International Transactions on Electrical Engineering and Computer Science
Arshita, Vol: 2, No: 3, pp: 118-127, Sep 2023

Implementation of the Optimized Dual Fingerprint Algorithm for Protecting Privacy Information

D. Ashritha Reddy*

Abstract: The electromagnetic spectrum (EM) is made up of a variety of wavelengths, but the only wavelength that can be seen by the human visual system (HVS) is the visible wavelength, which is also referred to as the digital image processing (DIP) wavelength. The visible wavelength is also known as the visible light spectrum (VLS). The DIP is a component of the signal processing, but the HVS is unable to see the other elements of the signal if the DIP is not there. This is because the HVS requires a digital screen in order to see them, which is an application of the DIP. Through the implementation of digitalization applications in a variety of study domains, the DIP transforms the current world into a center for technological innovation. In today's society, security is of the highest importance, and biometrics-based systems have gained appeal over conventional ones because to their simplicity of use, resilience, and accuracy. Biometrics-based systems are becoming more popular. In this research, a unique combinational manner-based security solution is provided by combining the two fingerprints and taking into account their distinct orientations and minute details. This approach is made possible by taking into mind the minutiae involved. The creation of a fingerprint template that is identical to the original fingerprint included taking elements from two separate fingerprints and combining them. The information is protected against theft using the suggested template, which also demonstrates a low error rate (FRR = 0.4% at FAR = 0.1%) when compared to conventional methods (FAR = 0.1%). In conclusion, as compared to traditional approaches, the suggested method possesses a superior virtual identity, which demonstrates positive outcomes when defending against incidental and inadvertent attacks.

Keywords: Digital image processing, Fingerprint, Biometric, Minutia

1. Introduction

The phrase "digital image processing" refers to both the process of acquiring digital content (Object) via the use of a digital sensor and the process of seeing the obtained digital material on a digital screen.

Article History
Received: 18-06-2023; Revised: 27-07-2023;
Accepted: 15-08-2023

*Corresponding author: Department of Data Analytics and visualization, Yeshiva University, 245 Lexington avenue, New York

E-Mail: dreddyashu@gmail.com

The use of digital image processing in research domains include medical, security, satellite imagery, computer vision, military, transportation, genetics, sonar applications, and so on. It has implemented the digitization process so that users may see digital material in an appealing way [1]. Not only have the discoveries and technological advancements of science revolutionized the world, but they have also turned the 21st century into the "era of technology." In addition, the security domain has evolved into an essential component of any program in order to provide an appropriate degree of protection for the data. This is due to the fact that the world has been altered as a result of many inventions and technological advances [2].

The advent of digitalization and the use of techniques like as cryptography, steganography, and watermarking have changed some aspects of modern security standards, which has made it possible for the field of security to go to the next level. The convergence of digitalization and the internet has resulted in ground-breaking shifts in the security standards, and the secure transmission of data has been an area of research for many years. However, further in-depth study is necessary to make it hacker-proof and attack-proof before it can be implemented. In today's world, the usage of digital pictures has soared, and its presence can be seen in a variety of well-known academic fields, such as robotics, medicine, genetics, satellite image processing, security, computer vision, and many more [3-4]. This presence can be observed in a number of well-known academic fields. This is due to the fact that digital images are easier to manipulate than their analog counterparts. The defects that are linked with the transmission of digital photographs through the internet have also expanded in an unfathomable way owing to the proliferation of the practice, which has occurred for a variety of reasons.

In this paper, a comparison is made between two different methods that were developed to safeguard the confidentiality of fingerprints. The first is an innovative approach to the problem of protecting an individual's fingerprint secrecy by merging aspects of two distinct fingerprints in order to create a new uniqueness [5]. During the registration practice, the system takes an imprint of both the user's left and right thumbs. The new identification includes certain minute details that are found on the right thumb, and it has an imprint that is oriented toward the left thumb. The subsequent method is a process that syndicates the minute details of two distinct fingerprints belonging to the same individual. The new identification will ensure that even the most minute details of each fingerprint are preserved. Filtering of the system's most minute details is carried out in order to boost both its efficiency and its precision [6]. In the last step, a comparison is made between the performance of all methods in terms of FRR, ERR, and FAR. This study employs the same methods for the pre-processing and post-processing of fingerprint descriptions. This is done so that the presentation of two dissimilar ways may be matched.

2. Literature review

2.1 Importance of Biometrics

In the 21st century, safety has become the primary focus of worry, and in order to give effective answers to the challenges associated with security, the amount of time spent researching biometrics has tripled over the course of the previous several years. The number of apps that are connected to the internet in this day and age has significantly expanded, and the primary challenge that is associated with online applications is producing authentication from a distant place, which produces a security chain. In conventional systems, the employment of passwords and tokens-both of which are vulnerable to being guessed or stolen-has been standard practice [7]. The use of biometrics for authentication and related identification of relevant entities has extended significant popularity in modern years as a means of overcoming the disadvantages associated with conventional algorithmic approaches.

2.2 What is biometric?

The field of study known as biometrics is primarily focused on the development of technologies that may give enhanced levels of safety by taking into consideration the psychological traits of an individual. In order to identify each user and verify their information in a trustworthy manner, the unique qualities of the users who have been taken into account are utilised. The user information may be identified in a dependable and effective manner using the fingerprint biometric appliance, which is the biometric instrument that is utilized the most all over the globe, including in university, companies, and laboratories, among other places. The simplicity of the fingerprint biometric mechanism is one of the primary reasons why it is the most often used [8]. One may simply construct a fingerprint biometric mechanism by keeping into consideration certain factors, most notably miniaturization. After years of intensive study on microscopic features, mostly ridges and valleys, several fingerprint algorithms were developed. The conclusions and divergences of the authority lines in a exclusive finger imprint image are the maximum common way in which particulars are presented. Edge finishing and edge bifurcation exceptional are the two aspects of particulars that are considered to be the most important neighborhood edge features. Edge

closure is the moment at which the edge abruptly shuts, and it is referred to by that word. The place at which an edge splits off into two or more branch edges is referred to as the edge's bifurcation point. The general structure of a one-of-a-kind mark verification framework is divisible, for the most part, into two distinct portions. Information based on a person's biometric characteristics, such as their fingerprints or iris scans, is gradually replacing security systems that rely on secret keys for authentication and identification purposes. Differentiating evidence from confirmation involves referring to two unique tasks, which are as follows: determining the personality of a man based on his biometric information, as opposed to confirming the personality based on his biometric evidence and the alleged behavior.

2.3 Overview of the Proposed Approach

In this study, we propose an enhanced fingerprint approach for providing exact privacy protection for the data at hand. Many theoretical studies and algorithms based on a single fingerprint have been offered in the past, which generally lacks secrecy and privacy [8]. Furthermore, methods relying on a single fingerprint technique fail to protect verified fingerprints in the database, and data may be readily destroyed as a consequence of unintentional or accidental hacking. The following is a summary of the approach's critical stages dedicated to description and debate:

- The initial stage is fingerprint enrollment, followed by the certified system collecting the two dissimilar related fingerprints from the two fingerprints that were registered.
- A revolutionary approach known as the "combined minutiae template generation algorithm," which aids in the construction of a template from the two independent fingerprints to give enhanced secrecy defense.
- At this period, important data is examined, which aids in the creation of a template. Furthermore, the necessary information is derived from two further fingerprint characteristics: minutiae locations and minutiae orientations.
- In this technique, the minute locations from one fingerprint and the minute directions from a second fingerprint, as well as alternative coding systems, are considered. This is done in parallel.
- The database stores the Fingerprint look similar template created for authentication reasons.
- In this study, an enhanced matching approach was used, which boosted the correctness of the corresponding query among the two independent fingerprints and the created pattern.
- The proposed work seeks to safeguard data from incidental or inadvertent assaults by developing an appropriate outline for record validation. Theft of a single template does not expose all information, and an unauthenticated user may be exploited by constructing a true fingerprint look alike template, which is the result of combining two separate fingerprints.
- Lastly, the mutual minutiae pattern creation technique provides the secured fingerprint alike template. The proposed strategy exhibits a lower false acceptance rate (FAR) and a lower false rejection rate (FRR) when compared to standard fingerprint techniques.

2.4 The advantages of proposed algorithm

- The high error rate in biometrics, in addition to the complicated nature that exists in each of the potential circumstances, is the primary reason of the safety breach of personal information in this industry. In recent years, there has been a lot of curiosity shown in the protection of privacy offered by biometrics, especially the fingerprint identification method. This is because biometrics may be used to verify the identity of a customer. This is partly due to the reality that, because of the computational approaches it employs, it is easy as well as complicated all at the same time.
- The suggested technique has been efficient at satisfying the practical needs such as the preservation of privacy in comparison to the traditional functions suggested in the research literature. This has been accomplished by substantially lowering the rate of mistakes FRR= 0.4% and FAR=0.1% correspondingly, which is 80% higher when contrasted to the methods that use a single scale fingerprint. Other practical necessities that have been met include the security of confidentiality.
- The fingerprint biometric mechanism has been split into two categories, named the feature level

and the image level, according to their respective features, as stated in the research literature. These categories are the feature level and the image level. The user's privacy is not better protected by either strategy, and the data that is utilized in either way is more susceptible to being stolen. Neither approach is successful. The proposed work would build a combined minutiae template that has the same appearance as the original fingerprint template. This will make it difficult for authorized users to tell the difference between the original and the combined template.

- Later the image level investigation in the step beyond, the second technique, which is known as image level approaches and was explained previously in the step above, fails to give the new virtual identity, which presents barriers in the process of providing a high degree of security to user data. The suggested approach is able to generate the new virtual uniqueness using the two distinct fingerprints in a manner that is trustworthy and accurate, hence protecting the private information in any situation.

3. Dual fingerprint algorithm

Let us consider the two fingerprints, namely A and B, respectively taken from the two unlike fingers, where this registration has been done by the method, which is further using these fingerprints to create the template, and later on, these templates are used for the verification of the genuine person in all of the different application areas [9]. Let us now consider the two fingerprints, respectively. The two most crucial stages of the projected procedure are as follows:

- The primary strategy that the suggested algorithm employs is to make use of certain strategies that aid to pinpoint minutiae places within the fingerprint mechanism A and the corresponding orientation inside another fingerprint.

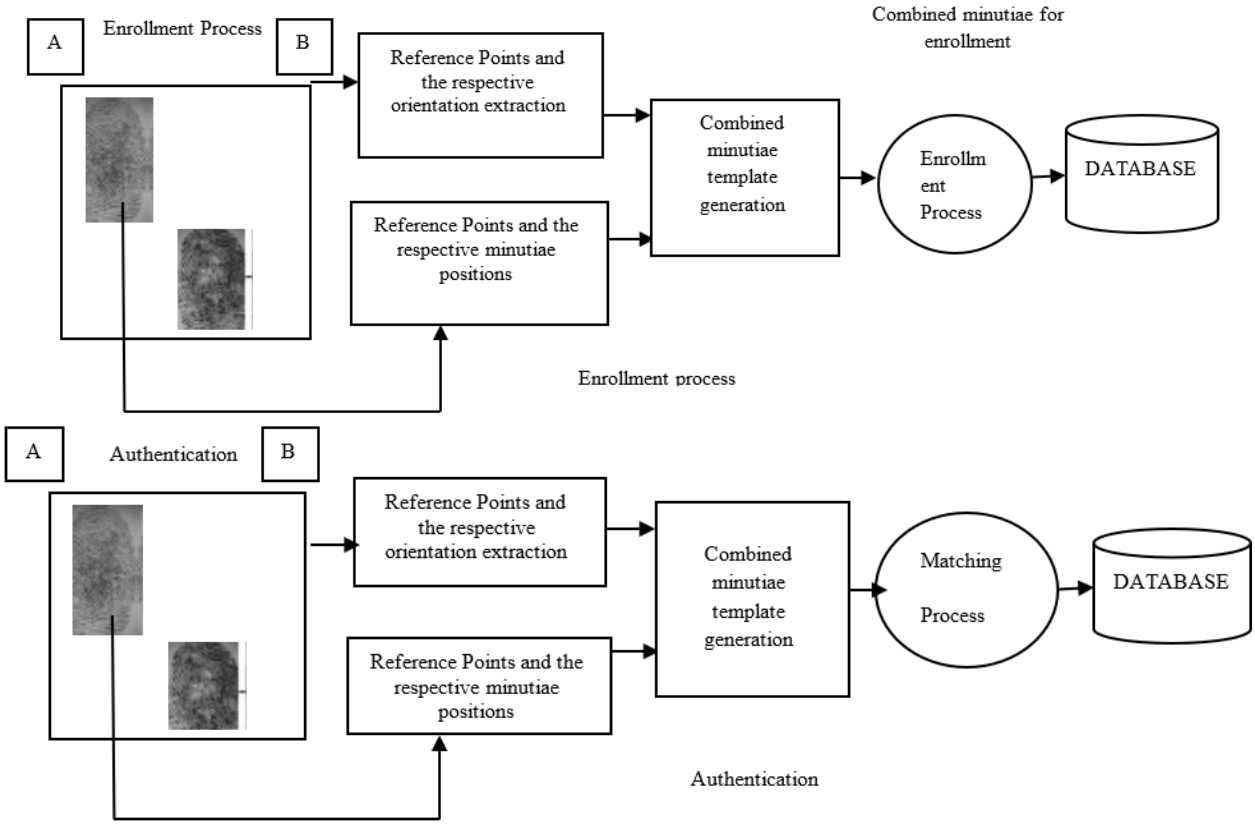

Fig.1: Fingerprint model for the privacy protection

- After that, a combined minutiae template is successfully constructed from the minutiae potions, orientations, and reference points, and lastly various coding schemes are used to secure the private data.

3.1 Detection of reference points

The detection of reference points is inspired by the traditional articles that are presented in the literature. These papers are either theoretical works or research works, depending on the context. The work that was offered by Nilsson and colleagues, in which the detection of points is accomplished by making use of complicated filters, served as inspiration for the approach that was shown here. The following is an outline of the primary stages involved in locating reference points:

(a) The extraction of the orientation is the most important stage in the suggested method. In this step, the orientation O from the corresponding fingerprint is determined with the assistance of orientation estimation methods that have been documented in the relevant body of research.

(b) The orientation O in the complex domain may be derived as follows, using the statistics that were collected from the orientation estimation techniques.

$$\mathrm{Z} = \cos(2O) + j\sin(2O) \qquad (1)$$

(c) The calculation of the certainty map of the orientation O are as follows, these calculation of certain map helps to find the best samples in next steps

$$C_{ref} = Z * \bar{T}_{ref} \qquad (2)$$

(d) Then the use of convolution operator finally gives the kernel reference points detection based on the convolution operator "*" as reported in the above step and the respective $\bar{T}_{ref}$ is the conjugate of

$$T_{ref} = (x + iy).\frac{1}{2\pi\sigma^2}\,.\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right) \qquad (3)$$

(e) Based on the above figure analysis the generation of combined minutiae template has started and the respective improved certainty map are stated as follows

$$C'_{ref} = \begin{cases} C_{ref}.\sin\left(Arg(C_{ref})\right) & if\ Arg(C_{ref}) > 0 \\ 0 & otherwise \end{cases} \qquad (4)$$

3.2 The generation of combined minutiae template

In this context, the phrase "Arg (z) value" refers to the most important value out of all the possible values on the enhanced confidence map, which is defined as falling somewhere between - and.

(f) The localization of the reference point that satisfies the two conditions is determined by using two norms, which are (1) the amplitude in terms of the local minimum and the threshold in terms of the local maximum.
(g) The steps described above are performed as many times as necessary until all reference sites that meet the two requirements are found.
(h) There are certain circumstances in which we are unable to retrieve a single reference point; in these instances, the whole fingerprint picture is evaluated based on the greatest certainty value.

The N minutiae locations from the fingerprint A, concurrently the extracted orientation from the fingerprint B, and lastly the combined minutiae template by references points from the fingerprints A and B, as illustrated in Fig. 2, are all included.

Positional Alignment of the Minute Details

(a) The minutiae position alignment was carried out based on reference points, and the reference point with the highest confidence value was taken into consideration as the principal reference point. As a result, we have two fingerprints. The reference points obtained from two fingerprints with the highest degree of confidence are denoted by the letters R_a and R_b, respectively.

(b) Lets make an assumption that the reference point R_a is located at certain point with the angle $ß_a$ and simultaneously R_b is located at certain point with the angle $ß_b$.

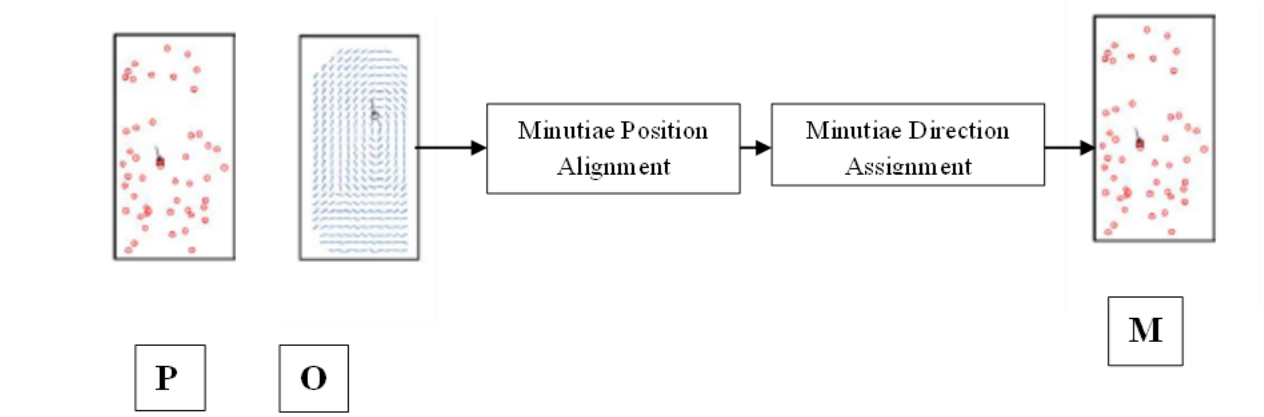

Fig.2: The process of combined minutiae template generation

(c) The final alignment process is completed by rotating and translating each and every minutiae point as shown in the following state

$$(p_{ic})^T = H.(p_{ia} - r_a)^T + (r_b)^T \quad (5)$$

While we make use of the convolution operator to determine the orientation of the complex domain, the usage of the transpose operator in the minutiae positions demonstrates a significant improvement in terms of obtaining accurate positions. This is accomplished after the rotation and translation of all minutiae positions have been finished, as stated in the following sentence:

$$H = \cos(\beta_b - \beta_a), \sin(\beta_b - \beta_a) \\ -\sin(\beta_b - \beta_a), \cos(\beta_b - \beta_a) \quad (6)$$

at this alignment, the odds of overlapping may also sometimes occur at the maximal certainty points of the two distinct fingerprints.

3.3 Minutiae Direction Assignment

If the alignment is given to the dependable direction of the collected minutiae locations and directions reference points, then the procedure of combining the minutiae templates has been successfully accomplished. The relevant alignment assignments are as described below.

$$\theta_{ic} = O_B(x_{ic}, y_{ic}) + \rho_i \pi \quad (7)$$

Where

Pi is either 0 or 1 as it is integer

O_B is ranges from 0 to π

Θ_{ic} is ranges from 0 to 2π.

Finally the respective three coding strategies are stated as follows

$$\rho_i = \begin{cases} 1 & if\ mod(\theta_{ia} + \beta_b - \beta_a, \pi) \\ & -O_B(x_{ic}, y_{ic}) > 0 \\ 0 & otherwise \end{cases} \quad (8)$$

$$\rho_i = \begin{cases} 1 & if\ mod(ave_b(x_{ic}, y_{ic}), \pi) - O_B(x_{ic}, y_{ic}) > 0 \\ 0 & otherwise \end{cases} \quad (9)$$

$$ave_b(x_{ic}, y_{ic}) = \frac{1}{n}\sum_{k=1}^{n} \theta_b^k(x_{ic}, y_{ic}) \quad (10)$$

These coding solutions were used to accomplish the greatest possible matching amongst coupled minutiae templates and also to give a very excellent balance between the variety and matching in a trustworthy manner.

3.4 Two stage fingerprint matching

By this step, with the following formulae and descriptions as follows, the accuracy of the matching scores is assessed by combined minutiae template production from the two distinct fingerprints. This evaluation is expressed with the following:

$$L_{ij} = \sqrt{(x_{ic} - x_{jc})^2 + (y_{ic} - y_{jc})^2} \quad (11)$$

$$\gamma_{ij} = \theta_{ic} \bmod \pi - \theta_{jc} \bmod \pi \quad (12)$$

$$\sigma_{ij} = \Re\left(\theta_{ic} \bmod \pi, atan2(y_{jc} - y_{ic}, x_{jc} - x_{ic})\right) \quad (13)$$

$$\Re(\mu_1, \mu_2) = \begin{cases} \mu_1 - \mu_2 & if -\pi < \mu_1 - \mu_2 \leq \pi \\ \mu_1 - \mu_2 + 2\pi & if\ \mu_1 - \mu_2 \leq -\pi \\ \mu_2 - \mu_1 + 2\pi & if\ \mu_1 - \mu_2 > \pi \end{cases} \quad (14)$$

$$F_i = \left(L_{ij}, L_{ik}, L_{il}, \gamma_{ij}, \gamma_{ik}, \gamma_{il}, \sigma_{ij}, \sigma_{ik}, \sigma_{il}\right) \quad (15)$$

$$D_\tau(u, v) = w_1 . \sum_{j=1}^{3} |F_u(j) - F_v(j)| + w_2 . \sum_{j=4}^{9} |F_u(j) - F_v(j)| \quad (16)$$

$$d_\tau = min_{u,v}\, D_\tau(u, v). \quad (17)$$

(a) The effectiveness of the matching procedure is assessed by first taking into account the closest, then the second nearest, and lastly the third nearest. The coding procedures are used to get an understanding of the distinctions that exist between the respective two sites, and they are also of assistance in the identification of the overlapping zonal regions.

(b) The relevant matching is conducted on all specified characteristics until the final selected reference in order to build a true fingerprint similar based on all of this information in order to preserve the private data.

(c) The stages of matching based on angle, coding schemes, and differences are repeated on all references until the final statistical result has been arrived at.

(d) At this step, two significant actions are carried out for each reference point: the first of these is the calculation of the matching difference based on the acquired query minutiae, and the second is the production of those. The second step is determining the final matching difference in order to create the combined template for the final output.

4. Algorithm flow

The dual fingerprint system for privacy protection is based on the orientation and minutiae locations, in addition to the coding schemes, in order to produce the template that gives the answer to all of the issues that are now present. In the past, many theoretical works and algorithms have been proposed that are based on a single fingerprint, which primarily lacks of secrecy and privacy. Furthermore, the algorithms that are based on a single fingerprint mechanism fail to provide security to the authenticated fingerprints in the database, and data can easily be lost as a result of incidental or accidental hacking. The suggested method includes a good algorithm that will give greater protection to the private data, and the main phases are as follows:

(a) Estimation of the Orientation O by using the orientation estimation methods on a collection of minutiae points.

(b) The use of the Gabor filter makes it simple to do the duty of analyzing local and global information without noise in orientations and tiny locations without requiring much effort.

(c) To estimate the phase image, the FM AM model is utilized, which is also the model that was used in the previous study that was described in the literature.

(d) The last step, which is the formation of a reconstructed phase picture, involves integrating the continuous phase image with the spiral phased image in order to get the precise phase image.

(e) Once the appropriate procedures have been carried out, a better phase will emerge, one that is devoid of false points.

(f) At long last, a real-looking fingerprint template that is devoid of noise and offers excellent security for the confidentiality of personal information has been created.

5. Simulation results

(a) Based on the information presented above, we can determine how to extract minute points and their intersections. To do this, we must first load picture 1, and then load image 2 in order to extract the appropriate characteristics.
(b) The first image and the second image in the preceding picture are completely distinct from one another; in this case, two distinct fingerprinting methods were used to get the combined minute details.
(c) The reconstruction process is carried out during this stage, and it is carried out in a trustworthy manner so that statistics can be obtained for the next step, which is the verification step.

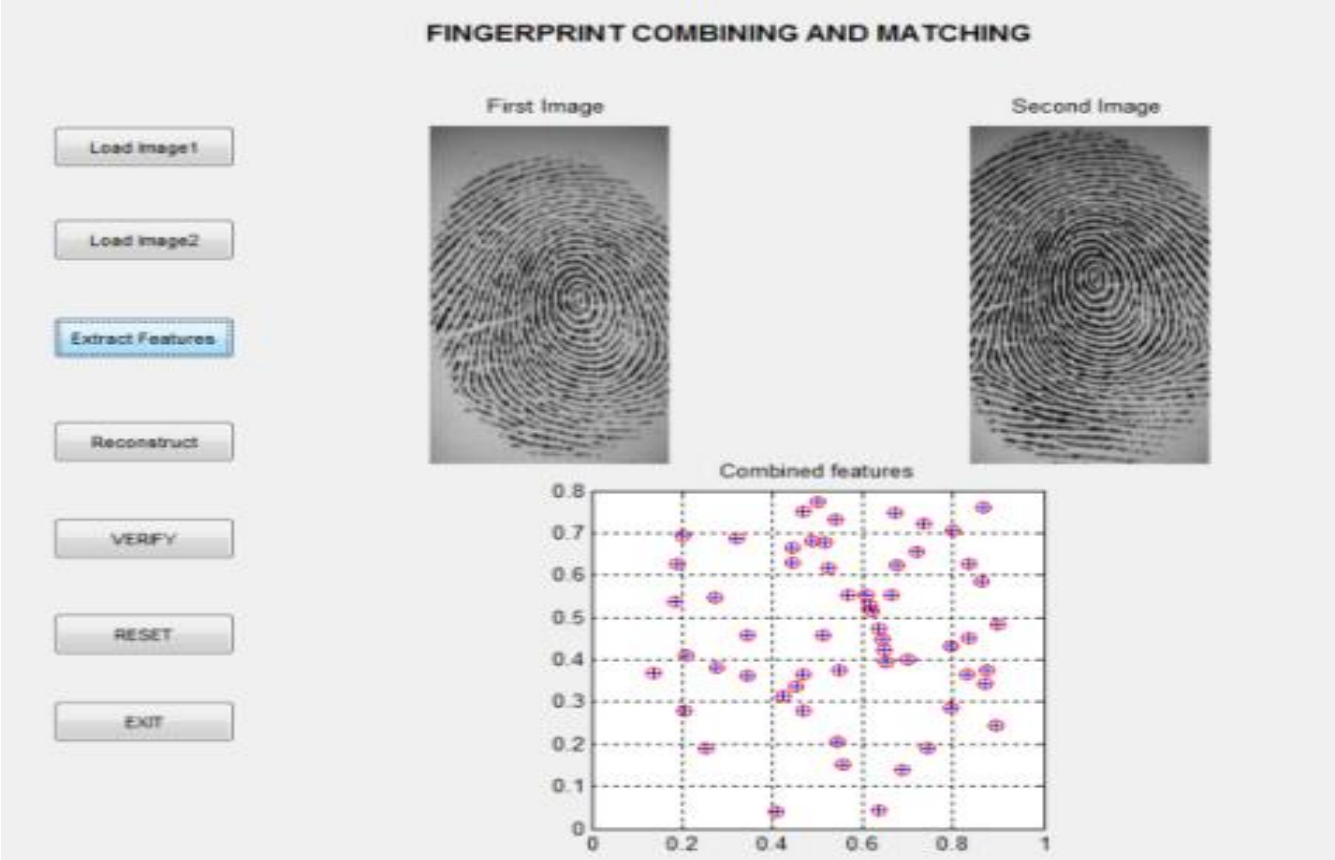

Fig.3: Extraction of minutiae points and its intersection analysis

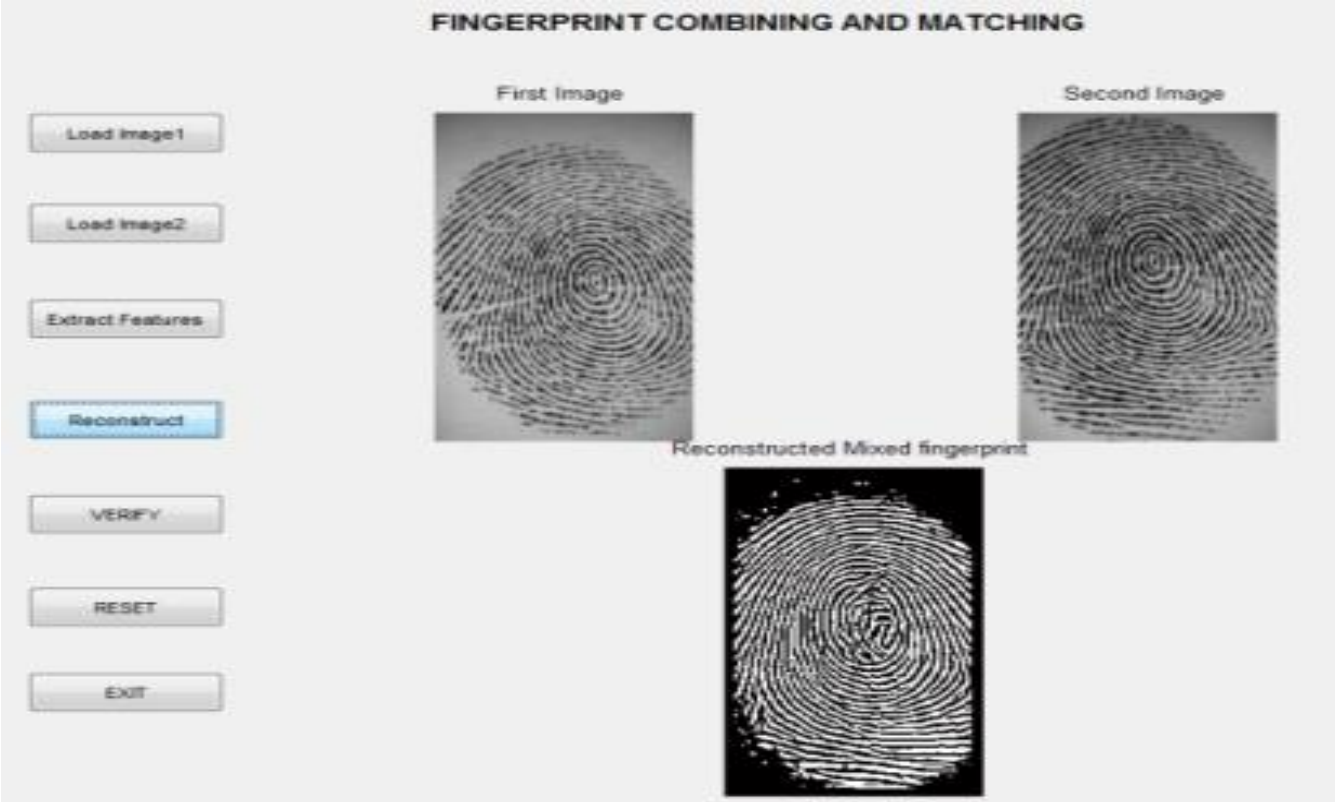

Fig. 4: Generation of mixed fingerprint

(d) After that, verification of the acquired features is carried out in this step in order to identify the reliable features, and this phase is repeated in order to get all of the reliable features, as indicated in the third content in the figure that was previously shown.
(e) This procedure is carried out once more for each dual fingerprint, after which the prior methodology is reset.
(f) In order to extract the relavant features, combined features are produced using the two distinct fingerprints.

5.1 Results analysis

(a) Based on the information presented above, we can determine how to extract minute points and their intersections. To do this, we must first load picture 1, and then load image 2 in order to extract the appropriate characteristics.
(b) The first image and the second image in the preceding picture are completely distinct from one another; in this case, two distinct fingerprinting methods were used to get the combined minute details.
(c) The reconstruction process is carried out during this stage, and it is carried out in a trustworthy manner so that statistics can be obtained for the next step, which is the verification step.
(d) After that, verification of the acquired features is carried out in this step in order to identify the reliable features, and this phase is repeated in order to get all of the reliable features, as indicated in the third content in the figure that was previously shown.
(e) This procedure is carried out once more for each dual fingerprint, after which the prior methodology is reset.
(f) In order to produce the necessary reconstructed mixed fingerprint, combined features are created from the two distinct fingerprints.

Table. 1: performance of the reference points detection at different Settings of threshold

	T			
	3	**4**	**4**	**6**
No.	**1141**	**650**	**291**	**207**
True detection rate (%)	99.5	99.5	99.5	98.5
Flase Detection rate (%)	0.5	0.5	0.5	1.5

6. Conclusion and extension

In this article, we provide an unconventional method for protecting fingerprint privacy by combining two different fingerprints to create a new identity. This method was developed by us. During registration, the arrangement takes two fingerprints from two different fingers on two different people. An arrangement of merged minutiae that is exacting just a fractional minutiae characteristic of each of the two fingerprints will be formed and saved in a database. During the process of producing the combined development arrangement, three distinct coding procedures are used in order to make the gathered minutiae template seem as perfect as an initial development template. In order to complete the authentication procedure, you will need to provide two fingerprints that come from the same two fingers. A two-stage fingerprint matching activity is presented for analogous the two concern fingerprints adjoin the enrolled template. This action will compare the fingerprints to one another. An original minutiae template has a cartography that is similar to the one that our combined minutiae arrangement uses. As a result, we are able to combine two distinct fingerprints into a single new basic character by reconstructing a real-look comparable accumulated fingerprint from the accumulated development template. This allows us to combine two different fingerprints into a single new basic character. The first findings indicate that our setup is successful in achieving a very low absurdity rate with FRR = 0.4% while maintaining FAR = 0.1%. When using the integrated development templates, an attacker will have a tough time breaking into additional suitable systems. If the two fingerprints that have been changed are picked at random, our address is capable of producing a much larger new virtual character in comparison to the state-of-the-art approach. According to the results of the test, the adversary does not have an easy time balancing the indigenous development templates by starting with an accumulated development arrangement or a mixed fingerprint. The addition of the work that was presented was done on a verification model that was based on palm prints. Palm prints are the most widely used biometric identification method after fingerprints, and the benefits of palm prints include rapid data gathering, dependability, and high user acceptance. We employ a palm print system for

authentication and identification in our extended work. This system operates on the basis of an advanced transform model known as wavelet transformation, and it does so in a variety of ways. For the purpose of conducting an accurate analysis, a number of distinct wavelet types, including Biorthogonal, Symlet, and Discrete Meyer, are used. Additionally, this process is carried out on around 500 photos contributed by fifty unique individuals, with a minimum sample size of ten samples during the course of a six-month-long program. The results of the experiments, which were collected from the data, revealed that the suggested system is feasible by demonstrating a Genuine Acceptance Rate (GAR) of 97.12%.

Conflict of Interest

Authors declare "No conflict of interest"

References

[1] B. Mauro, G. Droandi and R. Lazzeretti "Privacy protection in biometric-based recognition systems: A marriage between cryptography and signal processing", *IEEE Signal Processing Magazine*, Vol. 32, No. 5, pp. 66-76, 2015.

[2] A. Naami, Khaled, A. E. Ghamry, M. Shihabul Islam, L. Khan, B. Thuraisingham, K. W. Hamlen, Mohammed Alrahmawy, and Magdi Z. Rashad "Bimorphing: A bi-directional bursting defense against website fingerprinting attacks." *IEEE Transactions on Dependable and Secure Computing,* Vol. 18, No. 2, pp. 505-517, 2019.

[3] J. Kumar and A. K. Singh. "Copyright protection of medical images: A view of the state-of-the-art research and current developments", *Multimedia Tools and Applications*, pp. 1-31, 2023.

[4] X. Feiyi, H. Wen, Y. Li, S. Chen, L. Hu, Y. Chen, and H. Song "Optimized coherent integration-based radio frequency fingerprinting in Internet of Things", *IEEE Internet of Things Journal* Vol. 5, No. 5, pp. 3967-3977, 2018.

[5] K. Kanagalakshmi and J. K. Antony "A cancellable and irrevocable approach for fingerprint template protection using optimal iterative solubility algorithm and secure point BASE", *Biomedical Engineering: Applications, Basis and Communications* Vol. 35, No. 01, art.no. 2250049, 2023.

[6] F. A. Joseph and I. Kalokoh "Watermarking of Frequency and Steganography for Protection of Medical Images Based on Bacterial Foraging Optimization and Genetic Algorithm", *British Journal of Healthcare and Medical Research,* Vol. 10, No. 4, 2023

[7] K. Tamilarasi and A. Jawahar "Medical data security for healthcare applications using hybrid lightweight encryption and swarm optimization algorithm", *Wireless Personal Communications,* Vol. 114, pp. 1865-1886, 2020.

[8] K. Santosh, S. K. Singh, A. K. Singh, S. Tiwari, and R. S. Singh "Privacy preserving security using biometrics in cloud computing", *Multimedia Tools and Applications,* Vol. 77, pp. 11017-11039, 2018.

[9] E. Zekeriya, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk and T. Toft "Privacy-preserving face recognition", *In Privacy Enhancing Technologies: 9th International Symposium, PETS 2009, Seattle, WA, USA, August 5-7, 2009. Proceedings 9*, pp. 235-253, 2009.

Copyright: © 2023 by the authors, Licensee ITEECS, India. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https:// creativecommons.org/licenses/by/ 4.0/).

***