Z_k^*$, Calculate cipher data $c = I.r^k \; mod k^2$. An encryption system is effective in the secret images of original images. In the encryption procedure, it is recommended to possess the lock inside to encode all the image pixels.

2.2.4 Decryption

The decryption process consists of two masks, specifically a secret and a mask in a fixed order. Decrypt message bits (by pixels) from encrypted images and other secret variables.

2.3 SAE based Authentication Process

At the final stage, the decrypted fingerprint is authenticated using SAE model to determine whether the user is authenticated or not. AE is a type of NN which employs decoding and encoding procedure for unsupervised learning, i.e., largely utilized for dimension reduction and feature extraction. AE is a framework which has symmetry. The AE model consists of output layer, input layer, and latent layer. As illustrated in Figure 2, the output and input layers are equivalent in size, and the size of latent layer should be slighter when compared to the input layers. The constructed vector represent $\tilde{x} \in [0,1]^D$, the input vector denotes x, and the latent vector indicates $e \in [0,1]^d$. the encoding procedure from input to latent layers can be expressed as

$$e = f_\theta(x) = s(Wx + b) \quad (12)$$

and the decoding procedure from latent layer to output layer can be expressed as

$$\tilde{x} = g_{\theta'}(e) = s(W'e + b') \quad (13)$$

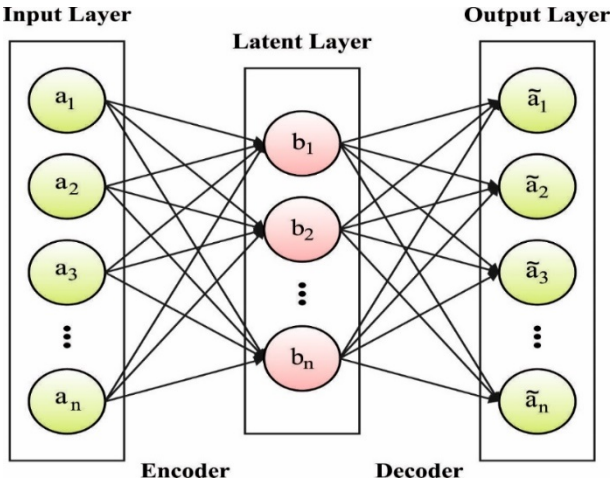


Figure 2. Structure of SAE

Whereas W & W' represents the input to latent layer and the latent to output weight, correspondingly b' and b represent the bias vector of latent layer and input layer [19], correspondingly as well as f_θ & g_θ, denotes the activation function of neurons in the latent layer and neurons in the output layer. Variables W, W', b and b' in the AE is learned through minimalizing the reconstruction error.

$$J(W, b, x, \tilde{x}) = \frac{1}{2}\|h_{W,b}(x) - \tilde{x}\|^2. \quad (14)$$

The abovementioned equation is a measure of errors among the input x and recreated $\tilde{x}$ for individual samples. In a training set having D sample, the cost function of AE is determined by

$$\sum_{l=1}^{n_l-1}\sum_{i=1}^{s_l}\sum_{j=1}^{s_l+1}(W_{ji}^{(l)})^2 = \left[\frac{1}{D}\sum_{i=1}^{D}\left(\frac{1}{2}\left\|h_{W,b}\left(x^{(i)}\right) - \tilde{x}^{(i)}\right\|^2\right)\right] + \frac{\lambda}{2}\sum_{l=1}^{n_l-1}\sum_{i=1}^{s_l}\sum_{j=1}^{s_l+1}(W_{ji}^{(l)})^2 \quad (15)$$

In which D represent the overall amounts of sample, s represent the numbers of node in layer l, λ denotes weight attenuation parameters, and the reconstruction error of all the training samples are the square error. The next item is presented for reducing the size of the weights that assist to avoid overfitting. Also, SAE is a framework, which has symmetry SAE is created using AE, stacked layer wise. When the single layer AE is trained the next AE is trained by the latent layers from the initial AE. Through reiterating this procedure, they could generate an SAE of some depth.

AE is stacked for achieving greedy hierarchical learning, in which l^{th} latent layer is utilized as input for the $l + 1th$ latent layers in the stack. The result created using the SAE is utilized for pertaining the weight of FC-DNN method rather than arbitrarily initiating the weight. This technique is very useful for the method for initializing the parameter closer to better local minimal value and enhance the optimization effects. This illustrates that the convergence of the model is smoother and the total performance is greater in classification tasks

3.0 RESULTS AND DISCUSSION

This section examines the performance of the OMHE-SAE biometric authentication model. The performance of the OMHE-SAE model is verified using decrypted fingerprint images, as shown in Figure 3. The results are also checked in terms of MSE, PSNR, CC, CT, and recognition rate.

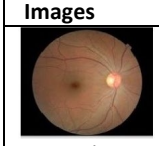
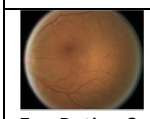
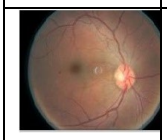
Cover Images	Secret Images	Encrypted Images	Decrypted Images
 Eye Retina 1	 Finger 1	 Encrypted 1	 Image 1
 Eye Retina 2	 Finger 2	 Encrypted 2	 Image 2
 Eye Retina 3	 Finger 3	 Encrypted 3	 Image 3
 Eye Retina 4	 Finger 4	 Encrypted 4	 Image 4
 Eye Retina 5	 Finger 5	 Encrypted 5	 Image 5

Figure 3 Sample Fingerprint Images

In Table 1 and Figure 4 shows the analysis results of the OMHE-SAE system using the comparative method for five different images. The simulation outcomes reported that the OMHE-SAE model has gained a lower MSE compared to other techniques. For example, in test image 1, the OMHE-SAE method showed a minimum MSE of 0.05, while the DLCM-WOA, DLCM-GWO, and DLCM-PSO methods achieved maximum MSEs of 0.176, 0.298, and 1.679.

Also in test image 5, the OMHE-SAE methodology showed a decrease in MSE to 0.094, whereas DLCM-WOA, DLCM-GWO and DLCM-PSO techniques have resulted in an increased MSE of 0.1980, 0.2660, and 2.5690.

Table 1 Result Analysis of Proposed OMHE-SAE Method with respect to MSE and PSNR

Test Images	OMHE-SAE		DLCM-WOA		DLCM-GWO		DLCM-PSO	
	MSE	PSNR	MSE	PSNR	MSE	PSNR	MSE	PSNR
Image 1	0.05	61.14	0.176	55.68	0.298	53.39	1.679	45.88
Image 2	0.094	58.40	0.187	55.41	0.309	53.23	2.321	44.47
Image 3	0.078	59.21	0.256	54.05	0.267	53.87	2.690	43.83
Image 4	0.065	60.00	0.221	54.69	0.209	54.93	2.124	44.86
Image 5	0.094	58.40	0.198	55.16	0.266	53.88	2.569	44.03

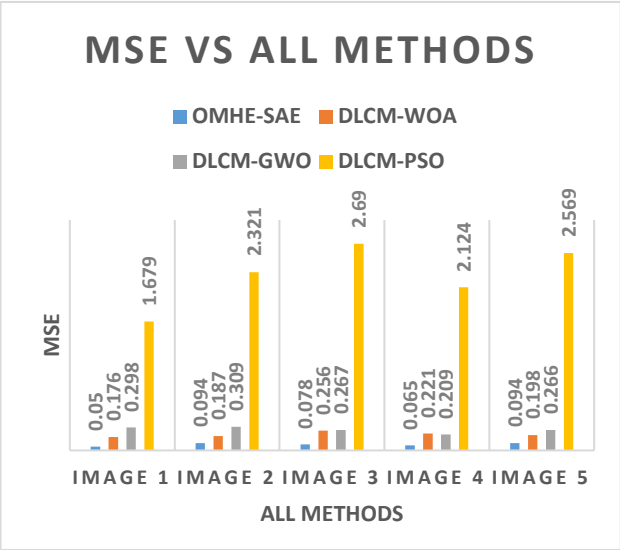


Figure 4. MSE analysis with All Methods

Next, The PSNR analysis of the OMHE-SAE model is shown in Figure 5. The results showed that the OMHE-SAE model outperformed with higher PSNR values in all test images used. For example, in image 1, the OMHE-SAE model suggested an increased PSNE of 61.140 dB, while the DLCM-WOA, DLCM-GWO and GLCM-PSO methods showed a reduced PSNR of 055.
68.0 dB, 53.390 dB, and 45.880 dB, respectively. Also in Image 5, the OMHE-SAE method gives a maximum PSNR of 58.400 dB, while the DLCM-WOA, DLCM-GWO and GLCM-PSO methods give a minimum PSNR value of 55.160 dB, 53.880 dB, and 44.030 dB, respectively.

Figure 5 PSNR analysis with All Methods

Afterward, the CC analysis of the OMHE-SAE method takes place on different test images in Table 2 and Figure 6. The outcomes showcased that the OMHE-SAE manner outperformed its supremacy with the superior CC values on every test image utilized. For instance, with image 1, an enhanced PSNE of 0.999 has been obtainable by the OMHE-SAE algorithm The DLCM-WOA, DLCM-GWO, and GLCM-PSO methodologies yielded minimum CCs of 0.994, 0.992, and 0.986, respectively. Also in image 5, the OMHE-SAE system received a high CC 0.998, DLCM-WOA, DLCM-GWO and GLCM-PSO algorithms produced lower CCs of 0.991, 0.990 and 0.982, respectively.

Table 2 Analysis of the results of the proposed OMHE-SAE method with respect to the correlation coefficient (CC)

Test Images	OMHE-SAE	DLCM-WOA	DLCM-GWO	DLCM-PSO
Image 1	0.999	0.994	0.992	0.986
Image 2	0.999	0.993	0.992	0.989
Image 3	0.999	0.992	0.989	0.984
Image 4	0.998	0.994	0.987	0.983
Image 5	0.998	0.991	0.990	0.982

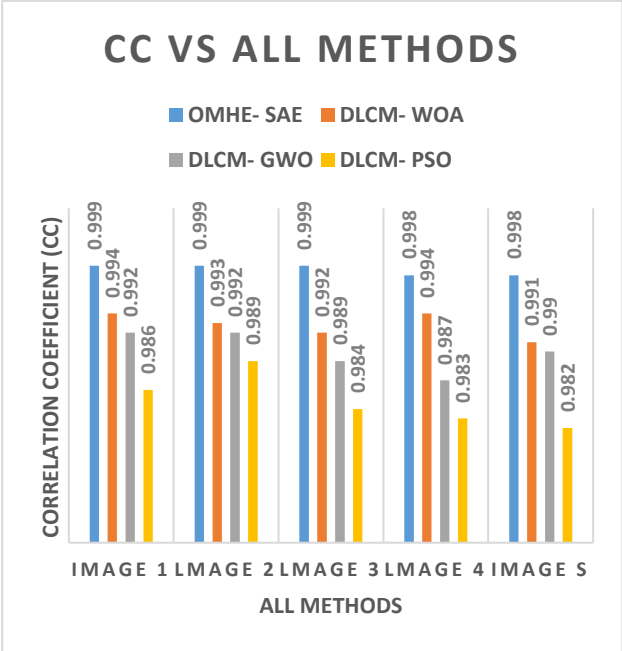


Figure 6 CC analysis with All Methods

In Table 3 and Figure 7 shows an analysis of the results of the OMHE-SAE method in relation to the method. in 5 varying images. The simulation outcomes stated that the OMHE-SAE approach has reached a minimum CT compared to other techniques. For example, in test image 1, the OMHE-SAE approach reduced CT by 01.087, whereas the DLCM-WOA, DLCM-GWO, and DLCM-PSO methodologies increased CT by 01.717, 02.202, and 02.924.

Additionally, in test image 5, the OMHE-SAE method obtained a minimum CT value of 01.154, and the DLCM-WOA, DLCM-GWO, and DLCM-PSO methods obtained extended CT values of 01.819, 02.012, and 02.254.

Table 3 Result Analysis of Proposed OMHE-SAE Method with respect to Computation Time(s)

Test Images	OMHE-SAE	DLCM-WOA	DLCM-GWO	DLCM-PSO
Image 1	1.087	1.717	2.202	2.924
Image 2	1.127	1.547	1.879	2.355
Image 3	1.289	1.871	2.022	2.445
Image 4	1.012	1.745	2.297	2.256
Image 5	1.154	1.819	2.012	2.254

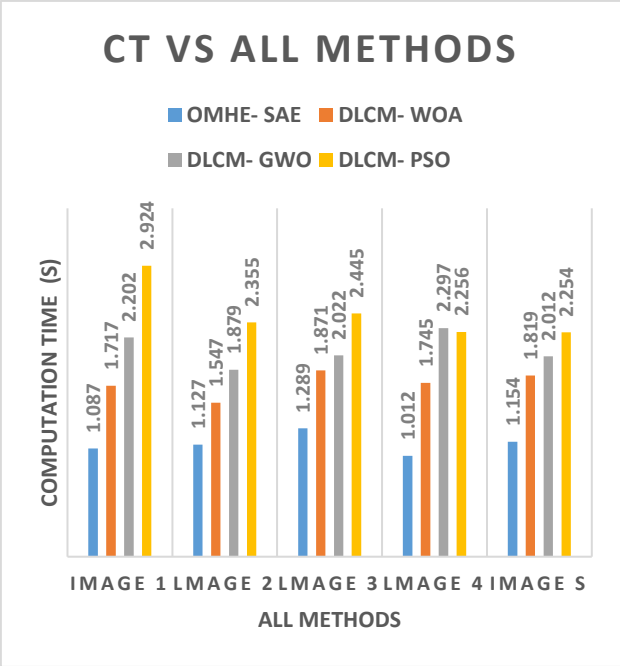


Figure 7 CT analysis with All Methods

Finally, the biometric recognition rate of OMHE-SAE using the existing method is shown in Table 4 and Figure 8. As a result, SVM and ELM models showed low recognition rates of 92.07% and 93.21%.

Together, the KELM approach achieved a median recognition rate of 95.98%. However, the OMHE-SAE model has resulted in an increased recognition rate of 98.43%. By looking into Looking at the table and figure above, it can be seen that the OMHE-SAE approach has been established as an effective tool for biometric authentication in a CC environment.

Table 4 Result Analysis of Proposed OMHE-SAE Technique with respect to Recognition Rate (%)

Methods	OMHE-SAE	KELM	ELM	SVM
Recognition Rate	98.43	95.98	93.21	92.07

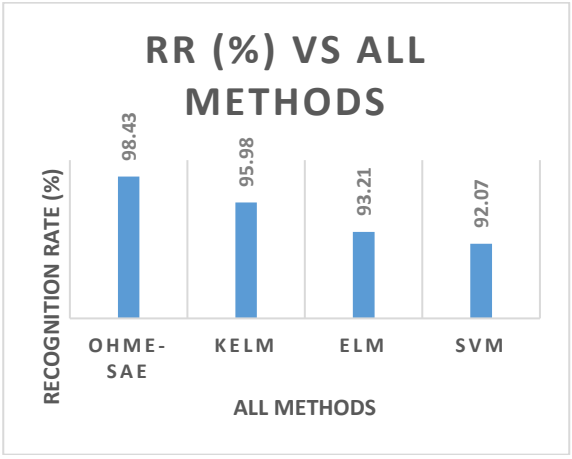


Figure 8 RR analysis with All Methods

4.0 CONCLUSION

This study uses a novel OMHE-SAE model for biometric authentication in a CC environment. The proposed OMHE-SAE model includes various sub-processes such as miniaturization, MHE-based encryption, SPO-based key generation, and SAE-based recognition. Enabling an optimal key generation process using the SPO algorithm maximizes overall performance and PSNR values. In addition, the decrypted biometric information determines whether the user is authenticated using the SAE model. To report the excellence of the OMHE-SAE model, a A comprehensive analysis of the simulation is performed. Experimental results show that the OMHE-SAE method outperforms other methods. Therefore, the OMHE-SAE model can be utilized as an efficient biometric authentication tool in the CC environment. In the future, a lightweight encryption method for biometric authentication in a CC environment may be developed.

Acknowledgement

It is my prime duty to express my gratefulness to the Almighty for His blessings. Without His divine grace and blessings, nothing would have been possible. With a deep sense of gratitude, I acknowledge my indebtedness to my revered guide Dr. S. Vijay Bhanu, Associate Professor, Department of Computer Science and Engineering, Annamalai University, Chidambaram and Dr. S. Suthir, Assistant Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai for their encouragement, appreciation, and guidance throughout this research article. I would like to thank my beloved Parents and Friends for their perpetual love and support and I am grateful to everyone who helped me to complete my research article.

References

[1] Kakkad, V., Patel, M. and Shah, M., 2019. Biometric authentication and image encryption for image security in cloud framework. *Multiscale and Multidisciplinary Modeling, Experiments and Design*, *2*(4): 233-248. DOI: https://www.mecs-press.org/ijigsp/ijigsp-v14-n4/v14n4-2.html

[2] Bothe S, Jadhao RM, Shinde S 2012 Cloud computing based image processing applications for agro informatics using 'self-learning system' approach. In*: Proceedings of AIPA*, 1–4. DOI: https://www.semanticscholar.org/paper/CLOUD-COMPUTING-BASED-IMAGE-PROCESSING-APPLICATIONS-Bothe-Jadhao/06cb232aa5ddc962b5e67c526f665384540bbc81

[3] Thieling L, Schuer A, Hartung G, Buchel G 2014. Embedded image processing system for cloud-based applications. In: *International Conference on sytems, signals and image processing*, 1–4. DOI:https://www.researchgate.net/publication/289352599_Design_of_image_sampling_and_processing_system_on_3D_measuring_machine

[4] Rathi R, Choudhary M, Chandra B 2012. An application of face recognition system using image processing and neural networks. nternational *Journal Computer Technology.* 3(1): 45–49. DOI: https://aip.scitation.org/doi/abs/10.1063/1.5005335

[5] Bala Y, Malik A 2018. Biometric inspired homomorphic encryption algorithm for secured cloud computing. In: Panigrahi B, Hoda M, Sharma V, Goel S (eds) Nature inspired computing. *Advances In Intelligent Systems And Computing,* 652: 13–21 Springer, Singapore. DOI: https://app.dimensions.ai/details/publication/pub.1092087643

[6] Wang S, Nassar M, Atallah M, Malluhi Q 2013. Secure and private outsourcing of shape-based feature extraction. In: *International Conference On Information And Communications Security*, 90–99 DOI: https://digitalcommons.newhaven.edu/electricalcomputereengineering-facpubs/108/

[7] Tuyls, P. and Goseling, J., 2004, May. Capacity and examples of template-protecting biometric authentication systems. In *International Workshop on Biometric Authentication* 158-170. Springer, Berlin, Heidelberg. DOI: https://eprint.iacr.org/2004/106.pdf

[8] Simoens, K., Bringer, J., Chabanne, H. and Seys, S., 2012. A framework for analyzing template security and privacy in biometric authentication systems. *IEEE Transactions on Information forensics and security*, *7*(2): 833-841. DOI: https://link.springer.com/chapter/10.1007/978-3-319-12280-9_19

[9] Biggio, B., Akhtar, Z., Fumera, G., Marcialis, G.L. and Roli, F., 2012. Security evaluation of biometric authentication systems under real spoofing attacks. *IET biometrics*, *1*(1): 11-24. DOI: http://pralab.diee.unica.it/en/node/667

[10] Joseph, T., Kalaiselvan, S.A., Aswathy, S.U., Radhakrishnan, R. and Shamna, A.R., 2021. A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment. *Journal of Ambient Intelligence and Humanized Computing,* 12(6): 6141-6149. DOI: https://ouci.dntb.gov.ua/en/works/7BmAXJg9/

[11] Kumar, P., Singhal, A., Saini, R., Roy, P.P. and Dogra, D.P., 2018. A pervasive electroencephalography-based person authentication system for cloud environment. *Displays,* 55: 64-70. DOI: https://www.sciencedirect.com/science/article/abs/pii/S0141938222000506#!

[12] Venkatachalam, K., Prabu, P., Almutairi, A. and Abouhawwash, M., 2021. Secure biometric authentication with de-duplication on distributed cloud storage. *PeerJ Computer Science*. 7: 569. DOI: https://peerj.com/articles/cs-569/

[13] Ilankumaran, S. and Deisy, C., 2019. Multi-biometric authentication system using finger vein and iris in cloud computing. *Cluster Computing,* 22(1): 103-117. DOI: https://dl.acm.org/doi/abs/10.1007/s10586-018-1824-9

[14] Bartuzi, E. and Trokielewicz, M., 2021. Multispectral hand features for secure biometric authentication systems. *Concurrency and Computation: Practice and Experience*, 33(18): 6471. DOI: https://www.researcher-app.com/paper/8283752

[15] Ali, Z., Hossain, M.S., Muhammad, G., Ullah, I., Abachi, H. and Alamri, A., 2018. Edge-centric multimodal authentication system using encrypted biometric templates. *Future Generation Computer Systems*, 85:76-87. DOI: https://pure.ulster.ac.uk/ws/portalfiles/portal/71152905/Multimodal_biometrics.pdf

[16] Pan, H., Lei, Y. and Jian, C., 2018. Research on digital image encryption algorithm based on double logistic chaotic map. *EURASIP Journal on Image and Video Processing*, *2018*(1):1-10. DOI: https://www.academia.edu/44376740/A_new_block_cipher_for_image_encryption_based_on_multi_chaotic_systems

[17] Shankar, K., Lakshmanaprabu, S.K., Gupta, D., Khanna, A. and de Albuquerque, V.H.C., 2020. Adaptive optimal multi key based encryption for digital image security. *Concurrency and Computation: Practice and Experience*, *32*(4): 5122. DOI: https://onlinelibrary.wiley.com/doi/10.1002/cpe.5122

[18] Kaur, A., Jain, S. and Goel, S., 2020. Sandpiper optimization algorithm: a novel approach for solving real-life engineering problems. *Applied Intelligence*, *50*(2): 582-619. DOI: https://dl.acm.org/doi/abs/10.1007/s10489-019-01507-3

[19] Tang, C., Luktarhan, N. and Zhao, Y., 2020. Saae-Dnn: Deep Learning Method on Intrusion Detection. *Symmetry*, *12*(10): 1695. DOI: https://www.mdpi.com/2073-8994/12/10/1695

[20] Prabhu.D, Vijay Bhanu.S, Suthir.S, 2022. Privacy preserving steganography based biometric authentication system for cloud computing environment, *Measurements Sensors. 24:* 100511. Elsevier. DOI: https://www.sciencedirect.com/science/article/pii/S2665917422001453?via%3Dihub

[21] Sunil Kumar Muttoo., Nisha, Archana Singhal. 2023. A novel privacy preserving technique using steganography and L – diversity for relations educational dataset. *International Journal of Information Technology 15: 3307–3325* Springer. DOI: https://link.springer.com/article/10.1007/s41870-023-01305-8

[22] Mohamed, and Ashiba. Hazzan A Youness, Huda Ashiba. 2023. Proposed homomorphic DWT for cancellable palm print recognition technique. *Multimedia Tools and Applications*. Springer. DOI:https://link.springer.com/article/10.1007/s11042-023-15710-5