

A novel multi-biometric technique for verification of secure e-document

Ammar Mohammed Ali¹, Alaa Kadhim Farhan²

¹Chemical Engineering Department, University of Technology, Baghdad, Iraq

²Computer Sciences Department, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received Jul 12, 2021

Revised Oct 5, 2023

Accepted Oct 6, 2023

Keywords:

Biometric technologies

Fingerprint

Security

Time

Verify the identity

ABSTRACT

Extracting unique and distinctive traits is one of the most important challenges that researchers face, who rely on biometrics to extract exceptional traits for an individual. A large amount of biometric evidence that can be identified and found in various research has been done. In this paper, a biometrics system is proposed that combines the benefits of fingerprinting and uses a novel strategy to combine it with the image-based fingerprint vein feature set. The proposed system is fast and performs effective personal identification by combining both features. The features extracted from the venous print and fingerprint are matched to the nearest neighbors of the authorized person forms to verify the identity of the person. Several experiments have been performed on selected datasets to evaluate the performance of the new biometrics system. The obtained results prove that our proposed system is superior to biometric systems that use the feature of single biometrics. However, our goal is to set up an algorithm that is inexpensive in terms of time complexity while keeping it at the required security levels.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Alaa Khadim Farhan

Computer Sciences Department, University of Technology

Baghdad-10066, Iraq

Email: 110030@uotechnology.edu.iq

1. INTRODUCTION

Biometric technologies usually refer to the use of innovation and research on an individual dependent on part of his knowledge. Recognition of the unique mark is one of the individual and unique biometric developments that were freely gathered under computerized criminology. The verification process, in general, can serve as a review, examination, and test to ensure the strength of the system. Manual verification suffers from many problems. It is old, inefficient methods, high cost, and lack of experience in error diagnosis steps. It takes a long time because it depends on the human. Discovering the current state of uses and studies on documenting and verifying electronic documents and electronic archives has become one of the most important things to transfer in this world. They occasionally adapt to various reports, confessions, licenses, and other records that secure more than the legitimacy of need, while others secure documents that are safer than lack of authentication [1], [2].

As a result of a large degree of continuous use of electronic documents, it caused the introduction of information technology in our daily lives for specific mobile devices and various social networks. There are many methods used to verify and authenticate, as we must think about modern electronic methods that do not depend in the verification process on the authenticity of documents, and human experience [3]–[5]. Technologies will significantly outperform deliver accuracy and save time where validation depends on the parameters extracted from the digital signature solution prepared for this purpose, based on several

techniques used to process different types of images. The main objective of this research paper is to reduce cases of forgery and tampering in electronic documents. Many researchers extracted different biometric features from finger veins and fingerprints such as [6]–[8]. Methods using biometric devices have been developed and optimized to simulate a high-safety feature. To achieve this goal, some researchers resorted to developing multimedia biometric systems. Individual biometric systems differ in many types, including fingerprints, finger veins, hands, iris, and amplifiers. Regardless of all the traditional methods of authentication studies, biometrics systems have emerged and have played an effective role in many areas, especially in industry and in various management matters. The different methods and techniques have been used to implement the system [9]–[11]. The proposed system observed respect for the issue of validation and verification, which are explained in detail in the rest of the paper.

2. SECURITY AND AUTHENTICATION SYSTEM

The data varies according to the different types and methods of storing it, including big data and database and their management [12] or electronic data and documents, and all types of data used in different systems need to follow different methods of extracting data and dealing with it [13], [14] and adopt the concept of authentication. Authentication may include approving individual personality records, confirming the credibility of a site with an electronic certificate [15], [16]. Lee *et al.* [15] have studied digital signature standard schemes to explore their potential applications in various fields. The term advanced verification, otherwise called electronic confirmation or e-validation, alludes to a gathering of procedures where the certainty for client characters is set up and introduced through electronic strategies to a data framework. The validation of data can present extraordinary issues with electronic correspondence, for example, weakness to man-in-the-center assaults, whereby an outsider takes advantage of the correspondence stream, and stances as every one of the two other imparting parties, to block data from each. Additional personality variables can be required to verify each gathering's character [17], [18].

3. PREVIOUS WORKS

Document validation has been carried out by comparing both the signature and the sample that was relied upon at the time of document verification. The merging of features of each of the fingerprints is combined with the venous finger, and each of them carries multiple biometrics features, which represent the traits of multiple traits that may be different and sometimes incompatible with each other, many conditions and obstacles accompany the use of biometric devices such as hand moisture, placing a weak finger, dirt, and dust on the screen of the scanner, which takes pictures of the fingerprint, whether the fingerprint or intravenous fingerprint, these conditions, and others, have helped open the magazine to researchers to overcome obstacles, through research the best way. Therefore, in this research, a proposal has been made to suggest a new way to create unique and powerful features that address the weak points and problems of fingerprint extraction. As a review of the finger vein recognition system, numerous ongoing existing finger vein acknowledgment frameworks including picture preprocessing, highlight extraction, and arrangement stage have been investigated. The examination should concentrate on the key issue and the future works that are talked about in this paper to beat the shortcomings of the past techniques to build up an all the more remarkable finger vein-based identification or verification or check framework [19].

The palmprint and palm vein images are fused by a new edge-preserving and contrast-enhancing wavelet fusion method in which the modified multiscale edges of the palmprint and palm vein images are combined [20]. In [21], a fusion of finger vein (FV) and finger-knuckle-print (FKP) images have been applied and planned to build up a quick calculation for individual distinguishing proof. Since there is no open multimodal database of FV and FKP pictures, in this paper a gadget that can catch both FV and FKP pictures has been arranged to carry out this responsibility.

In the area of secure document authentication, facial recognition techniques were used to authenticate secure documents based on a two-to-two diode pattern and a directed gradient graph. It offers benefits for clinical registry purposes, web-based banking services, driver's licenses, personal identification, and robotic identity verification-officer controls and law requirements as well. This relies on a strategy based on facial features such as eyes, nose, and mouth, and they take care of their areas and nearby visions in the workbook. In this paper, we addressed the problems related to the feature extraction from the palmprint in a framework related to the biometric authentication of individuals [22]–[24].

4. PROPOSED METHOD

Our use of several additional successful features has had a major impact on increasing the ability to recognize and verify the system. Therefore, it can be said that the biometric system is used to identify and at

the same time authenticate. The merging of features of each of the fingerprints is combined with the venous finger and each of them carries multiple biometrics features, which represent the traits of multiple attributes that may be different and sometimes incompatible with each other, so it came to our suggested way to create new features that are capable of to overcome the weaknesses in the features extracted from the fingerprint. Not so long ago, different types of composite biometrics frameworks were created and synthesized, which include unique frames for each of the distinctive features of the face, voiceprint, and fingerprint. Regardless of the traditional verification strategies, isometric frameworks have been effectively developed in various businesses and management matters, and these methods go forward in giving higher safety points to reach the control framework. Fingertip vein design is a new and fast biometric feature that has been considered by many professionals as a promising option for identifiable identification.

The design of biometric veins, such as the human blood vessels of a distinct individual, depends on how each individual has a unique vein-type design. Since many external biometric traits, for example, a unique mark, palm imprint, and face accentuation are progressively helpless against spelling and can be manufactured using moderate endeavors for it, dependence and safety are becoming a major problem against these discriminatory biometric traits evidence-proof. Likewise, clinical tests have shown that the design of veins in each individual is unique and stable for an extended period.

4.1. Main structure of proposed algorithm

The document authentication process is based on biometric features. Where the extracting unique features and described both fingerprints and at the same time it is veins. These properties are documented on the document in the form of an electronic fingerprint. It is used to get to know the authenticity of the document later. Accordingly, different arithmetic settings are adopted to process regular and safe biometric accounts. The computing of this field depends on two parties, the first party represents the basic database that contains the ideal characteristics of fingerprints and finger veins for authorized persons. The second part represents the fingerprint on the document, meaning that each party has their entries, and they will work together to calculate a function and validate the document. Therefore, the advantages and characteristics of biometric features such as fingerprints and veins are difficult to counterfeit, especially in the case of merging them just as in our proposed system, unlike ID cards where it is easy to copy and falsify the signature while it is difficult to copy biometric features. Verifications were made by following different methods and techniques, which range from following traditional methods through the calculation of a simple Euclidean distance or by relying on crossbreeding works. In this paper, a system has been proposed to verify the authenticity of electronic documents by relying on multi-character biometric features that depend on both the fingerprint and the fingerprint. As a result of the different acquisition conditions of the biometric devices for taking fingerprint images or finger veins, many obstacles appeared, such as moisture on the hand, dust on the screen of the open, or even the poor position of the finger, making the field open for researchers to search for an appropriate method that can overcome all these obstacles. The merging of features of each of the fingerprints is combined with the venous finger, and each of them carries multiple biometrics features, which represent the traits of multiple traits that may be different and sometimes incompatible with each other, so it came to our suggested way to create new features that are capable of to overcome the weaknesses in the features extracted from the fingerprint. Our proposed system relies on two main features: The designation circular projection was launched to calculate the density of the image for which the features were to be extracted While the second type relied on groups for multi-set features as these two types of features were used in our proposed methods and as will be explained in the next sections.

- Proposed algorithm 1 (discrete processing): Creating features from separate finger vein and fingerprint

In our proposed multi-biometric system on the method of combining both fingerprints, the scanning is done through the use of a special scanner whose specifications are shown in this paper, which performs a scanning process for both the fingerprint and veins at the same time and gives us two different devices. We can clarify the basic steps that will be explained in the following diagram. The main steps of the proposed algorithm 1 can be summered as flowing. The first proposed algorithm (discrete processing).

The feature vectors extracted from both the fingerprint and finger vein data are stored in the system as two separate vectors, denoted as (PPF) for fingerprint features and (VPF) for finger vein features. These vectors, (PPF, VPF), are designed to be used for verification purposes at a later stage. This verification can take place either independently, where the fingerprint and finger vein data are checked separately, or in a combined manner, where both sets of data are considered together to enhance the accuracy of the authentication process. Figure 1 illustrates this concept further.

- Proposed algorithm 2: Create a novel 67 features as proposed multiset features (discrete processing).
- Proposed algorithm 3 (combine processing): Creating features from finger vein and fingerprint.

Algorithm 1. Creating features from separate finger vein and fingerprint

Input: Fingerprint and finger vein image

Output: Biometric features

Begin

Step 1: The vein image is extracted from the special biometric scanner.

Step 2: The image is initially processed to improve it.

Step 3: The fingerprint is extracted from the special scanner device.

Step 4: Initially manipulate the image to improve it,

Step 5: The edges of both images (fingerprint and veins) are extracted by applying the sharp edges method using canny edge detection.

Step 6: The intensity of the projection is calculated circularly, through the center of the image, and it is adopted to calculate the precipitation at all angles at an angle of 360 degrees, to obtain 360 features that represent the density of the image in different directions, where this method can be called a circular projection.

End

Algorithm 2. Multiset features (discrete processing)

Input: Fingerprint and finger vein image

Output: Biometric features

Begin

Step 1: The first 60 features can be obtained by any method of algorithm1: the 360 features are divided into 60 features. Each of these features is an average of 6 out of 360 features, meaning that we used to choose a sliding window in the form of a fan blade.

Step 2: Two features from the center of gravity [25] of the first image (p1) the center of gravity concerning the individual (i) can demonstrate in the following format.

$$cog = \frac{\sum(x * y)}{\sum(y)}$$

Step 3: Two features from the center of gravity of the second image (p2).

Step 4: Number of intersect between p1 & p2.

Step 5: Calculate the mean of the image: mean(p1), mean(p2); Where xi denotes the pixel of the image

Step 6: Mean(intersect)

End

Algorithm 3. Features from finger vein and fingerprint

Output: Biometric features

Begin

Step 1: The vein image and fingerprints are extracted from a biometric scanner and enhanced these images as we explained in the previous method.

Step 2: The image of the finger vein and fingerprints is combined to produce a new image that will be dealt with and extract features from it.

Step 3: The edges of the image are extracted using (canny Edge Detection). And then preprocess the vein images to match the size of the fingerprint image.

Step 4: The 360-degree circular features are extracted as in the previous method, but the difference in this method is that we applied this method by extracting the features after combining the two images (the vein image and the fingerprint image). This method can be called circular projection, which denotes the set of properties of both images, as shown in Figure 2 which illustrates the basic steps illustrating the block diagram of proposed algorithm 1 (combine processing).

End

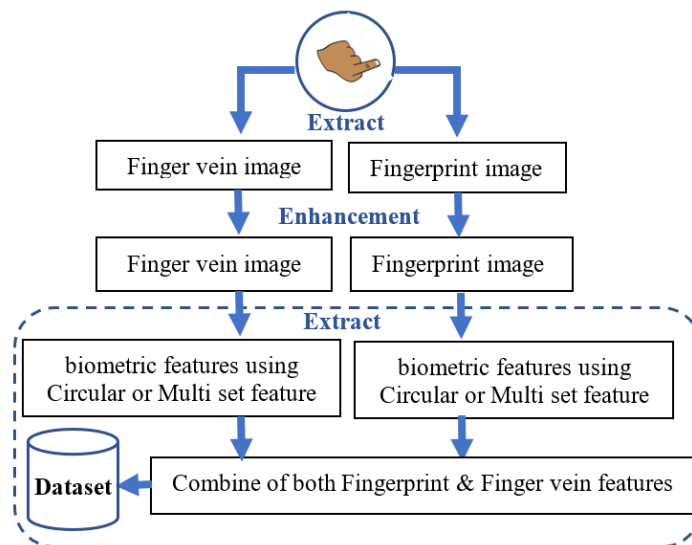


Figure 1. The block diagram of the proposed algorithm discrete processing

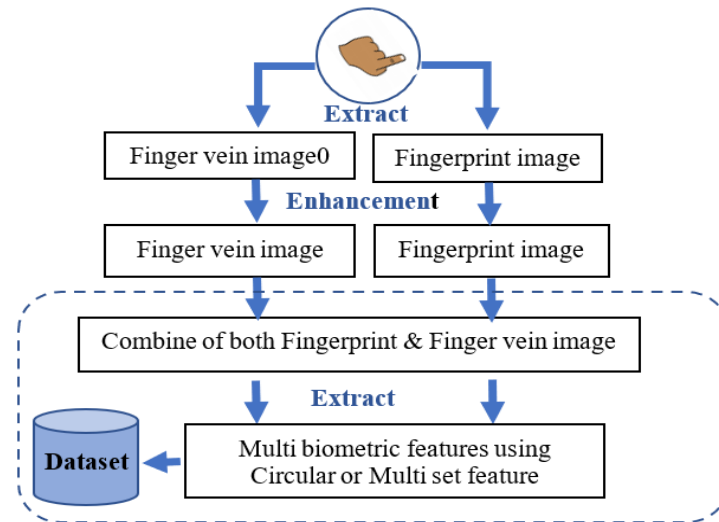


Figure 2. The block diagram of the proposed algorithms 1 and 2 (combine processing)

5. EXPERIMENTAL RESULTS AND DISCUSSION

The verifications are made by different methods, which range from traditional methods through the calculation of a simple Euclidean distance or by relying on crossbreeding works. In this paper, a system has been proposed to verify the authenticity of electronic documents by relying on multi-character biometric features that depend on both the fingerprint and the fingerprint. In light of the results inspired by practical experiences, we can see the great effectiveness of our proposed method by achieving high degrees of accuracy and distinction as we relied on various methodologies for each approach, and the calculation time is required to extract properties. This research relied on a versatile scanner device that takes both fingerprint and vein fingerprints at the same time and stores them as two separate images. This will be addressed later in this research. We can observe from the practical results, the great superiority of our system by achieving the highest levels of accuracy and distinction by relying on methodologies that rely on new and different structures that adopt an approach that avoids complexity while maintaining the time required for calculating and extracting properties. A very large number of experiments were conducted on the selected data groups to evaluate the features extracted from our biometric system. In the step of obtaining information, intravenous images are taken using an infrared scanner. This is another major feature of validating finger vein design by adopting biometrics. Correct index finger index images were used for individuals to create and evaluate forms, knowing that our proposed system can rely on any of the fingers of the hand. Moreover, the proposed framework is organized in a single layer that combines the integration of extracted characteristics with the preservation of information security. The verification accuracy of the proposed default dataset when using an expansion procedure by combining the features of a fingerprint with a vein is better than using a dataset that relies on individual features. There are many problems with the finger, such as the deformation of the skin surface, which weakens the accuracy of the frame.

5.1. Evaluate proposed different methods to extracted different features vector

Features are extracted from fingerprints and venous fingers in several ways that a comparison has been made between these methods. We can notice that each of the extracted features depends on the method and mechanism of work that differs from the other. The extracted features are variable with the different and changing method, which are the outputs of each road different from the outputs of the second method, in terms of the number of features extracted, which represents the size of the feature vector.

5.1.1. First way

Features derived from the first method using a multi-biometric principle. Multiple biometric features were extracted by doing a pre-treatment of the features extracted by the template, by making the size of the finger vein features the same size as the fingerprint features including performing one of the two operations: i) Delete from the fingerprint features file if its size is larger from 702 arranged to be the same size and ii) Add a set of zeros if it is smaller than 702 arranged to be the same size). Then the procedure for dividing the two features is taken. This requires adding the number 1 to all elements in extracted features, that is, to all ranks for each feature, to avoid dividing by zero in the next stage. This addition of number one did not affect

the general distribution structure of the features; that means the relationship (distance) between extracted features is the same. For example, if the extracted trait is 7 4 3 2 1 then when adding 1 it becomes 8 5 4 3 2. Note that the trip connecting the elements is the same ($7-4=8-5$) and ($4-3=5-4$).

The last steps of this method are introduced using a multi-biometric principle: We denote the fingerprint features as FPF:($FPF+1=FPF1$). Where we code FPF1 fingerprint features after adding 1. We denote the finger vein, characterized by the symbol FVF which means ($FVF+1=FVF1$) It is characterized by the symbolization of FVF1 fingerprint vein after adding 1. Multiple biometrics features= $FPF1/FVF1$.

5.1.2. Second way

Features are extracted from proposed algorithm 1 (discrete processing): creating a novel 360 features from separate finger vein and fingerprint in this research to extract the circular projection features of fingerprint and venous finger separately. Initial treatment of this is done by adding No. 1 to all elements of the extracted features. Accordingly, as in the previous method, multiple features will be extracted as multiple biometrics features= $FPF1/FVF1$.

5.1.3. Third way

Features are extracted from fingerprints and venous finger separately by applying proposed algorithm 2 that create a novel 67 features as proposed multi set features (discrete processing) as we discussed before. Initial processing is done by adding no. 1 to all elements of the extracted features. Accordingly, as in the previous method, multiple features will be extracted as multiple biometrics features= $FPF1/FVF1$.

5.1.4. Fourth way

The paragraph discusses a feature extraction process involving both fingerprints and finger vein characteristics. It employs algorithm 1, known as "combine processing," to create a novel set of 360 features by merging information from finger vein and fingerprint features. The key aspect of this feature extraction method is the utilization of circular projection features, which are derived from the combination of two distinct images, namely fingerprint and venous finger images, as previously explained in the text. This paragraph underscores the innovative nature of this approach, highlighting the integration of two different biometric data sources to produce a comprehensive set of 360 features, with a particular focus on the circular projection technique.

5.1.5. Fifth way

Features have extracted both fingerprints and fingering by applying proposed algorithm 2 that creates a novel 67 features as proposed multi set features (combine processing). Extraction of multiset features is supported by combining the two images (fingerprint and venous finger), as discussed before. Accordingly, after making a comparison between the previous methods in this research paper, the highest level of distinction for the extracted features is recorded in the fourth method and the fifth method. So, we recommend adopting them in extracting features due to their high efficiency.

5.2. Create a new real dataset to improve the proposed system

5.2.1. The first sub dataset

In this paragraph, a new data sets resulting mentions from experimental tests. These data sets consist of a total of 260 images depicting finger veins, and they have been positioned in a manner corresponding to the fingers mentioned in the data labeled as Figure 3. This implies that the data sets have been carefully curated and organized to align with the specific conditions and parameters. This information signifies a crucial step in the research or study being conducted, indicating the availability of a well-prepared data resource for further analysis or investigation.

5.2.2. Second sub dataset

In 260 fingerprint pictures, 26 people were chosen; each person has ten pictures of the same finger. Each picture is from the ten pictures of the same finger taken in a different position and at different times. were taken, in each position, one of two different images is extracted, the first is the image for the vein and the second with a fingerprint, and that is the base of the number of 26 items each class represents a person. Figure 4 gives an example of the first two classes in the dataset.

5.2.3. The third sub dataset

The special photos collect a fingerprint of the special needle in the same position as the fingers at the base of the data. That gives an example of the first two classes in the dataset. Our proposed system is applied to a large group of fingerprints and venous fingers that were randomly selected to demonstrate the

strength of our proposed system. Our proposed algorithms were adopted in this research to feed data sets for use in electronic document authentication and verification systems. In addition to the tests conducted on the selected models, where all the results we obtained were satisfactory and subject to the criteria of the balance between time and complexity, Figure 5 gives an example of computing circular projection features on canny edge detection of Finger vein and fingerprint. It is easy and clear to explain this method through the simple mathematical model that can be found with following equation:

$$\sum_0^{360} \text{circular_projection_of}(efp) + (efv)$$

where *efp* denotes the edge of the fingerprint image, *efv* denoted the edge of the finger vein image, and circular projection computes over 360-degree projection. As samples (A, B, C, D, E, F, Z) were tested, 26 classes were tested of the items by extracting the fingerprint from the testing operations. The traditional distance between the test samples and the items in the data set is calculated. Fifty samples of the items were tested, but other fingerprints were in different conditions from the one that was done. Record the samples in the collection base. Fifty samples of different varieties were tested.

The affiliation of the samples that are from the same classifications are recorded, but with different fingerprints taken to the original items, with a high accuracy rate of most samples, reaching 100%. The lack of affiliation with samples that are from varieties other than those registered in the system has also been recorded. Achieves the research path which is adopted in this research by calculating the Euclidean area, which is one of the efficient and easy methods that achieve the highest levels of balance between time and complexity.

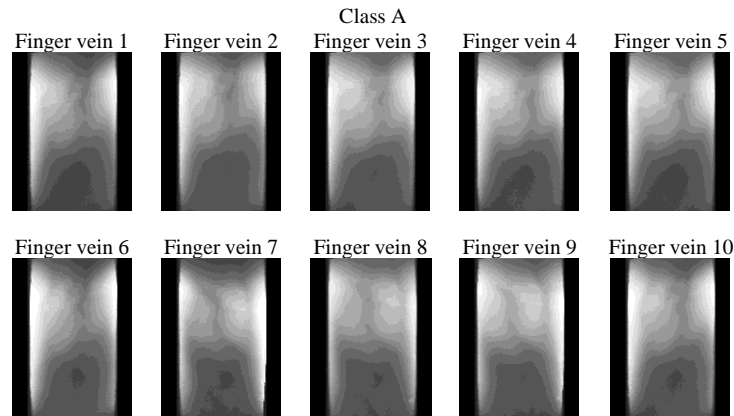


Figure 3. Sample of experimental results that demonstrate the image of finger vein of the first two classes as an example class A

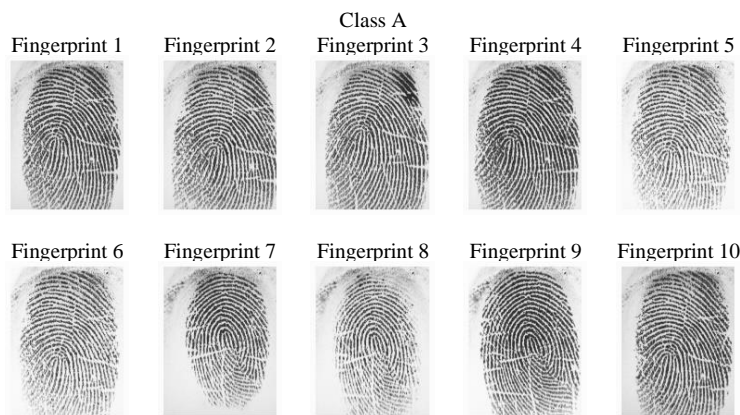


Figure 4. Samples of experimental results that demonstrate the image of fingerprints

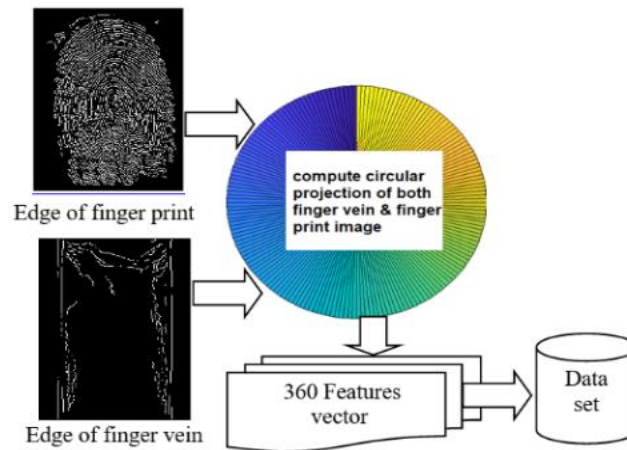


Figure 5. Block diagram for applying Canny edge detection of finger vein and fingerprint

5.3. Devises specification (fingerprint and finger vein scanner)

A special scanner is used to capture two different images at the same time. The first image is a fingerprint image, while the second image is a finger vein. We used a special scanner called (FPV10R) as shown in Figure 6. The output of this scanner is used to build real datasets, the first sub-data set for a finger vein and the second sub-data set for a fingerprint, as we explained before. These datasets are used in the experiment results to examine the proposed features, which in turn were used in the suggested validation system.



Figure 6. The FPV10R scanner

6. VERIFICATION OF SECURE E-DOCUMENT USING PROPOSED SYSTEM

The combination of features derived from different patterns of fingerprint image and vein image in this system has outperformed biometric systems that use only one biometric feature. This proves the forces of the multiple systems that address what unilateral systems cannot handle, such as reduced accuracy in the process of recognition, plagiarism, and non-discrimination, among other things that stand in the way of the use of individual features of biometric systems. In this work, we have ignored and supported the techniques and verses that depend on the details of the complex extract features related to the feature of fingerprint extraction as well as veins, each of which has a special structure of features that may not be compatible. We resorted to choosing the level of integration in the level of features chosen from both types to increase the level of security and the same high efficiency. We have suggested a fast and powerful calculation of the unique single directory using finger vein and fingerprint images. The method chosen is fast, robust, and secure and it can be used in both document authentication and Data integrity. In our proposed biometric system, various strategies have been envisaged, which depend on the combination of both the fingerprint image and the image of the vein of the same finger to create a strong, effective system of high speed and accuracy. Combining the fingerprint with the vein helped to solve the safety problem that plagued electronic documents. These strategies have relied on efficient and less sophisticated methods.

7. MATCHING AND MATCHING SCORE

Classification in our proposed system is used using the method of closest neighbors, which depends on measures of marital distance, as the classification of query points is done by measuring the distance from

the training data points and this is considered a simple and effective way to classify the new points to know the extent of their affiliation to the classes used for training. The distance scales used to find the distance between the data set and query points differ. It can use any of these methods to calculate closest neighbors (Euclidean distance, Cosine distance, Correlation distance, Hamming distance, Jaccard distance, and Spearman distance). As an example, Euclidean distance has been used in this paper. Given an $m \times n$ data matrix X , which is treated as m (1-by- n) row vectors x_1, x_2, \dots, x_m , and an $m \times n$ data matrix Y , which is treated as m (1-by- n) row vectors y_1, y_2, \dots, y_m .

8. CONCLUSION

This idea reliably replaces the multi-solution frameworks achieved in many businesses. For example, gives a more noteworthy diversity to precisely discovering the weaknesses of previous methods to address them in the proposed system. The performance of the recognition system in the proposed system is distinguished by extracting the important features of the fingerprint and linking it successfully to the veins of the same finger to extract unique and new features that are distinctive for this finger and used in a novel way in the proposed recognition system.

As a result of these research pursuits, one of the creative commitments of our work is the structure of general and time-efficient protection safeguarding arrangements and conventions which might be utilized with other biometric modalities, yet additionally, in different sorts of calculations where the security of the information is one of the principal concerns. Furthermore, we took a shot at different regular modalities that have diverse true applications. Accordingly, different arithmetic settings are adopted to process regular and safe biometric accounts, as computing in this field depends on two parties. The first party represents the basic database that contains the ideal characteristics of fingerprints and veins for authorized persons. While the second part represents the fingerprint on the document. It is meaning that each party their entries, and they will both work together to calculate a function and validate the document.

Our proposed system is characterized by its strength and the difficulty of its penetration, as it depends on both fingerprints and veins at the same time, which are considered to be biometric features, which are difficult to falsify and copy in the case of merging them, unlike other traditional methods that use identity cards and that suffer from the easy forgery and forgery of the existing signature it must obtain a false document. Therefore, it is necessary to think in a new way to find radical solutions to the issue of forgery and tampering with electronic documents.




REFERENCES

- [1] G. Thenmozhi, R. A. Jothi, and V. Palanisamy, "Comparative analysis of finger vein pattern feature extraction techniques an overview," *International Journal of Computer Sciences and Engineering*, vol. 7, no. 5, pp. 867–872, May 2019, doi: 10.26438/ijcse/v7i5.867872.
- [2] H. Patel, S. Desai, P. Desai, and A. Damani, "Review on offline signature recognition and verification techniques," *International Journal of Computer Applications*, vol. 179, no. 53, pp. 35–41, Jun. 2018, doi: 10.5120/ijca2018917233.
- [3] A. M. Ali and A. K. Farhan, "A novel improvement with an effective expansion to enhance the MD5 hash function for verification of a secure E-document," *IEEE Access*, vol. 8, pp. 80290–80304, 2020, doi: 10.1109/ACCESS.2020.2989050.
- [4] A. M. Ali and A. K. Farhan, "A new approach for expansion the throughput capacity of the quick response code," in *2019 First International Conference of Computer and Applied Sciences (CAS)*, Dec. 2019, pp. 226–231, doi: 10.1109/CAS47993.2019.9075492.
- [5] A. M. Ali and A. K. Farhan, "Enhancement of QR code capacity by encrypted lossless compression technology for verification of secure E-document," *IEEE Access*, vol. 8, pp. 27448–27458, 2020, doi: 10.1109/ACCESS.2020.2971779.
- [6] J. Blue, J. Condell, and T. Lunney, "A review of identity, identification and authentication," *International Journal for Information Security Research*, vol. 8, no. 2, pp. 794–804, 2018.
- [7] S. Daas, M. Boughazi, M. Sedhane, and B. Bouledjane, "A review of finger vein biometrics authentication system," in *2018 International Conference on Applied Smart Systems (ICASS)*, Nov. 2018, pp. 1–6, doi: 10.1109/ICASS.2018.8652005.
- [8] D. Hebri and V. Vasudeva, "Multimodal authentication of ocular biometric and finger vein verification in smartphones: a review," *International Journal of Engineering and Technology*, vol. 7, Jul. 2018, doi: 10.14419/ijet.v7i3.12.15909.
- [9] K. Shaheed, H. Liu, G. Yang, I. Qureshi, J. Gou, and Y. Yin, "A systematic review of finger vein recognition techniques," *Information*, vol. 9, no. 9, Aug. 2018, doi: 10.3390/info9090213.
- [10] K. Syazana-Itqan, A. R. Syafeeza, N. M. Saad, N. A. Hamid, and W. H. Bin Mohd Saad, "A review of finger-vein biometrics identification approaches," *Indian Journal of Science and Technology*, vol. 9, no. 32, Aug. 2016, doi: 10.17485/ijst/2016/v9i32/99276.
- [11] W. Kang, H. Liu, W. Luo, and F. Deng, "Study of a full-view 3D finger vein verification technique," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1175–1189, 2020, doi: 10.1109/TIFS.2019.2928507.
- [12] A. Kadhim and H. Emad, "Mouse movement with 3D chaotic logistic maps to generate random numbers," *Diyala Journal For Pure Science*, vol. 13, no. 3, pp. 24–39, Jul. 2017, doi: 10.24237/djps.1303.268B.
- [13] A. Roy and S. Karforma, "A survey on digital signatures and its applications," *Journal of Computer and Information Technology*, vol. 3, no. 1, pp. 45–69, 2012.
- [14] F. Alaa Kadhim, G. H. Abdul-Majeed, and R. S. Ali, "Enhancement CAST block algorithm to encrypt big data," in *2017 Annual Conference on New Trends in Information and Communications Technology Applications (NTICT)*, Mar. 2017, pp. 80–85, doi: 10.1109/NTICT.2017.7976119.




- [15] J. Lee *et al.*, "A finger-vein imaging and liveness detection for identity authentication using 2-axis MEMS scanner," in *International Conference on Optical MEMS and Nanophotonics*, Jul. 2016, pp. 1–2, doi: 10.1109/OMN.2016.7565871.
- [16] A. M. Ali, "Design a robust system for ratification and distinguish Fake documents using barcode technology," *Journal of The Iraqi University*, vol. 38, no. 3, pp. 695–707, 2017.
- [17] X. Zhang, D. Cheng, P. Jia, Y. Dai, and X. Xu, "An efficient android-based multimodal biometric authentication system with face and voice," *IEEE Access*, vol. 8, pp. 102757–102772, 2020, doi: 10.1109/ACCESS.2020.2999115.
- [18] S. P. Shrikhande and H. S. Fadewar, "Personal identification using local and global feature of finger vein patterns using SVM based classification," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 12, pp. 138–145, Dec. 2018, doi: 10.26438/ijcse/v6i12.138145.
- [19] E. Ting and M. Z. Ibrahim, "A review of finger vein recognition system," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 10, no. 1–9, pp. 167–171, 2018.
- [20] A. M. Al-juboori, W. Bu, X. Wu, and Q. Zhao, "Palm vein verification using multiple features and locality preserving projections," *The Scientific World Journal*, vol. 2014, pp. 1–11, 2014, doi: 10.1155/2014/246083.
- [21] W. M. Yang, Y. C. Li, and Q. M. Liao, "Fast and robust personal identification by fusion of finger vein and finger-knuckle-print images," *Applied Mechanics and Materials*, vol. 556–562, pp. 5085–5088, May 2014, doi: 10.4028/www.scientific.net/AMM.556-562.5085.
- [22] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "A fingerprint and finger-vein based cancelable multi-biometric system," *Pattern Recognition*, vol. 78, pp. 242–251, Jun. 2018, doi: 10.1016/j.patcog.2018.01.026.
- [23] V. M. Patel, R. Chellappa, D. Chandra, and B. Barbelo, "Continuous user authentication on mobile devices: recent progress and remaining challenges," *IEEE Signal Processing Magazine*, vol. 33, no. 4, pp. 49–61, Jul. 2016, doi: 10.1109/MSP.2016.2555335.
- [24] A. K. Farhan, R. S. Ali, H. Natiq, and N. M. G. Al-Saidi, "A new S-Box generation algorithm based on multistability behavior of a plasma perturbation model," *IEEE Access*, vol. 7, pp. 124914–124924, 2019, doi: 10.1109/ACCESS.2019.2938513.
- [25] Y. Cao, A. Shen, J. Xu, M. Qiao, and Y. Wang, "Calculation and accuracy analysis of center of gravity of payload rack," in *Proceedings of 2011 6th International Forum on Strategic Technology*, Aug. 2011, vol. 2, pp. 669–673, doi: 10.1109/IFOST.2011.6021114.

BIOGRAPHIES OF AUTHORS



Ammar Mohammed Ali    received a bachelor's degree in computer science from the University of Technology, Baghdad, and received an M.S. degree in computer science (computer programming) from Harbin Engineering University, China, in 2012 and he is now a Ph.D. student (data security) in computer science from University of Technology, Baghdad. His research interest includes privacy, security, biometric techniques, image processing, and pattern recognition applications. He can be contacted at ammar.m.ali@uotechnology.edu.iq.



Alaa Kadhim Farhan    received the bachelor's degree in computer science and the M.Sc. degree in information security from the Department of Computer Science, University of Technology, Baghdad, in 2003 and 2005, respectively, and the Ph.D. degree in information security from the University of Technology, in 2009. He is an assistant professor at the Department of Computer Science, University of Technology. In 2005, he joined the Department of Computer Science, University of Technology, as an Academic Staff Member. He has been the author of numerous technical articles, since 2008. His research interests include cryptography, programming languages, chaos theory, and cloud computing. He can be contacted at dralaa_cs@yahoo.com.