2023, 20(6 Suppl.): 2559-2567
https://dx.doi.org/10.21123/bsj.2023.8362
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

AlexNet Convolutional Neural Network Architecture with Cosine and Hamming Similarity/Distance Measures for Fingerprint Biometric Matching

Ahmed Sabah Ahmed AL-Jumaili*[1], Huda KadhimTayyeh[2], AbeerAlsadoon[3, 4, 5]

[1]Department of Business Information Technology, College of Business Informatics, University of Information Technology and Communications, Baghdad, Iraq.
[2]Department of Informatics Systems Management, College of Business Informatics, University of Information Technology and Communications, Baghdad, Iraq.
[3]School of Computing, Mathematics and Engineering, Charles Sturt University, Australia (CSU).
[4]School of Computer Data and Mathematical Sciences, Western Sydney University (WSU), Sydney, Australia.
[5]Asia Pacific International College (APIC), Sydney, Australia.
*Corresponding Author.

Received 12/01/2023, Revised 24/06/2023, Accepted 26/06/2023, Published 05/12/2023

Abstract

In information security, fingerprint verification is one of the most common recent approaches for verifying human identity through a distinctive pattern. The verification process works by comparing a pair of fingerprint templates and identifying the similarity/matching among them. Several research studies have utilized different techniques for the matching process such as fuzzy vault and image filtering approaches. Yet, these approaches are still suffering from the imprecise articulation of the biometrics' interesting patterns. The emergence of deep learning architectures such as the Convolutional Neural Network (CNN) has been extensively used for image processing and object detection tasks and showed an outstanding performance compared to traditional image filtering techniques. This paper aimed to utilize a specific CNN architecture known as AlexNet for the fingerprint-matching task. Using such an architecture, this study has extracted the significant features of the fingerprint image, generated a key based on such a biometric feature of the image, and stored it in a reference database. Then, using Cosine similarity and Hamming Distance measures, the testing fingerprints have been matched with a reference. Using the FVC2002 database, the proposed method showed a False Acceptance Rate (FAR) of 2.09% and a False Rejection Rate (FRR) of 2.81%. Comparing these results against other studies that utilized traditional approaches such as the Fuzzy Vault has demonstrated the efficacy of CNN in terms of fingerprint matching. It is also emphasizing the usefulness of using Cosine similarity and Hamming Distance in terms of matching.

Keywords: Biometric Cryptosystem, Convolutional Neural Network, Cosine Similarity, Fingerprint Matching, Information Security.

Introduction

Biometrics is the distinctive mark that identifies the uniqueness of a human for identity authentication purposes [1]. Unlike conventional security approaches like passwords or tokens which are subjected to loss and forgetting, biometrics represent a solid mechanism that offers a sophisticated way of privacy. It is associated with the physical features of people including fingerprint, retina, hand, eye, and face geometry. Since template data of biometrics is vulnerable to leakage, an integration between biometrics and cryptography has been introduced in a so-called bio-crypto system [2]. Recently, a wide range of real-world applications have become more reliant on bio-crypto systems.

2023, 20(6 Suppl.): 2559-2567
https://dx.doi.org/10.21123/bsj.2023.8362
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

The authentication of bio-systems has been examined through a validation process in which the physical features (i.e., fingerprint, face, eye, etc.) stored are compared with the collected features by a genuine user to ensure the match. In contrast, the cryptographic systems aim at securing the data by generating public and private keys using common encryption techniques such as Advanced Encryption System (AES), Rivest-Shamir-Adleman (RSA), Elliptic Curve Cryptography (ECC), and others [3-5]. Hence, the stored data is encrypted and the retrieval of such data would require decryption. In this regard, bio-crypto systems aim at securing the cryptography key using biometric features.

The literature showed a great interest in using sophisticated cryptography technologies, in particular, the fuzzy vault technique which aims to supplement the conventional cryptographic systems by incorporating biometric authentication. It relies on identifying the most significant/interesting patterns or features within the biometric which then be encrypted and stored. In such a coding process, the determination of significant features or vaults within the biometric is highly subjected to brute force attacks since fuzzy vaults are finite [6]. With the dramatic development of deep learning techniques, plenty of architectures have emerged to boost a wide range of tasks [7]. One of these architectures is the Convolutional Neural Network (CNN) which showed a remarkable performance in the image processing domain. CNN has magnificent capabilities to extract significant features of the image through the pooling mechanism.

This paper will extend the utilization of the CNN architecture for fingerprint biometric matching through distance measures including Cosine similarity and Hamming Distance. The contribution of this work can be summarized as follows:

- Utilizing the pretrained model of AlexNet to extract features of fingerprint biometric images.
- Perform matching on the extracted features using Cosine and Hamming distance measures.
- Compare results against the state-of-the-art.

The paper is organized as; Section 2 summarizes the related work, Section 3 describes the framework of the proposed method, Section 4 presents the results and discussion, and, Section 5 provides the final conclusion.

Related Work:

Several research efforts have been presented in the field of fingerprint verification using different techniques. For instance, Chitra and Sujitha[8] have proposed a bio-crypto system for fingerprint authentication using fuzzy vault technique. The authors have used the FVC 2002 database to collect fingerprint images.

Consequentially, the images have been segmented and preprocessed to collect minutiae features with a secret key to produce the fuzzy vault. Testing the proposed method through querying the stored template showed an accurate matching with the corresponding keys. This is due to the ability of fuzzy vault to produce a cryptographic framework that binds both the secret key and the biometric template.

Within a comparative analysis study, Tantubay and Bharti [9] established a comparison between bio-crypto system and traditional cryptography method. The authors have utilized the fuzzy vault technique as a bio-crypto method and the ECC as the traditional cryptography method. Results showed that an outperformance of the bio-crypto method in which the traditional cryptography has suffered from the large size of generated keys which affect the performance of matching among fingerprints.

Mehmood and Selwal[10] proposed a modified fuzzy vault for a secure fingerprint biometrics. The authors have increased the level of security by adding an integral operator to hide the key in case of polynomial leakage. Using the FVC-2002 database, the authors have demonstrated an enhancement in terms of False Accept Rate (FAR) and False Reject Rate (FRR).

Chang et al. [11] have proposed a bio-crypto system based on a combination of fuzzy commitment and fuzzy vault. Using the FVC-2002 database the authors have demonstrated an enhancement compared to the state of the arts fuzzy vault techniques.

Rahman et al. [12] have utilized the fuzzy vault approach in a parameterized manner where the extracted minutiae's parameters were used to hide the real minutiae information. This has been depicted by inserting additional synthetic minutiae. Rathgeb et al. [13] showed a multimodal bio-cryptography based on fuzzy vault where the

2023, 20(6 Suppl.): 2559-2567
https://dx.doi.org/10.21123/bsj.2023.8362
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

authors have examined human face along with fingerprint images.

Other studies have taken the advantage of deep learning architecture to accommodate the fingerprint matching. For example, Bakhshi and Veisi[14] have utilized a specific Convolutional Neural Network (CNN) architecture known as AlexNet to perform the fingerprint image matching. The authors have utilized the FVC2002 database to test their proposed method and it showed competitive performance against traditional techniques. Recently, Barzut et al. [15] have proposed the AlexNet architecture as an image discrimination technique. The authors have followed the traditional fuzzy commitment scheme in terms of key storing and retrieval. Yet, the CNN has been utilized to extract image features and accommodate the image matching (i.e., image classification). Using the FVC-2002 database, the authors have demonstrated an enhancement in terms of FAR and FRR.

Materials and Methods

The framework of the proposed method begins with the FVC2002 database where the fingerprint images are being brought. An image augmentation will be applied to increase the number of images. Consequentially, the images will be splitted into training and testing sets each of which will have the application of feature extraction using a particular CNN architecture. However, within the training, the feature vector extracted of each image will be stored in a reference database. Similarly, a key will be generated based on the biometric feature of the images and stored in such a reference database. Hence, the feature vector extracted of each image will be compared to the reference database using cosine similarity in order to identify the top match vector, as well as, a comparison of the key will be conducted using Hamming distance. Here, different thresholds will be explored for better matching results. Finally, based on the cosine matching and thresholding, a verification and evaluation phase will take a place in order to identify the robustness of the proposed fingerprint matching mechanism. Fig.1 shows the framework of the proposed method.

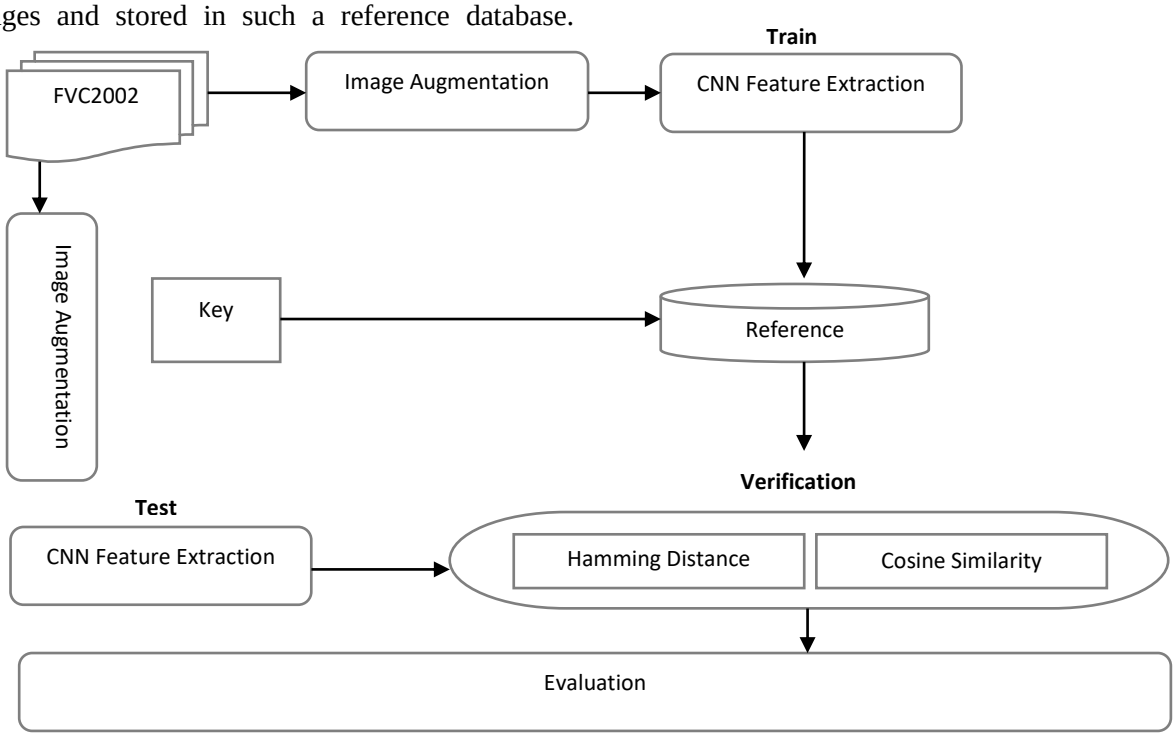


Figure 1. Framework of the proposed method

FVC2000 Dataset and Image Augmentation

In order to examine the fingerprint matching, a dataset with fingerprint images of FVC2002 [16] has been used. Such a dataset contains images of 110 fingers derived from an optical sensor that has a resolution of 500dpi. Every finger within such a dataset is composed of 8 impressions. Since the number of images seems insufficient, this paper has

2023, 20(6 Suppl.): 2559-2567
https://dx.doi.org/10.21123/bsj.2023.8362
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

utilized an image augmentation process inspired by [14, 17]. Such a process aims at increasing the images by creating variations through rotations and cropping. Such an augmentation process led to increase the number of each finger impression images by six. This has led to a total of images of 5280 (110×8×6) including genuine ones and imposters. Hence, a training and testing splitting has took a place where 90% of the images where randomly selected for training (i.e., 4752 images) and the remaining 10% were selected for testing (i.e., 528 images). The reason behind selecting such a ratio of splitting is to align with the baseline studies. Table 1 shows the details of the dataset.

Table 1. Dataset details

Attribute	Description
Image resolution	500dpi
Image dimension	256x364
Finger quantity	110
Impression quantity	8
Total images	880
Total images after augmentation	880×6 = 5280
Training set	5280×90% = 4752
Testing set	5280×10% = 528

On the other hand, a key will be generated along with the biometric features of each image. Such a key will be also stored in the reference database for later comparison. Advanced Encryption Standard (AES) has been used to generate 128-bit keys.

CNN Feature Extraction

CNN is a feedforward neural network that has been widely used for image processing and object recognition. Based on convolutional filters, CNN would have the ability to extract significant features of the image that enables the recognition and classification [18, 19]. In this study, a particular architecture of CNN known as AlexNet[20] will be used for extracting the features of each fingerprint image. AlexNet is a pretrained model that has been trained on a large set of images used for object detection brought from ImageNet dataset [21]. The reason behind using such an architecture lies in the advantage that would be acquired of the vast number of images that this architecture previously trained on which leads to robust features. Fig.2 shows the original architecture of AlexNet.

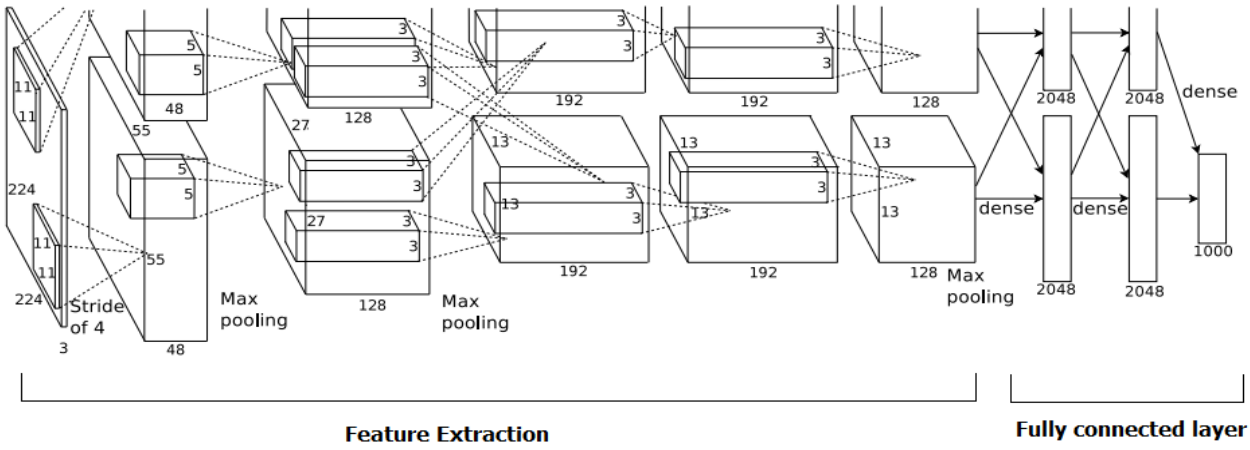


Figure2. Original architecture of AlexNet

Note that, only the feature extraction part (shown in Fig.2) will be used in this study to extract the feature vector of fingerprint images. As mentioned earlier, the goal is to take advantage of the robust features of AlexNet and then employ it for the task of matching rather than using it as a classification. The result of feature extraction has led to a vector with fixed length of 2048 for each fingerprint image. This vector will be stored as a reference within the training, and used in the comparison against reference within the testing. Table 2 shows the details of the original AlexNet architecture.

2023, 20(6 Suppl.): 2559-2567
https://dx.doi.org/10.21123/bsj.2023.8362
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Table 2. Hyperparameters of AlexNet

Attribute	Description
Convolutional layers	5
Epochs	200
Learning rate	0.0001
Batch size	96

Note that, the features of each image will be extracted from the flatten layer where pooling is adequately performed.

Cosine Similarity and Thresholding

Once the feature vector is extracted through AlexNet CNN during the testing, a comparison against the reference database is taking the place to identify the most similar fingerprint. For this purpose, the Cosine similarity is used to determine the similarity between the feature vectors. Cosine is a measurement that has been extensively utilized for the identifying vectors' similarity and it can be calculated as follows [22]:

$$Cosine(V_1, V_2) = \frac{V_1 . V_2}{\|V_1\| \times \|V_2\|} \qquad 1$$

where V1 and V2 are the feature vectors of the fingerprint images in which the former belongs to the testing and the latter belongs to the training as shown in Fig.3 The reason of selecting Cosine is that it performs better in computing the similarity of vectors [23].

The result of cosine similarity is a value between 0 which reflects total dis-similarity and 1 which reflects full match between the vectors. However, the between values would seem challenging to decide whether there is a matching or not. Therefore, multiple threshold values have been used for the matching decision including 0.3, 0.4, 0.5, 0.6, 0.7 and 0.8. Note that, the selection of threshold values will significantly be impacting the accuracy. This is because selecting a high value like 0.8 would only bring the most similar templates which will be few compared to selecting a low value like 0.3 which will bring many templates with low similarity.

Hamming Distance

Hamming distance is one of the algorithms used in the information theory where two keys with a fixed lengths are being compared in terms of differences. It aims to calculate the minimum number required for replacing bits to gain the full correspondence. In this regard, the Hamming distance will be used to identify the error rate between the train key and the test key. In this regard, there will be no threshold used, instead, an exact match is considered and mismatches will be accompanied with an error rate.

Evaluation

To evaluate the matching results, three common metrics will be used including False Accept Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (ERR). These metrics are intended to measure the accuracy and error rate of each fingerprint matching system. In addition, the reason behind selecting them is to align with the baseline studies since most of the state-of-the-art are using them frequently [24]. First, FAR concerns the number of correctly matches of imposters over the total number of imposters and it can be computed as follows:

$$FAR = \frac{correctly\ matches\ of\ imposters}{total\ number\ of\ imposters} \qquad 2$$

Whereas, FRR concerns the number of incorrectly matches of genuine over the total number of genuine and it can be computed as follows:

$$FRR = \frac{incorrectly\ matches\ of\ genuine}{total\ number\ of\ genuine} \qquad 3$$

Lastly, EER refers to the error rate at a particular threshold for which both FAR and FRR are identical.

2023, 20(6 Suppl.): 2559-2567
https://dx.doi.org/10.21123/bsj.2023.8362
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

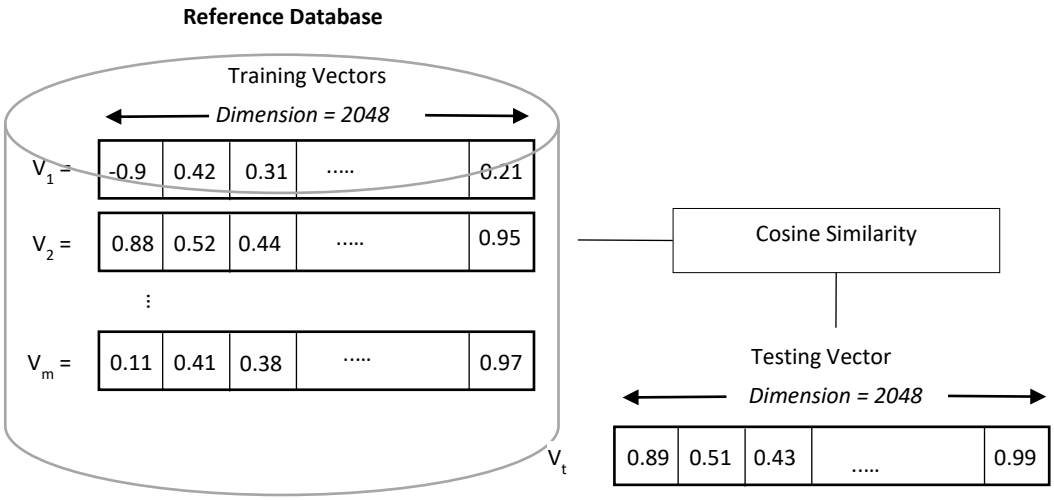


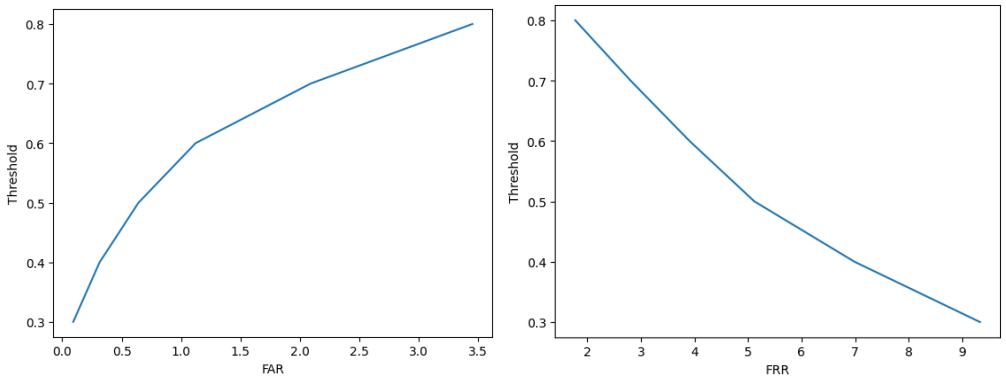
Figure 3. Matching through cosine similarity

Results

Using the proposed method with different values of threshold, the acquired results can be depicted in Table 3 and Fig.4 As shown in the results table, increasing the threshold value led to increase the FAR, meanwhile, decrease the FRR. This has been depicted where the lowest threshold (i.e., 0.3) had a FAR value of 0.092 and a FRR value of 9.333, while, the highest threshold (i.e., 0.8) had a FAR of 3.451 and a FRR of 1.776. Yet, the best results where both FAR and FRR are relatively similar were occurred at the threshold 0.7 in which the ERR was 2.49.

Table 3. Experimental results

Metrics	Threshold					
	0.3	0.4	0.5	0.6	0.7	0.8
FAR	0.092	0.314	0.641	1.122	2.09	3.451
FRR	9.333	6.988	5.119	3.91	2.81	1.776



(a) **(b)**

Figure 4. FAR and FRR results using different threshold of cosine

To put such results in the context of state-of-the-art, a comparison has been made against some baseline studies as shown in Table 4. It is obvious that the proposed method has outperform the studies with traditional techniques such as fuzzy vault. For example, the study of Chitra and Sujitha[8] along with the study of Mehmood and Selwal[10] have attained lower FRR compared to the proposed method as 25% and 8% respectively. In addition , the proposed method has outperformed the study of Bakhshi and

2023, 20(6 Suppl.): 2559-2567
https://dx.doi.org/10.21123/bsj.2023.8362
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Veisi[14] who used AlexNet with a fully connected CNN layer and achieving an ERR of 17.5%. Yet, the study of Barzut et al. [15] who used AlexNet has outperformed the proposed method in terms of FAR, FRR and ERR. The reason behind such an outperformance lies on the sophisticated classifier used by the study of Barzut et al. [15] compared to our method which depends on a pair-wise comparison through cosine and hamming distances. However, since the scope of this study is to address the capabilities of pre-trained CNN in terms of identifying significant patterns within biometric matching (i.e., feature extraction) thus, the role of classifier might seem as out of scope.

Table 4. Comparison against baselines

Study	Method	FAR	FRR	ERR	Dataset
Chitra and Sujitha[8]	fuzzy vault	1.00%	25.00%	-	FVC2002
Bakhshi and Veisi[14]	CNN (AlexNet)+ fully connected layer	-	-	17.5%	FVC2002
Mehmood and Selwal[10]	Enhanced fuzzy vault	-	8.00%	-	FVC2002
Barzut et al [15]	CNN (AlexNet) + XOR	1.25%	1.00%	1.13%	FVC2000
Proposed method	CNN (AlexNet) + Cosine	2.09%	2.81%	2.49%	FVC2002

Discussion

As depicted in the results, pre-trained CNN showed a competitive performance in terms of determining interesting patterns within biometric images. This demonstrates the promising capabilities of CNN and deep learning in general in the bio-crypto domain. CNN would not take the place of conventional approaches but it can be utilized as a complementary method since it has better analyzing of image features. Especially when dealing with a pre-trained model like AlexNet which has trained on a vast number of images and can articulate image features precisely.

Along with producing fair accuracy, the utility of using a pretrained model would accelerate the matching since it does not require training from the scratch. This could decrease the resource needed by biometric systems. On the other hand, the magnificent size of the pretrained model could contribute toward handling a wide range of datasets. Although this study has examined only one dataset which considered to be the main limitation behind this study, AlexNet can be utilized for different datasets.

Conclusion

In this paper, a fingerprint matching technique based on a pretrained CNN also known as AlexNet has been proposed. In this study, the AlexNet architecture has been used to extract the feature of the fingerprint image. Consequentially, a matching mechanism based on Cosine similarity and Hamming Distance has been used to compare the testing fingerprint image against a reference database. Using the FVC2002 database, the proposed method has demonstrated better performance against traditional techniques and competitive performance against other CNN architectures. Besides, since AlexNet is a pretrained model it will accelerate the matching while reducing the resources needed. The main limitation behind this study lies in using only one dataset yet, the capabilities of AlexNet can be demonstrated on different datasets. For future directions, the utilization of Multi-task Cascaded Convolutional Neural Network (MTCNN) would contribute toward better matching results.

Acknowledgment

This study is supported by the University of Information Technology and Communications.

Authors'Declaration

- Conflicts of Interest: None.

- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, anyFigures and images, that are not ours, have been included with the necessary permission for re-publication, which is attached to the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in University of Information Technology and Communications.

Authors' Contribution Statement

This paper was carried out in collaboration between all authors. A. S.A has identified the research gap prepared the literature and wrote the manuscript. Whereas, H.K.T carried out the experiments and analyzed the results. Lastly, A. A was mentoring the entire process and gave the needed feedbacks.

References

1. Ackerson JM, Dave R, Seliya N. Applications of Recurrent Neural Network for Biometric Authentication & Anomaly Detection. Info. MDPI. 2021; 12(7): 272. https://doi.org/10.3390/info12070272
2. Ryu R, Yeom S, Kim SH, Herbert D. Continuous Multimodal Biometric Authentication Schemes: A Systematic Review. IEEE Access. 2021; 9: 34541-57. https://doi.org/10.1109/ACCESS.2021.3061589
3. Asthana R, Walia GS, Gupta A. A Novel Biometric Crypto System Based on Cryptographic Key Binding with User Biometrics. Multimed Syst. Springer. 2021 Mar; 27(5): 877-91. https://doi.org/10.1007/s00530-021-00768-8
4. Hasoun RK, Khlebus SF, Tayyeh HK. A new approach of classical Hill Cipher in public key cryptography. Int J Nonlinear Anal Appl. Semnan University. 2021 Jul; 12(2). https://doi.org/10.22075/ijnaa.2021.5176
5. Tayyeh HK, AL-Jumaili ASA. A combination of least significant bit and deflate compression for image steganography. Int J ElectrComput Eng. 2022 Feb; 12(1): 358. https:/doi.org/10.11591/ijece.v12i1.pp358-364
6. Abiega-L'Eglisse AFD, Gallegos-Garcia G, Nakano-Miyatake M, Otero MR, Hern´andez VA. A New Fuzzy Vault based Biometric System robust to Brute-Force Attack. Comp y Sist. 2022 Sep; 26(3): 1151-1165. https://doi.org/10.13053/cys-26-3-4184
7. AL-Jumaili ASA, Tayyeh HK. Recurrent neural network document embedding method for adverse drug reaction detection from medical reviews. Int J InnovComputInf Control. 2022 Jan; 16(1): 101-8. https://doi.org/10.24507/icicel.16.01.101
8. Chitra D, Sujitha V. Security Analysis of Prealigned Fingerprint Template Using Fuzzy Vault Scheme. Cluster Comput. Springer. 2018 Jan; 22(S5): 12817-25. https://doi.org/10.1007/s10586-018-1762-6
9. Tantubay N, Bharti J. A Survey of Biometric Key-Binding Biocrypto-System Using Different Techniques. Int J Emer Tech; 2020. 11(1): 421-32. https://www.researchtrend.net/ijet/pdf/A%20Survey%20of%20Biometric%20Key-Binding%20Biocrypto-System%20using%20different%20Techniques%20IJET-RT-1491-CSE-%20Neeraj%20TantubayI_New.pdf
10. Mehmood R, Selwal A. Polynomial Based Fuzzy Vault Technique for Template Security in Fingerprint Biometrics. Int Arab J Inf Technol. 2020; 17(6): 926-34. https://doi.org/10.34028/iajit/17/6/11
11. Chang D, Garg S, Ghosh M, Hasan M. BIOFUSE: A Framework for Multi-Biometric Fusion on Biocryptosystem Level. Info Sci, Elsevier. 2021; 546: 481-511. https://doi.org/10.1016/j.ins.2020.08.065
12. Rahman MM, Mishu TI, Bhuiyan MAA. Performance analysis of a parameterized minutiae-based approach for securing fingerprint templates in biometric authentication systems. J InfSecur Appl. 2022; 67: 103209. https://doi.org/10.1016/j.jisa.2022.103209
13. Rathgeb C, Tams B, Merkle J, Nesterowicz V, Korte U, Neu M. Multi-Biometric Fuzzy Vault based on Face and Fingerprints. arXiv. 2023. https://doi.org/10.48550/arXiv.2301.06882
14. Bakhshi B, Veisi H. End to End Fingerprint Verification Based on Convolutional Neural Network. 2019 27th Iranian Conference on Electrical Engineering.IEEE. 2019; 2019: 1994-8. https://doi.org/10.1109/IranianCEE.2019.8786720
15. Barzut S, Milosavljević M, Adamović S, Saračević M, Maček N, Gnjatović M. A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks. Math. MDPI. 2021; 9(7): 730. https://doi.org/10.3390/math9070730
16. Maltoni D, Maio D, Jain AK, Prabhakar S. Handbook of Fingerprint Recognition. Springer. 2009. https://doi.org/10.1007/978-1-84882-254-2
17. Zhu Y, Yin X, Hu J. Robust Fingerprint Matching Based on Convolutional Neural Networks. Lect Notes InstComput Sci. Springer. 2018: 56-65. https://doi.org/10.1007/978-3-319-90775-8_5
18. Alsaedi EM, KadhimFarhan A. Retrieving Encrypted Images Using Convolution Neural

2023, 20(6 Suppl.): 2559-2567
https://dx.doi.org/10.21123/bsj.2023.8362
P-ISSN: 2078-8665 - E-ISSN: 2411-7986
Baghdad Science Journal

Network and Fully Homomorphic Encryption. Baghdad Sci J. 2022; 20(1): 0206-0206. https://doi.org/10.21123/bsj.2022.6550
19. Hasan AM, Qasim AF, Jalab HA, Ibrahim RW. Breast Cancer MRI Classification Based on Fractional Entropy Image Enhancement and Deep Feature Extraction. Baghdad Sci J. 2022; 20(1):0221-0221. https://doi.org/10.21123/bsj.2022.6782
20. Krizhevsky A, Sutskever I, Hinton GE. ImageNet Classification with Deep Convolutional Neural Networks. Commun ACM. 2017; 60(6):84–90. https://doi.org/10.1145/3065386
21. Deng J, Dong W, Socher R, Li LJ, Li K, Fei-Fei L. ImageNet: A Large-scale Hierarchical Image Database. Conference on Computer Vision and Pattern Recognition. IEEE. 2009: 248-55. https://doi.org/10.1109/CVPR.2009.5206848
22. Zhou L, Xiao Y, Chen W. Imaging Through Turbid Media with Vague Concentrations Based on Cosine Similarity and Convolutional Neural Network. IEEE Photonics J. 2019; 11(4): 1-15. https://doi.org/10.1109/JPHOT.2019.2927746
23. Artetxe M, Labaka G, Agirre E. Learning Principled Bilingual Mappings of Word Embeddings While Preserving Monolingual Invariance.In Proceedings of the 2016 Conference on Empirical Methods in Natural Language Processing. ACL. 2016; 2016:.2289-94.http://dx.doi.org/10.18653/v1/D16-1250
24. Hammad M, Liu Y,Wang K. Multimodal Biometric Authentication Systems Using Convolution Neural Network Based on Different Level Fusion of ECG and Fingerprint. IEEE Access. 2019; 7: 26527-42.https://doi.org/10.1109/ACCESS.2018.2886573

التعرف على بصمات الأصابع باستخدام الشبكات العصبية اللفائفية (اليكس نت) ومقاييس التشابه جتا الزاوية وهامنج

أحمد صباح أحمد الجميلي[1]،هدى كاظم تايه[2]،عبير السعدون[3,4,5]

[1]قسم تكنولوجيا معلومات الاعمال، كلية معلوماتية الاعمال، جامعة تكنولوجيا المعلومات والاتصالات، بغداد، العراق.
[2]قسم ادارة انظمة المعلوماتية، كلية معلوماتية الاعمال ، جامعة تكنولوجيا المعلومات والاتصالات، بغداد،العراق.
[3]كلية الحوسبة والرياضيات والهندسة، جامعة تشارلز ستورت، أستراليا (CSU).
[4]كلية بيانات الكمبيوتر والعلوم الرياضية، جامعة غرب سيدني (WSU)، سيدني، أستراليا.
[5]كلية آسيا والمحيط الهادئ الدولية (APIC)، سيدني، أستراليا.

الخلاصة

يعد التحقق من بصمة الأصبع أحد الطرق الحديثة في مجال أمن المعلومات والذي يهدف إلى إيجاد أنماط مميزة للتعرف على هوية الفرد. يتم ذلك عبر عملية مقارنة بين أزواج من نماذج معدة مسبقا للبصمة وإيجاد نسبة التشابه بينهم. غالبية الدراسات السابقة كانت تعتمد على طريقة تدعى (فازي فالت) بالإضافة إلى طرق فلترة الصور. لكن هذه الطرق لا تزال تعاني من ضعف تمييز النقاط المهمة في البصمات، ظهور التقنيات الحديثة من التعلم العميق مثل الشبكات العصبية اللفائفية قد ساهم بشكل كبير في تحليل الصورة والتعرف على الكيانات داخل الصور وقدأظهرت دقة أعلى من الطرق التقليدية. هذه الدراسة استغلت إحدى هذه الشبكات المدربة مسبقا على صور بصمات وتعرف باسم (اليكس نت) بحيث تم استخراج أهم الخصائص الكامنة بالصور وتم توليد مفتاح خاص بكل صورة ومن ثم تم تخزين كل تلك المعلومات في قاعدة بيانات مرجعية. باستخدام أدوات قياس التشابه مثل جتا الزاوية وهامنج استطاعت هذه الدراسة من تبيان التشابه خلال مقارنة صور اختبارية بالنسبة لقاعدة البيانات المرجعية. تم استجلاب الصور من قاعدة بيانات عامة وقد أظهرت نتائج دقة القبول دقة الرفض على نسبة 2.09% و 2.81% على التوالي. بمقارنة هذه النتائج مع نتائج الدراسات السابقة خصوصا تلك التي استخدمت أدوات تقليدية مثل (فازي فالت) تفوق الطريقة المطروحة بهذه الدراسة. وبذلك تم استنتاج أهمية استخدام الشبكات العصبية اللفائفية مع أدوات قياس التشابه في التعرف على بصمة اليد.

الكلمات المفتاحية:أنظمة تشفير أصبع اليد،الشبكات العصبية اللفائفية،جتا الزاوية،تطابق بصمة اليد،أمن المعلومات.