Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 26 (2023), No. 3, pp. 729–738
DOI : 10.47974/JDMSC-1745

Blockchain technology combined with the CNN and Hashing algorithms enabled the secure storage of 3D biometric face and ear data

Veerpal Kaur [§]
Devershi Pallavi Bhatt [†]
Manipal University Jaipur
Jaipur
Rajasthan
India

Pradeep Kumar Tiwari*
Birla Global University
Bhubaneswar
Odisha 751029
India

Sumegh Tharewal [‡]
Symbiosis International (Deemed) University
Symbiosis Institute of Computer Studies and Research (SICSR)
Pune
Maharashtra
India

Abstract

The integration of biometrics and blockchain is proposed as a sophisticated and enduring security strategy to protect sensitive information in the digital era. 3D biometric data will not be affected by changes in posture and changes of illumination. This research proposed a security model for 3D multimodal (face and ear). To secure the 3D data uses the convolutional neural networks (CNNs) for 3D image feature extraction based on fusion of 3D face and ear data. Further compare the different hashing algorithms for the security of

[§] *E-mail:* parwinder366@gmail.com
[†] *E-mail:* bhattdevershi@gmail.com
* *E-mail:* pradeeptiwari.mca@gmail.com (Corresponding Author)
[‡] *E-mail:* sumeghtharewal@gmail.com

3D multimodal Biometric model in Blockchain. This research also compares the different hashing algorithm efficiency and impact of blockchain mechanism on 3D face and ear data.

Subject Classification: *68M25 Computersecurity.*

Keywords: *Blockchain, Biometric, Security, CNN, Hashing, Cryptography.*

1. Introduction

In modern society, secure authentication of user becomes an important issue. Traditional user authentication methods involve tokens, PINs, or basicpasswords, all of which have numerous security flaws, including the ease with which passwords can be deduced. A biometric authentication system has been suggested as a solution to these issues [1]. Firstly, combining data from several biometric sources has the effect of making the feature area more dimensional and reducing the similarity between different people's feature distributions [2]. Second multimodal biometric system is more exclusive than a single biometric trait. The creation of such multimodal biometric systems with the ability to automatically choose the appropriate fusion rule parameters, fusion rules and decision threshold to obtain the greatest performance [3]. Compared to 2D Biometrics, 3D Biometrics is far more resistant to lighting and position changes. Systems using 3D biometrics data are the most resistant to attack because 3D data is more difficult to replicate. 3D scanners are extremely quick and precise [4]. Since biometric data is typically maintained in a centralized database, problems including data tampering, identity theft, spoofing, channel interception, and database theft become more prevalent [5]. To solve these problems, new blockchain technologies are introduced to guarantee sensitive data protection. A distributed database is called blockchain which is consists of a group of data produced through cryptography [6]. Blockchain is a cutting-edge technology that has the potential to enable distributed ledgers of transactions, making it suitable for protecting biomedical records [7].

2. Proposed Model

Blockchain is an emerging technology that enables distributed ledgers of transactions, making it suitable for protecting data from biometric repositories. [8]. Integration of biometric and blockchain have many advantages as accountability, availability universal access, immutable etc. with these advantage, blockchain technology is useful for providing security the biometric template and also used for privacy of

data at some cost [9]. Security problems are growing along with the rise of smart, personalized digital devices, necessitating a detailed study of new and emerging concepts. This result an important and expansive area of research is biometric security using blockchain [10]. Face and ear are used to produce a better combination of Keys with respect to its size and sensitivity. The human face and ear are those body parts that have a high concentration of distinctive traits that allow for the distinct identification of numerous users and can be used as part of effective biometric systems for a wide range of applications. The system's capacity to recognize 2D biometrics may be influenced by factors like lighting, occlusion, posture, and illumination [11]. 3D biometric data will not be affected by changes in posture and changes of illumination [12]. To secure the multimodal biometric data using blockchain, the proposed model has different steps which are listed in Figure 1. the given proposed modal for security of multimodal biometric data is consist of two phases:

1. First is biometric system which includes biometric image acquisition, pre- processing, Feature extraction, Matching features, Recognition and Fusion.
2. Second phase is Blockchain based security System use biometric data generated by first phase applying hashing algorithm, encryption, create block of data and store it into blockchain.

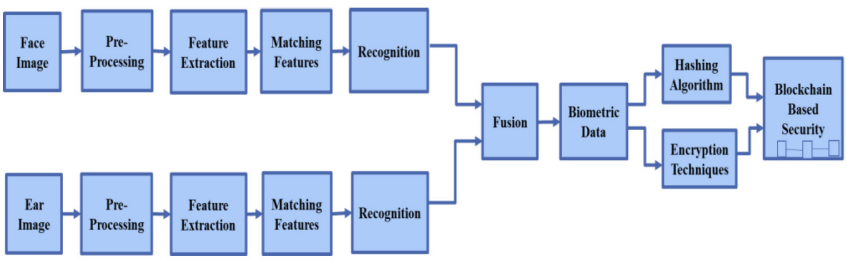

Figure 1

Blockchain Technology using to secure biometric information

2.1 *Feature Extraction using CNN*

In preprocessing step, noise and hole filling from the data collection procedure are removed, and the ear and face is cropped out from image [13]. In deep learning convolution neural network (CNN) has ability to extract the best features from 3D biometric images. The CNN model

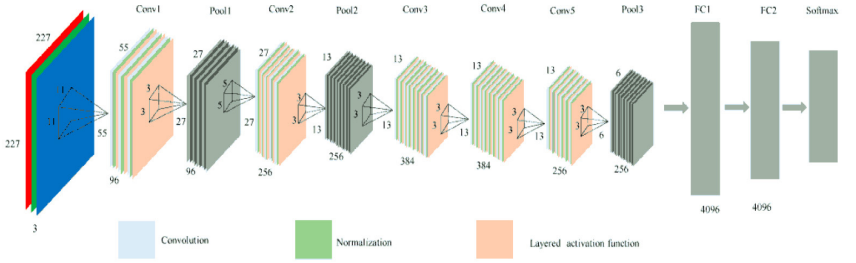

Figure 2

CNN model based on feature extraction of 3D biometric

comprises of probabilistic max-pooling, fully connected layers, layered activation functions with convolution, normalization, and layers. In this method, Utilizing CNN as a feature extractor, to extract different features from images after being pre-trained on a large sample size as shown in Figure 2 [14].

First, to alter and extract the picture information, the input image is convoluted using a variety of convolution kernels. Throughout the training phase, the filter coefficients are automatically calculated based on the characteristics of the input training images. The next layer, called the normalization layer, essentially stops the network from being over-fit and offers efficient gradient descent by normalizing the results of the convolutional process. The layer of the activation function receives the normalized data to increase the network's ability to express non-linearly. The activation function's output is then pooled, preserving the key characteristics and enhancing the model's tolerance to distortion. The forward propagation and feature extraction of network parameters are the fundamental component of the CNN's pre-training [14].

i. Forward Propagation

Through forward propagation, the network's parameters were discovered. The input features are computed as follows for each layer:

$$^{(i+1)} = LA(NA(C^{(i+1)}v^{(i)} + b(i+1)) \quad (1)$$

$v^{(i)}$ is the i-th layer's output vector, $v^{(i+1)}$ is (i+1)-th layer's vector output, LA() is the function of layered activation, NA is the normalized algorithm, $C^{(i+1)}$ is an inter-layer coefficients matrix, $b^{(i+1)}$ is biases vector.

1) Normalization Algorithm:

In order to avoid over-fitting and ensure the gradient effectively declines, it is typically important to choose the minimum learning rate while pre-training the network. When utilizing a high learning rate, normalization can stop over-fitting from happening. The chain rule was used to determine the normalization layer's back propagation gradient during the training phase [14]:

$$\frac{\partial L}{\partial \sigma^2} = -\frac{1}{2}\sum_{i=1}^{s}\frac{\partial L}{\partial y_i}(x_i-\mu)(\sigma^2)^{\frac{3}{2}} \tag{2}$$

Where Mean: $\mu = \frac{1}{s}\sum_{i=1}^{s} x_i$ Variance: $\sigma^2 = \frac{1}{s}\sum_{i=1}^{s}(x_i-\mu)^2$, Normalized value:

$$y_i = \frac{x_i-\mu}{\sigma}$$

$$\frac{\partial L}{\partial \mu} = \left(S_{i=1}^{s}\frac{\partial L}{\partial y_i}\frac{-1}{\sigma}\right) + \frac{\partial L}{\partial \sigma^2}\frac{-2\Sigma_{i=1}^{s}(x_i-\mu)}{s} \tag{3}$$

$$\frac{\partial L}{\partial x_i} = \frac{\partial L}{\partial y_i}\frac{1}{\sigma} + \frac{\partial L}{\partial \sigma^2}\frac{2(x_i-\mu)}{s} + \frac{1}{s}\frac{\partial L}{\partial \mu} \tag{4}$$

Back propagation formula is [14]:

$$\frac{\partial L}{\partial \varphi} = \frac{\partial L}{\partial \mu_B}\frac{\partial \mu_B}{\partial \varphi} = \frac{\partial L}{\partial \mu_B}(\mu-\mu_B) \tag{5}$$

$$\frac{\partial L}{\partial \psi} = \frac{\partial L}{\partial (\sigma_B{}^2)}\frac{\partial (\sigma B^2)}{\partial \psi} = \frac{\partial L}{\partial (\sigma_B{}^2)}(\sigma^2-\sigma_B{}^2) \tag{6}$$

Where φ and ψ are the combinations coefficients, global mean: $\mu_B = (1-\varphi)*\mu_B + \varphi*\mu$, global variance: $\sigma_{B^2} - (1-\psi)*\sigma_{B^2} + \psi*s^2$ [14]. In order to simplify the normalized calculation procedure, using the mini-batch data's mean and variance as well as the mean and variance over all dimensions were estimated. The mean and variance were both then updated in order to link all and someof these values.

2.2 *Feature Extraction*

The biometric images features are extracted using a feature extractor that is a pre-trained CNN model. The final fully linked layer's 4096-dimensional output is the eigenvector that CNN extracted. Figure 3 shows the structure of the fully connected layer.

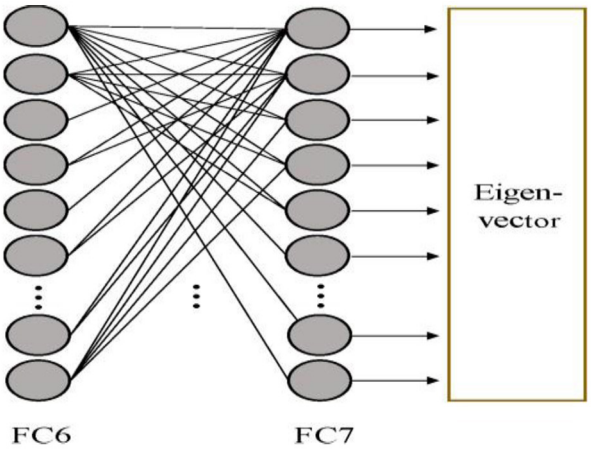

Figure 3

Fully connected layer's structure

The fully connected layered output is calculated using following formula [14]

$$v^{(i+1)} = \psi(W^{(i+1)}v^{(i)} + b^{(i+1)}) \tag{7}$$

Where (i) is the output vector, $v^{(i+1)}$ is the (i+1)-th layer's output vector, $^{(i+1)}$ is the biases vector, ( ) is the activation function and $W^{(i+1)}$ is represent the inter-layer linear coefficients matrix.

3. Role of Hashing Algorithms:

When assessing the security of the blockchain, it is crucial to take into account the encryption algorithm as analyzed by the attacker, the relationship between the cryptographic scheme's security notions and the mathematically difficult problems that underlie them, and any potential vulnerabilities introduced to the cryptosystem by the real-world application environment.[15]. A mathematical model known as a cryptographic hash function produces an alphanumeric string of fixed length from any input of data (string) of arbitrary length. Regardless of how many times the calculation is made, the function always returns the same hash for the same data. The hash can be used to check the accuracy of data because it cannot be reversed to recover the input data. This is why it is referred to as a one-way hash function [16]. The data inside a blockchain is secured using a hashing technique, blockchain networks are regarded as the most

Table 1

Hashing Algorithms with Output size (Bits)

Algorithms	Output size(bits)
MD5	128
SHA-1	160
SHA-2-224	224
SHA-2-256	256
SHA-2-512	512
SHA-3-224	224
SHA-256	256
SHA-512	512

secure. Different hashing algorithms are MD5, Secure hashing families (SHA-1, SHA-256, SHA-512) etc. Two levels of comparison between these hashing algorithms [17]. 1) On basis of output size (Bits) hashalgorithm. 2) CPU time according to input size. Table 1 shows the different hashing algorithms with their output size in Bits.

Different hashing algorithms are examined based on the output size (in bits).

Figure 4 shows that the security increases with the number of hash bits increases.

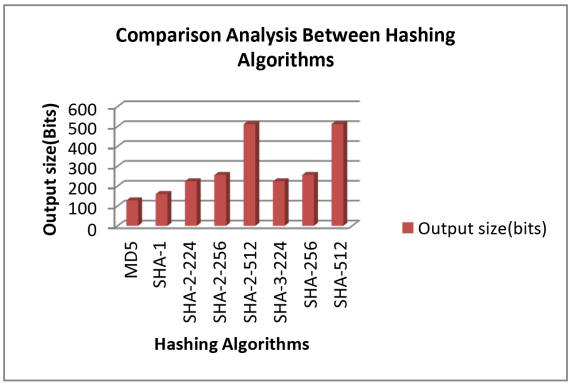

Figure 4

Comparative analysis between different hashing algorithmsbased on output size (bits)

Table 2

Three different input size with assigned time of each HashAlgorithm

Algorithms	Input Size(1KB)	Input Size(5KB)	Input Size(10KB)
MD5	0.2	0.2	0.2
SHA-1	0.01	0.1	0.1
SHA-256	0.1	1.5	1.6
SHA-512	0.6	2.6	3.4

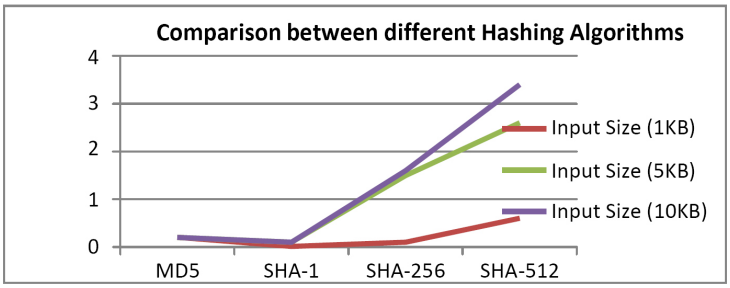

Figure 5

Comparison of Hashing Algorithm with blockchain usingdifferent input size

Table 2 shows three different input sizes with the assigned time of each Hash algorithm. According to the processing time limit, which shows that MD-5 is the fastest, speed can be taken into account as shown in Figure 5. Although SHA256 is superior to other algorithms in terms of security, so SHA-256 may be used to create hash values using the blockchain to attain a higher level of security.

4. Conclusion

In this work, we present a novel security system using the blockchain and biometrics, where face and ear biometric traits are used. Some of the most popular application areas that benefit from the integration of biometrics with Blockchain include distributed management, efficiency enhancement, security, prediction, and decision-making. Applications become more secure, effective, and productive when these two technologies are combined. Hashing algorithms used in blockchain increase the security of biometric information. Future work will focus on integrating deep learning more thoroughly and conventional methods for

using machine learning to address security issues of biometrics in more challenging contexts.

References

[1] Brown, R., Bendiab, G., Shiaeles, S., & Ghita, B. A Novel Multimodal biometric authentication system using Machine Learning and Blockchain. In International Networking Conference, pp. 31-46 (2020, September). Springer, Cham.

[2] Jagadiswary, D., & Saraswady, D. Biometric authentication using fused multimodal biometric. *Procedia Computer Science*, 85, 109-116 (2016).

[3] Kumar, A., Kanhangad, V., & Zhang, D. A new framework for adaptive multimodal biometrics management. *IEEE transactions on Information Forensics and Security*, 5(1), 92-102 (2010).

[4] Tharewal, S., Gite, H., & Kale, K. V. 3d face & 3d ear recognition: process and techniques. In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC), *IEEE*, pp. 1044-1049 (2017, September).

[5] Thawre, A., Hariyale, A., & Chandavarkar, B. R. Survey on security of biometric data using cryptography. In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), *IEEE*, pp. 90-95 (2021, May).

[6] Pothumani, S., & Arunachalam, A. R. Effective Security Mechanisms for Big Data Using Block Chain Technology. In 2021 International Conference on Computer Communication and Informatics (ICCCI). *IEEE*, pp. 1-6 (2021, January)

[7] Ramesh, G., Sharma, A., Lalitha Parameswari, D. V., Mallikarjuna Rao, C., & Somasekar, J. Blockchain in healthcare: Moving towards a methodological framework for protecting Biomedical Databases. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 891-901 (2022).

[8] Ramesh, G., Sharma, A., Lalitha Parameswari, D. V., Mallikarjuna Rao,C., & Somasekar, J. Blockchain in healthcare: Moving towards a methodological framework for protecting Biomedical Databases. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(4), 891-901 (2022).

[9] Nandakumar, K., & Jain, A. K. Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine,* 32(5), 88-100 (2015).

[10] Verma, I., & Jain, S. K. Biometrics security system: A review of multimodal biometrics based techniques for generating crypto- key. In 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) *IEEE*, pp. 1189-1192 (2015, March).

[11] Tharewal, S., Gite, H., & Kale, K. V. (2017, September). 3d face & 3d ear recognition: process and techniques. In 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC) (pp. 1044-1049). IEEE.

[12] Tharewal, S., Malche, T., Tiwari, P. K., Jabarulla, M. Y., Alnuaim, A. A., Mostafa, A. M., & Ullah, M. A. (2022). Score-Level Fusion of 3D Face and 3D Ear for Multimodal Biometric Human Recognition. ComputationalIntelligence and Neuroscience, 2022.

[13] Ganapathi, I. I., Ali, S. S., Vu, N. S., Prakash, S., & Werghi, N. (2022). A Survey of 3D Ear Recognition Techniques. ACM Computing Surveys (CSUR).

[14] Li, J., Qiu, T., Wen, C., Xie, K., & Wen, F. Q. (2018). Robust face recognition using the deep C2D-CNN model based on decision-level fusion. Sensors, 18(7).

[15] Wang, M., Duan, M., & Zhu, J. (2018, May). Research on the security criteria of hash functions in the blockchain. In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts (pp. 47-55).

[16] Ali, W. A., Sahib, N. M., & Waleed, J. (2019, August). Preservation authentication and authorization on blockchain. In 2019 2nd International Conference on Engineering Technology and its Applications (IICETA) (pp. 83-88). IEEE.

[17] Parmar, M., & Kaur, H. J. (2021). Comparative Analysis of Secured Hash Algorithms for Blockchain Technology and Internet of Things. *International Journal of Advanced Computer Science and Applications*, 12(3).