Generating SSI Decentralized Identifiers Through Hand Vein Patterns

GIANLUCA LAX, ROSARIO MORELLO
University of Reggio Calabria,
Via dell'Università, 25, Reggio Calabria, 89124
ITALY

Abstract: Self-Sovereign Identity (SSI) provides individuals with the ability to control how their data are managed. In this model, individuals are identified by Decentralized Identifiers (DIDs) that are derived from a secret information. Consequently, compromising this secret allows an attacker to impersonate the victim. In this paper, we propose a novel strategy for generating DIDs leveraging hand vein patterns as the source of identity. We focus on using thermal imaging for contactless, hygienic, and liveness-guaranteed acquisition of hand and vein patterns. To ensure the generation of a stable DID despite minor, unavoidable variations in biometric acquisition, we incorporate fuzzy extractors. This mechanism guarantees that feature variations below a specified threshold result in the same consistent cryptographic key from which the DID is derived. Furthermore, our proposal supports the SSI Pseudonymity Principle by allowing individuals to generate multiple distinct DIDs to counter tracking across different contexts.

Key-Words: Biometrics, FLIR, Fuzzy Extractors, Pseudonymity, Self-Sovereign Identity, Thermal Imaging.

Received: April 23, 2025. Revised: September 21, 2025. Accepted: October 18, 2025. Published: June 16, 2026.

1 Introduction

In computer science, authentication is the mechanism used to verify the identity of a user who requests access to a resource. It is based on factors such as something the user knows, possesses, or is. The latter type, known as *biometrics*, is considered one of the most secure and effective methods because users do not have to remember or carry anything with them, [1]. Alongside fingerprint, facial, and iris recognition, in recent years, thanks to the use of thermography, other body parts that exhibit unique characteristics have been studied, [2].

In this work, we focus on the use of images of hands and hand vein patterns acquired by thermal imaging as a biometric technique for individual recognition. This technique offers several advantages. Since veins are an internal characteristic, they are difficult to steal or replicate. Furthermore, this solution guarantees user *liveness*, as authentication only works if there is blood in circulation. Finally, this approach is very hygienic because it does not require any type of contact (unlike fingerprint recognition).

The hands have the characteristics necessary to be usable for authentication, [3], which are:

1. *Universality*: they are possessed by every person;
2. *Permanence*: they are sufficiently invariant over a long period of time;
3. *Distinctiveness*: they are sufficiently different between two individuals;
4. *Collectibility*: they are quantitatively measurable.

The first two characteristics are easily verifiable (except in rare but identifiable cases, such as hand amputation). Regarding distinctiveness, it is conceivable that it derives from the same phenomenon observed for fingerprints and irises, which occupy a significantly smaller surface area. However, providing a formal proof of this characteristic would require experimentation on a very large number of individuals (and this is beyond the scope of this paper). The characteristic of collectibility is discussed extensively in the paper.

Authentication is closely related to the well-known concept of digital identity and the probably lesser-known concept of Self-Sovereign Identity, [4]. Self-Sovereign Identity (SSI) is a recent implementation of a new model of digital identity that aims to give users the ability to decide what personal information to share and with whom. This solution is decentralized, as it eliminates the need for a centralized third party. It relies on technologies such as DLT (Distributed Ledger Technologies), [5], along with verifiable credentials, to ensure that only strictly necessary data are shared securely and privately. In this model, a user is identified by a Decentralized Identifier (DID), which is registered by the user without the need for a central authority. Usually, the DID is generated from a pair of cryptographic keys that are known only to the user, [6]. However, if this

secret is violated, an attacker can impersonate the user.

One contribution of this research is to propose a strategy to generate the DID directly from the biometric trait, ensuring a strong link between the DID and the user to whom it refers. Since the DID is derived from the features extracted from the user, no secret information is necessary, and an attacker cannot break the association between the user and their DID. Moreover, the proposal allows a user to generate more DIDs in such a way that the SSI Pseudonymity Principle is preserved, [7].

The remainder of this paper is structured as follows. Section 2 details our proposed methodology for biometric authentication carried out using hand vein patterns extracted by thermal images. Section 3 introduces the model of SSI and defines the proposed technique to generate DIDs from biometric features. Finally, Section 4 concludes the paper.

2 Authentication by vein patterns

Thermography is a non-invasive technique that, starting from the measurement of the infrared radiation emitted by a body, is able to compute the corresponding surface temperature, [8]. The equipment used in thermography, known as a thermal imaging camera, can detect the thermal energy radiated by any body that has a temperature above absolute zero with an accuracy of nearly a hundredth of a degree. From an analysis of the temperature distribution of the different objects in the captured scene, it is possible to reconstruct the shape of any object into an image. The application of thermography on the human body is supported by the fact that it is a non-invasive and harmless technique. This technique is widely used in the medical field for endocrinology, neurology, orthopedics, traumatology, and many other specialties. Furthermore, because the surface temperature of the skin is highly dependent on the blood flow in the underlying vessels and the homeostatic processes of the organism, it can be used in many applications to study a person's psychological and emotional state or for lie detection, [9].

The acquisition of thermograph images of the hands has been proposed for biometric authentication. Besides the geometry of the hand, vein patterns are also considered to enhance security. Indeed, the shape of the veins in the fingers, palms, or wrists are distinctive characteristics of the individual, which are different for each subject, [10]. Moreover, this type of biometric authentication guarantees that the subject is a real individual who is alive, since it is based on blood perfusion.

The vein-pattern-based authentication system that is proposed involves five phases:

1. *Acquisition.* This procedure consists of placing the hand in front of the thermal imaging camera, which captures the image. The image acquisition step is crucial because the higher the image quality, the fewer errors will be made during the later steps. The system uses the concept of absorption of deoxyhemoglobin relative to hemoglobin through infrared rays.

2. *Image enhancement*. In this phase, a suitable filter is applied to enhance image contrast and to detect the vein profile.

3. *Segmentation*. The image is partitioned to extract a smaller and more specific area to be used for vein feature extraction.

4. *Feature extraction*. Through measurements relating to the geometry of the hand and the associated veins, the characteristics of the vein pattern are extracted to authenticate the individual.

5. *Classification*. By suitably comparing the characteristics obtained from two different acquisitions, it is possible to verify whether the vein features come from the same individual.

In the following, such phases will be carefully described by applying the authentication system to a case study.

2.1 Acquisition

For the acquisition, a Flir X8400sc thermal camera was used. It is a high-sensitivity thermal camera produced by FLIR Teledyne Systems, having an advanced Indium Antimonide cold sensor. The detector allows for the generation of thermographic images at 1280 x 1024 pixels resolution and can detect temperature differences of less than 18 mK.

FLIR ResearchIR software has been used to acquire and process thermographic records. The recording options have allowed us to set the relative start and end times and the number of frames to be captured. In detail, since the main vessels cross the back surface of the hand, a case study was considered to apply the proposed model. Figure 1 reports an example of a hand image captured by the thermal imaging camera.

2.2 Image enhancement

The next step concerns the analysis of the images in order to enhance the contrast of the dorsal venous network. To this aim, the tools provided by the ResearchIR software were used to verify

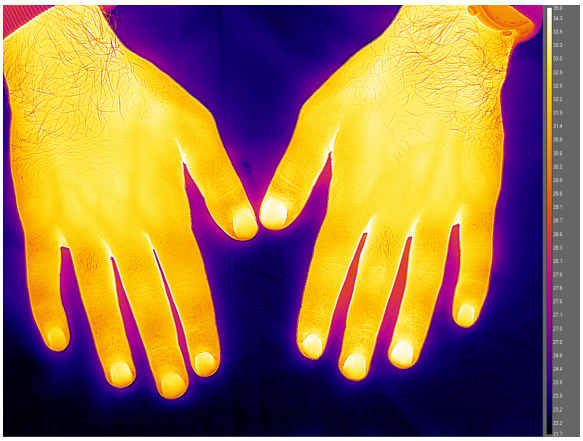

Fig. 1: An example of the initial image captured by the thermal imaging camera during the acquisition phase. *Source: created by the authors.*

which configuration allowed to increase the color shade difference between the vein patterns and the skin. Several experiments were carried out using different configurations. Regarding the position of the hand, both the extended hand and the closed fist configurations have been considered. Two types of thermal stress were used.

The first thermal stress is performed by an *IR lamp*, which is a common infrared (IR) lamp used as a thermal stimulus to induce a thermoregulatory process. The lamp emits light in the range of the infrared electromagnetic spectrum, which is not visible to the human eye. This lamp has been exploited for its ability to generate heat through the emission of infrared rays without contraindications for humans (in fact, they are commonly used in different contexts, including biomedical ones).

The second thermal stress is an *NIR lamp*, which emits light in the part of the electromagnetic spectrum known as Near Infrared (NIR) with wavelengths slightly longer than visible light, but shorter than the traditional infrared one. This lamp has been chosen because it is often used in medical applications.

The configuration that provided the greatest enhancement of the vein patterns was the one with the hand extended and using an IR lamp. The *Fusion2 palette* was used to generate the thermographic image. This palette attributes different colors, from black to white, to different temperature ranges in order to increase contrast and enhance heat variations within the region of interest. This palette overlays thermographic information with visual images, assigning different shades of thermal colors to temperature changes, maintaining the visual structure of the image, and providing a simultaneous view of thermal and visual information.

The *Adaptive Process Enhancement*(APE) scale was used to increase the image contrast. It optimizes the thermal image according to environmental variations, thus improving the color shade. Figure 2 reports an example of this processing phase applied to Figure 1, where the vein pattern appears to be well highlighted.

Fig. 2: An example of the thermographic image (from Figure 1) after applying the Fusion2 palette and Adaptive Process Enhancements scale, highlighting the vein patterns. *Source: created by the authors.*

2.3 Segmentation

To extract the vein pattern features from the thermographic images of both hands, appropriate Regions of Interest (ROI) have been considered. The proposed authentication biometric model is based on the geometric measurements of the hand and on the individual vein pattern detection.

In order to extract the features of the veins, the centroid of the back of the hand must be detected. It is the *average position* of all its points (i.e., the geometric center of the hand). A distance mapping method is applied to find the centroid. The Euclidean distance between the centroid and the contours of the hand (the so-called radial distance or radius) is calculated by Equation 1:

$$D_{ki} = \sqrt{(Q^x - P_i^x)^2 + (Q^y - P_i^y)^2} \qquad (1)$$

where:

- D_{ki} is the Euclidean distance (or radial distance) from the centroid to the i-th point of the hand outline,
- Q^x and Q^y are the coordinates of the hand centroid (the geometric center of the hand),
- P_i is the i-th point of the hand outline, and

- P_i^x and P_i^y are the coordinates of the i-th point of the hand outline.

2.4 Feature extraction

Once the centroid has been identified, the square and the respective inscribed circumference are delineated in order to measure the hand dimensions. Subsequently, each vein is represented by a line to measure its length using the number of pixels.

In detail, to evaluate the distance in terms of millimeters, the IFOV (Instantaneous Field of View) of the thermal camera is calculated, which is the angular projection of a single pixel. The area associated with a pixel depends on the distance between the lens and the object. It is possible to compute this value by converting the angular aperture of the used lens into radians and dividing the two values by the number of pixels present in the image. This result returns the IFOV, expressed in millimeters, for a distance of one meter, which can then be related to the current distance of the target from the lens.

In the analyzed case, the used lens is 50 mm and has an angular aperture of 22° x 17°, as defined by FLIR specifications. The image resolution is 1280x1024 pixels, whereas the distance of the hand from the lens is 0.79 meters. Consequently, each pixel has a spatial length of approximately 0.23 mm.

Figure 3 shows an example of ROIs used to measure the biometric features of the vein patterns for both hands. Table 1 reports some examples of extracted features (specifically, the length in pixels and millimeters of some of the veins detected in Figure 2).

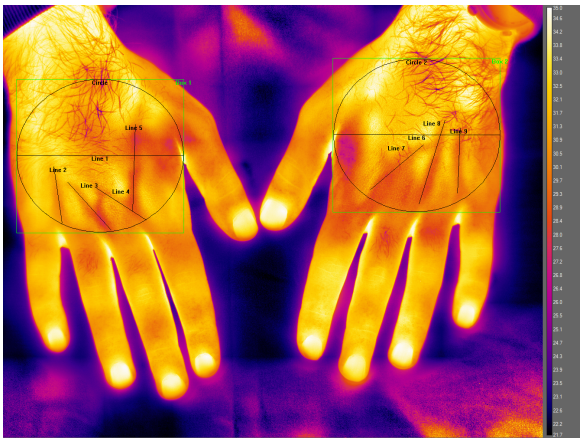

Fig. 3: An example showing the regions of interest and guide lines used to measure the biometric features on the enhanced thermal image. *Source: created by the authors.*

Table 1: This table reports examples of the measured length, expressed in pixels and millimeters (mm), of detected veins for both the hands. *Source: created by the authors.*

Right Hand			Left Hand		
ROI	**pixels**	**mm**	**ROI**	**pixels**	**mm**
Line 1	396	91.08	Line 6	397	91.31
Line 2	135	31.05	Line 7	126	28.98
Line 3	115	26.45	Line 8	200	46.00
Line 4	118	27.14	Line 9	155	35.65
Line 5	206	47.38			

2.5 Classification

In this phase, a template (composed of the hand image and its vein pattern) is matched against a stored template to verify whether both belong to the same user. Vein patterns can be compared using distance metrics applied to their geometric features (lines and numbers). For the image, the same approach used for face detection and other recognition techniques can be used. One of the most promising methods is based on the use of Principal Component Analysis (PCA), [11], which reduces the feature dimension of the hand image. After being trained on a large dataset of different hands, PCA can detect the most relevant components, which are the parts of the image that show the most significant variations across the images. A new hand image is represented as a linear combination of these components, and the comparison between these linear combinations is used for classification. Obviously, since each acquisition differs slightly from other acquisitions of the same individual, a suitable threshold of the maximum difference should be found.

Performing this task is beyond the scope of this paper because it would require the use of thousands of hand images to determine both the most relevant components and the threshold. However, since this approach has been successfully adopted for the recognition of other parts of the body, we expect that good results can also be reached in this case.

3 DID Generation

In this section, we define the procedure that is carried out to generate a Decentralized Identifier for SSI, leveraging vein patterns. We start by introducing the model of SSI.

3.1 Self-Sovereign Identity

SSI is a new form of digital identity that allows individuals to control what personal data they disclose and with whom they share them. To eliminate the need for a centralized intermediary, it relies

on blockchain, a distributed ledger that guarantees transparency and immutability, [4].

In SSI, a Decentralized Identifier (DID) is an alphanumeric string uniquely associated with an individual (called a *Prover*). Typically, the Prover generates a pair of cryptographic keys, which are called *public* and *private* keys. The DID is generated from the public one, typically by applying a cryptographic hash function, [12].

When the Prover needs certification of the possession of some attribute (e.g., a driver's license), a request to a suitable *Issuer* is made. The Issuer, after verifying the possession of this attribute and that the Prover knows the key pair from which the DID is derived, generates and signs a digital document called *Verifiable Credential* (VC). A VC certifies the possession of an attribute and associates it with the DID that requested it. This VC is sent back to the Prover.

When the Prover needs to demonstrate the possession of this attribute to a *Verifier*, they present the VC (which contains the DID) and prove the knowledge of the key pair from which the DID is derived.

In this procedure, the DID is associated with the key pair used for its generation, and compromising the secrecy of the private key would allow an attacker to impersonate the Prover. To avoid this possibility, we define a schema to derive the DID from the biometric features extracted by thermal hand images.

3.2 From patterns to DID

Following the procedure described in Section 2.4, we extract the features used for biometric authentication. However, these features cannot serve the same role as the public key in the generation of the DID. Indeed, each extraction produces slightly different features, and these cannot be used as a basis to calculate the DID because each authentication would generate a different DID.

To solve this problem, we propose the use of *fuzzy extractors*, [13]. Briefly speaking, a fuzzy extractor is composed of two functions (*Generate* and *Reproduce*) and essentially works as a hash function that returns the same value for all inputs that differ less than a given threshold.

In our scheme, let FE^P be the features extracted from the prover P. Based on the procedure described in Section 2.5, we can calculate the maximum distance that two extracted features must be within to be considered belonging to the same individual. Let d be such a distance.

When the features are acquired from the hand of P, and after FE^P is computed, the generation is performed as shown in Equation 2:

$$(K, H) = Gen(FE^P, d) \tag{2}$$

where the function Gen is a fuzzy extractor that receives the template of the features and the threshold d and returns a key K (a value that remains constant under slight variations of the input) and *helper* data H (used to detect and correct small changes in the input).

The DID associated with the Prover P is obtained according to Equation 3:

$$DID^P = HF(K) \tag{3}$$

where HF is a cryptographic hash function, [12], and K is the unique key generated from the Prover's hand vein features by the fuzzy extractor's function Gen.

The DID generated in this way is derived from the features retrieved from the Prover P, and this association cannot be broken by compromising a secret (as is the case when the DID is derived from a private key).

3.3 DID Registration

The crucial step for integrating the biometric subsystem with the Self-Sovereign Identity framework is the registration of the generated DID onto a blockchain. This process ensures the immutability and global discoverability of the Prover's identifier.

After DID^P is generated, P creates a DID Document, a structured data object that describes how to interact with the DID. The DID Document is linked to DID^P and is then anchored to the chosen blockchain. This step makes DID^P universally resolvable, which means that any Verifier can retrieve the associated information and metadata necessary for the authentication processes.

Moreover, P must store in a personal wallet the helper data H, which is the piece of public information required to successfully run the fuzzy extractor's function `Res` for every authentication attempt.

This procedure guarantees that the resultant DID^P is strongly linked to the Prover's unique physiological characteristic (the hand vein pattern) and eliminates the dependency on a traditional secret key. The blockchain provides the tamper-proof public registry required by the SSI model, while the fuzzy extractor ensures that this registration process is reliable despite the inherent noise of biometric data.

3.4 DID verification

When the Prover needs to use their SSI to access a resource of the Verifier, the Verifier acquires the thermal image of the prover's hand and the helper H from the Prover wallet. Now, the Verifier computes $K' = Res(FE', H)$ and $DID' = HF(K')$, where

K' is the reconstructed key, FE' is the features extracted during the current authentication attempt by the Verifier, Res is the fuzzy extractor's Reproduce function, H is the helper value generated during the initial DID creation and extracted from P's wallet, which assists in reconstructing the key, and DID' is the newly computed Decentralized Identifier obtained by applying the cryptographic hash function HF on the reconstructed key K'.

If the new features FE' are close enough (differ less than the threshold d) to the original features FE^P, then K' will equal the original key K and $DID' = DID^P$, thus returning the initial DID of the prover P.

Finally, the Verifier can resolve the DID using the blockchain and obtain the DID document, thus concluding the procedure.

3.5 DID regeneration

If the same DID is used in different contexts, each Verifier will know that it is interacting with the same Prover, which may violate the SSI Pseudonymity Principle, [7]. For this reason, the Prover should have the possibility of regenerating DIDs.

In our case, this is done by repeating the hand image acquisition task or by using a different frame if a video, instead of only a single image, was acquired. Indeed, as previously observed, biometric measurements are always imperfect due to variations in blood pulse, rotation, lighting, and positioning. Even a single pixel variation in FE^P is enough to obtain a completely different key after the execution of the Generate function.

4 Conclusion

This paper addresses a challenge inherent in the reliance on a cryptographic secret for generating the Decentralized Identifier (DID) in a Self-Sovereign Identity framework. If this secret is compromised, the associated identity is compromised, enabling impersonation. Our core contribution is the design and proposal of a schema in which the DID is generated directly from the hand vein pattern captured via thermal imaging.

The proposed methodology integrates two modules. The first module acquires the thermal hand image and extracts suitable biometric features (geometric measurements and anatomical properties), thereby establishing a strong link between the individual and their extracted features. Since extracted features are inherently noisy and variable, the second module exploits a fuzzy extractor to generate a unique key (K) from inputs (FEP) that are slightly different, provided the variation remains within a pre-defined threshold (d). The DID is derived from K by a cryptographic hash, which ensures that it remains constant for the same individual across multiple, slightly varying authentication attempts.

In this way, the decentralized identity is tied to the physical body of the individual, thus eliminating the need for a private key. Furthermore, by allowing the Prover to simply re-acquire a thermal image (e.g., a different frame from a video stream), the system allows for the regeneration of distinct DIDs. This feature is necessary to implement the SSI Pseudonymity Principle, preventing attackers from tracking the individual's activities across different interaction contexts.

However, the use of fuzzy extractors introduces new security concerns tied to the nature of biometrics. If an attacker can successfully mimic or replicate the biometric patterns (e.g., creating a synthetic hand with the victim's vein pattern), the system will generate the correct key (K) and allow impersonation, regardless of the fuzzy extractor's cryptographic strength. The proposed system counters this somewhat by using thermal imaging, which guarantees user liveness because authentication requires blood circulation.

Although the conceptual framework is well-defined, a limitation of this research concerns the tuning of its parameters. Specifically, the most important parameter to set is the threshold d measuring the maximum distance between two feature sets of the same individual. As already discussed, establishing this threshold requires extensive experimentation on a large and diverse dataset of hand images. Addressing this threshold determination remains a key avenue for future research.

References:

[1] C.-W. Lien and S. Vhaduri, "Challenges and opportunities of biometric user authentication in the age of IoT: A survey," *ACM Computing Surveys*, vol. 56, no. 1, pp. 1–37, 2023. DOI: 10.1145/3603705. URL: https://doi.org/10.1145/3603705

[2] S. Minaee, A. Abdolrashidi, H. Su, M. Bennamoun, and D. Zhang, "Biometrics recognition using deep learning: A survey," *Artificial Intelligence Review*, vol. 56, no. 8, pp. 8647–8695, 2023. DOI: 10.1007/s10462-022-10237-x. URL: https://doi.org/10.1007/s10462-022-10237-x

[3] P. S. Biswas and S. D. Mishra, "An assessment of biometrics tools: Fingerprint and knuckle crease patterns," in *Fostering Multidisciplinary Research for Sustainability*, Allied Publishers, 2024, p. 145. ISBN: 978-93-89934-77-9.

URL: https://books.google.gr/books?hl=el&lr=&id=2owDEQAAQBAJ&oi=fnd&pg=PA145&dq=.+S.+Biswas+and+S.+D.+Mishra,+%E2%80%9CAn+assessment+of+biometrics+tools:+Fingerprint+and+knuckle+crease+patterns,%E2%80%9D+in+Fostering+Multidisciplinary+Research+for+Sustainability,+Allied+Publishers,+2024,+p.+145.+ISBN:+978-93-89934-77-9.&ots=LOe2mMrH7l&sig=8IY_guY0kp6TRgPwL4RAozKo7gk&redir_esc=y#v=onepage&q&f=false [Access Date: 01/01/2026]

[4] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103 059–103 079, 2019. DOI: 10.1109/ACCESS.2019.2931173. URL: https://doi.org/10.1109/ACCESS.2019.2931173

[5] S. G. Savadatti, S. Krishnamoorthy, and R. Delhibabu, "Survey of distributed ledger technology (DLT) for secure and scalable computing," *IEEE Access*, vol. 13, pp. 8393-8415, 2025. DOI: 10.1109/ACCESS.2025.3528211. URL: https://doi.org/10.1109/ACCESS.2025.3528211

[6] I. Ahmed, K. Toyoda, T. Nakano, S. Kasahara, S. R. Goyal, and T. H. Tran, "A systematic review on blockchain-enabled eKYC: Leveraging SSI and DID for secure and efficient identity verification," *IEEE Internet of Things Journal*, vol. 12, no. 21, pp. 44381-44401, 2025. DOI: 10.1109/JIOT.2025.3597356. URL: https://doi.org/10.1109/JIOT.2025.3597356

[7] G. De Mulder and B. De Meester, "Pseudonymity for personal data stores: Pseudonymous webids and decentralized identifiers," in *International Conference on Availability, Reliability and Security (ARES 2024)*. Springer, 2024, pp. 111–129. DOI: 10.1007/978-3-032-00639-4_7. URL: https://doi.org/10.1007/978-3-032-00639-4_7

[8] M. F. A. Abuhussein, A. Darwish, and A. E. Hassanien, "Exploring thermography technology: a comprehensive facial dataset for face detection, recognition, and emotion," *arXiv preprint arXiv:2407.09494*, 2024. DOI: 10.48550/arXiv.2407.09494. URL: https://doi.org/10.48550/arXiv.2407.09494

[9] F. Fardian, M. Mawarpury, K. Munadi, and F. Arnia, "Thermography for emotion recognition using deep learning in academic settings: A review," *IEEE Access*, vol. 10, pp. 96 476–96 491, 2022. DOI: 10.1109/ACCESS.2022.3199736. URL: https://doi.org/10.1109/ACCESS.2022.3199736

[10] R. V. Adiraju, K. K. Masanipalli, T. D. Reddy, R. Pedapalli, S. Chundru, and A. K. Panigrahy, "An extensive survey on finger and palm vein recognition system," *Materials Today: Proceedings*, vol. 45, no. 2, pp. 1804–1808, 2021. DOI: 10.1016/j.matpr.2020.08.742. URL: https://doi.org/10.1016/j.matpr.2020.08.742

[11] P. Peng, I. Portugal, P. Alencar, and D. Cowan, "A face recognition software framework based on principal component analysis," *PLOS ONE*, vol. 16, no. 7, p. e0254965, 2021. DOI: 10.1371/journal.pone.0254965. URL: https://doi.org/10.1371/journal.pone.0254965

[12] S. Windarta, S. Suryadi, K. Ramli, B. Pranggono, and T. S. Gunawan, "Lightweight cryptographic hash functions: Design trends, comparative study, and future directions," *IEEE Access*, vol. 10, pp. 82 272–82 294, 2022. DOI: 10.1109/ACCESS.2022.3195572. URL: https://doi.org/10.1109/ACCESS.2022.3195572

[13] Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," in *International conference on the theory and applications of cryptographic techniques*. Springer, 2004, vol. 3027, pp. 523–540. DOI: 10.1007/978-3-540-24676-3_31. URL: https://doi.org/10.1007/978-3-540-24676-3_31

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

Gianluca Lax was responsible for the design and validation of the DID generation from vein patterns. Rosario Morello was responsible for the design, implementation, and experimentation of the vein pattern authentication. Both authors discussed the results and contributed to the final manuscript.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

This work was partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU.

Conflicts of Interest

The authors do not have any conflict of interest.