Preventing biometric authentication using steganography

Vishwa Nakrani, Janak Maru
Department of computer engineering Atmiya university Gujarat, India

Abstract*- Individual biometrics are essential to authentication procedures in the modern world. Despite their convenience, biometrics present a number of difficulties. For instance, a conventional passphrase can be easily changed to a new one if it is compromised. However, a person's biometric information is irreplaceable if it is compromised. Furthermore, biometric systems are susceptible to a number of attacks, including Trojan horse attacks and the deployment of fake physical biometrics, which can be used to maliciously alter the authentication process. The goal of this study is to use steganography to present a new and safe authentication method. The feature extraction module, the payload creation and authentication module, the Trojan horse countering module, and the false physical biometrics countering module are the four main modules that make up the suggested solution's all-encompassing strategy for addressing these issues. This solution's design makes it simple to incorporate into current biometric authentication systems, improving user experience and security in today's widely used multi-factor authentication procedures.

***Keywords*- biometric threats, steganography, biometric vulnerabilities, biometric systems, biometric authentication, and security.**

I. INTRODUCTION

The process of determining and confirming the legitimacy of a user's stated identity is known as authentication. Usually, this is accomplished by cross-referencing stored information with user-submitted credentials, like passwords or PINs. However, biometrics have become a more effective and practical substitute in a world where there are many ways to break passwords and get beyond conventional authentication. Because of this, a lot of people now favour biometric authentication over passphrases or passwords.

Biometrics have shown to be quite successful for authentication because of their special qualities. Additionally, biometrics provide a high degree of convenience for users by removing the need to memorize complicated passwords. As a result, "multi-factor authentication" is now a feature that many devices and apps offer as an extra security safeguard. In a two-step verification process, this enables users to confirm their identity using a password and biometric information.

However, the "open" character of biometrics has turned out to be a major disadvantage in biometric authentication, despite its convenience. Within 24 hours of the debut of the iPhone 5S in 2013, Jan Krissler, commonly known as "Starbug," from the Computer Chaos Club (CCC), was able to effectively spoof Apple's TouchID sensors. Then, using wood, glue, and sprayable graphene, a prosthetic finger could be made using photos of a user's fingerprints obtained from a glass surface. By using images from a regular camera to mimic the fingerprint of Ursula von der Leyen, Germany's then-defense minister, Starbug once more exposed the flaws in biometrics in 2014. These events demonstrate the ease with which biometric information can be compromised.

Biometrics continue to be a practical and efficient means of authentication in spite of security concerns. Therefore, the goal of this research is to improve the security of the biometric authentication process rather than replace it. Two fingerprint templates are typically compared in fingerprint authentication. However, the suggested method will use steganography to incorporate a payload into the fingerprint templates. These embedded payloads will be taken out and compared during authentication. The security of the authentication procedure won't be impacted by any hacked biometric data because the verification process depends on matching the payloads rather than the fingerprint templates.

In addition to secure authentication, this study tackles two distinct forms of authentication-related attacks: trojan horse attacks, which manipulate the authentication process to further the goals of a malevolent user, and attacks involving phony physical biometrics that aim to reconstruct minutiae. Therefore, the goal of this research is to provide a complete solution that improves and protects the biometric authentication procedure.

The main objective of this study is to suggest a novel and safe biometric authentication technique that eliminates the possibility of hacked biometric information endangering the authentication procedure. Furthermore, this study attempts to improve the security and dependability of the multi-factor authentication techniques now in use.

There are five sections in this research paper. The pertinent literature for this investigation is reviewed in Section II. The results and approach are presented in Sections III and IV. Section V brings the study to a close and makes recommendations for possible directions for further research.

II. RELATED WORK

The best technologies for creating a more secure authentication algorithm include digital watermarking, cryptography, and steganography, according to extensive study. Ghouti and Bouridane's study included a watermarking technology for biometric data authentication that showed great resilience without appreciably changing the fingerprint picture.

Li and Cot stressed in their paper that a safe system that uses data concealing shouldn't reveal the existence of such a method to an attacker. As a result, cryptography is less appropriate because potential hackers may readily identify its use. The drawbacks of employing digital watermarking and cryptography for this research subject are listed in Table I.

Table I: Disadvantages of Using Cryptography and Digital Watermarking

Digital water marking	cryptography
Watermarks may vanish if the picture is compressed, resized, or altered.	Attackers can easily identify cryptography.
It doesn't limit data access.	The incapacity to encrypt pictures with consistent color or grayscale.
Visible only in certain circumstances.	There is a high chance of key generation errors.
If there is a noticeable distortion in the carrier signal, it loses its effectiveness.	Deterioration of the image and decreased correlation.

In their paper, Peethala and Kulkarni suggested an approach that uses steganography in conjunction with a cryptosystem to provide authentication. By strengthening their resistance to several types of attacks across open networks, this technique improved the security of biometric cryptosystems. Steganography was therefore shown to be quite successful at concealing data in authentication applications.

Steganography has a number of benefits over encryption and digital watermarking. Most notably, it is a covert defense mechanism that is difficult for attackers to discover. Steganography also allows for hidden communication and offers increased security, capacity, and robustness. Table II illustrates why steganography is the best method for authentication by contrasting the detectability, confidentiality, and removability of digital watermarking, cryptography, and steganography.

Table II: Comparison of Properties Against Technologies

Technology	Confidentiality	Removability	Detectability
Digital watermarking	✓	✓	✓
Cryptography	✓	✗	✓
Steganography	✓	✗	✗

Matsumoto et al. tested the acceptance rate of different false fingerprints against fingerprint sensors in a series of studies. They discovered that all 11 of the fingerprint systems they studied allowed for the enrolment of phony fingerprints. Furthermore, these biometric identification systems have a 68% to 100% acceptance rate for phony physical biometrics.

Chaudhari and Deore claim that tricking an authorized user into entering a phony fingerprint into a biometric system is the use of fake physical biometrics. These synthetic fingerprints can be made from silicone, wax, and other materials. With or without the victim's consent, this makes it possible for an attacker to swiftly create a phony fingerprint and access extremely protected systems. Verifying the finger's "liveness" is a useful countermeasure in these situations. This technique aids in establishing the legitimacy of the biometric signal by confirming that it originates from a real, living person.

According to a preliminary review, there are two sorts of technologies that can be used to determine whether a fingerprint is live: software-based and hardware-based technologies. The previously costly fingerprint systems have grown in size and expense since the advent of hardware-based systems. In the end, it was determined that a software-based strategy would be more advantageous.

A liveness detecting system that tracks subtle movements on the surface of the fingertip that are brought on by variations in blood flow volume was proposed by Drahansky, Notzel, and Funk. The authors proposed two optical solutions to measure these frequent surface alterations. While the second system uses a laser sensor to identify variations in blood flow and fingertip volume, the first system uses a Charge-Coupled Device (CCD) camera in conjunction with an image capture macro lens.

Moon et al.'s publication suggested a liveness detection system for fingerprints that looked at a person's fingertip features. They used a wavelet-based approach to denoize the noise residue that resulted from representing a picture as a fingerprint. The resulting mix's harshness was then evaluated using the standard deviation of the noise leftover from the mixed composite signal. Furthermore, according to the scientists, one way to determine liveness is to use an ultrasonic sensor to look at the fingerprint beneath the dermis (underlying layer) and epidermis (outer layer), with the deeper layer being put on a softer, more yielding substance.

According to Mwema, Kimani, and Kimwele's publication, trojan horse attacks—those that take the place of matcher programs and allow access to all users, including unauthorized ones—were found to be the third most frequent type of attack on biometric authentication systems, occurring at a rate of 24.4%.
In their paper, Jain, Nandakumar, and Nagar talked about Dr. Fred Cohen's 1984 introduction of the undecidability principle, which states that malicious code may be correctly detected. They clarified that there is a limit to the detection accuracy because of the inherent complexity of malicious code in a Von Neumann system, which makes it difficult to forecast all of such code in a polynomial computation time.

III. METHODOLOGY

The enrolment and authentication phases are the two main stages of fingerprint authentication. The system records a person's fingerprints during the enrolment stage. A user who claims to be authentic gives their fingerprint in order to access the system during the authentication step. The functioning of the suggested solution in each of these stages will be described in this section.

A. Fingerprint Extraction

The first step is to use image processing techniques to turn the fingerprint into an image file. The intensity values in this image are standardized by applying a pixel-by-pixel normalizing procedure. The block orientation is then ascertained by averaging, voting on, or optimizing the pixel gradient, which represents the orientation of the ridge directions in the fingerprint. The main characteristics of a fingerprint are depicted in Figure 1.

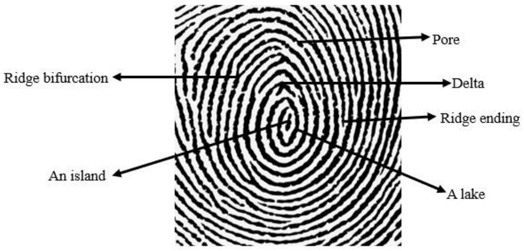

Fig. 1. Major features in a fingerprint [13]

common The received frequency should be rounded, and filters that correspond to these frequencies must be made in order to decrease the number of unique frequencies. The same filters used for ridge segmentation can be used for directional smoothing, which smoothes out the ridges after identification.
Prior to minutiae extraction, thinning is the last stage of pre-processing. Pixel values are reduced by a structural process called thinning until they are just one pixel wide. Fine features are then extracted from the skeletonized binary image that results from thinning.

P4	P3	P2
P5	P	P1
P6	P7	P8

Fig. 2. A 3x3 window used in minutiae extraction [15]

In the minutiae extraction stage, each ridge in the picture pixels is examined for similarity using a 3x3 window, as illustrated in Figure 2. To extract minutiae, the Crossing Number (CN) approach is used. A ridge point can be categorized as a ridge terminus, a bifurcation, or an anti-minutiae point based on the computed CN score, as indicated in equation (1).

$$\text{CN} = ½ \sum_{i=1}^{8} |\text{Pi} - \text{Pi} + 1|$$

Following the CN method's identification of the fingerprint image's bifurcation and termination locations, the slope of the minutiae is computed using the nearby pixels. After that, a text file containing these minute details is saved.

The right minutiae points are then extracted from the thinned fingerprint image using a neural network that consists of an encoder, a hidden layer, and an output vector. After being transformed into hexadecimal representation, these minute values are transmitted to the subsequent module to produce a payload.

B. Fingerprint Authentication

As demonstrated in equation (2), a payload is created during the enrolment step by combining the hexadecimal value obtained from the feature extraction module with a distinct value produced by a Cryptographically Secure Pseudo Random Number Generator (CSPRNG). The payload and its matching CSPRNG value are then saved in the database after being steganographically inserted within the fingerprint template.

Hexadecimal value + CSPRNG value = Payload (2)

During the authentication process, a payload is created by combining the incoming hexadecimal value with a CSPRNG value that was obtained from the database. In parallel, reverse steganography is used to extract the payload from the stored template that corresponds to the returned CSPRNG value. After comparing the two payloads, a similarity score is determined. The user gets authenticated if the similarity score is higher than the cutoff point of 0.889999.

This module carries out match-in-database or match-on-server authentication. The module compares the user with the database 1:N each time a user tries to authenticate in order to confirm the user's identity. However, this module is susceptible to a number of attacks, including malicious data injection, fingerprint reconstruction from saved templates, illegal threshold score manipulation, and residual reuse. To reduce these hazards, a number of countermeasures have been put in place.

The transmission channel between this module and the feature extraction module is the target of the reuse-of-residuals attack. Variables are flushed right away after usage to reduce this danger and stop hackers from using out-of-date variables maliciously.

Attackers may try to replace database templates in a malicious data injection attack that targets the communication channel between this module and the template database without detecting the use of steganography. The authentication process makes it simple to thwart this attack. During the steganography decoding process, the template is instantly deleted if no payload is extracted.

"Reconstructing fingerprints using cached templates poses a serious risk to this module. Avoiding keeping minute details in the fingerprint template is a popular remedy. The suggested method embeds a payload into the template rather than saving details. Furthermore, steganography is used to disguise the template in the database, thus thwarting this kind of assault.

Unauthorized modifications to the threshold score could make this strategy less effective. This will be avoided by using a straightforward challenge-response system to confirm that the threshold score doesn't change. A module that prevents trojan horse assaults also provides additional security.

C. Countering Fake Physical Biometrics

This module records the minutiae values at the enhancement point and improves the image to a preset degree when the user places their finger on the sensor. After several iterations of this procedure, the average value is determined. The improved average value of the fingerprint image utilized for authentication is then contrasted with the minutiae values of the enrolled user's reference template.

It is impossible to ensure that fingerprint images taken by a scanner will be 100% correct. Therefore, it is effective to preserve sufficient contrast by employing a higher resolution that captures detailed ridges and furrows. Several procedures, such as binarization, thinning, augmentation, extraction, and matching, were used to improve the fingerprint template picture during registration and authentication.

To guarantee a consistent transformation, localized threshold expansion was used in the binarization transformation of an index fingerprint image. This excluded pixels with a single zero value instead of two different values for discrete ridges. After that, the binary image is thinned to highlight its geometric structure and simplify the data. By making the entire image one pixel wide, this image's pixel count is reduced.

The amount of valuable information that can be gleaned from a fingerprint determines the extent to which image processing techniques can improve fingerprint photographs. The minutiae matching algorithm completes the pre-processing steps after the minutiae are extracted. After minutiae have been spatially mapped till they are finished, the percentage match is computed. No matter how minor it may appear, no detail is missed.

A Fingerprint Analysis and Management System (FAMS), which contains the fingerprints of more than 500 people of different ages and genders, was used for image augmentation. The dataset contained both real and fake fingerprints, which were made by placing them on a biometric device after they had been traced on silicone.

D. Countering Trojan Horse Attacks

The authenticity of the authentication code is checked before authentication starts. First, the system's current code and the valid code are both encoded. After that, a comparison window is used to evaluate how similar these codes are. The authentication procedure proceeds if the codes match; if not, the valid code is entered into the system and the authentication procedure is completed.

This anti-trojan algorithm makes use of Message Digest 5 (MD5), a one-way cryptographic function that generates a fixed-length 128-bit digest as output after accepting an input message of arbitrary length. After dividing the input message into 512-bit blocks, the overall length is made sure to be a multiple of 512 bits by padding the blocks. Several directions specified by Putri Ratna et al. in their article were followed to perform this technique as mentioned below:

- "To make sure the message's overall length is 64 bits less than a multiple of 512, a single bit, 1, was attached to the end of the message and followed by the required number of 0s.
- Values corresponding to the message's initial length modulo 2^64 were entered into the remaining 64 bits.

The four 32-bit words designated A, B, C, and D make up the 128-bit state on which the suggested algorithm runs. In their low-order bytes, these words are originally initialized to the following fixed constant values:

WORD A: 89 ab cd ef
WORD B: 01 23 45 67
WORD C: 76 54 32 10
WORD D: fe dc ba 89

The state is updated by processing each 512-bit message block in four identical steps called 'rounds.'"

IV. RESULTS AND DISCUSSION

This section presents the results achieved upon the conclusion of this research. It also covers the challenges encountered and the strategies implemented to address them whenever feasible.

A. Feature Extraction

The retrieved fingerprint minutiae were successfully converted into a hexadecimal value by the system. However, this module's fake minutiae structures presented a problem. All minutiae points found in the valleys between ridges are regarded as spurious minutiae in fingerprint segmentation. Furthermore, a number of inaccurate details were noticed in the fingerprint pattern's components. One striking feature of these fake minutiae was their proximity to each other. Consequently, the instructions suggested by Cao and Wang in their study [19] were used to delete these incorrect minutiae structures.

B. Fingerprint Authentication

The Big O Notation, which indicates the upper bound of the algorithm's time complexity, can be represented as seen in (4), according to the results of the payload injection module's time complexity study. Usually, a value n that indicates the size of the input (e.g., the number of elements in an input array) affects the temporal complexity T. However, because this approach just takes the payload's length into account, it functions regardless of the amount of the input. Thus, it may be said that the payload injection module functions in "constant time" since its execution time, T, is constant. Regardless of the template format, it was also found that this module operates consistently.

$$T = 0(1) \qquad (4)$$

A reference fingerprint template, which contains important details, is compared to an incoming template to check for similarities in standard fingerprint authentication. But in this case, two payloads are compared, which results in a much reduced time and resource requirement.

A particular set of fingerprint minutiae points match to the hexadecimal value utilized for payload creation. Problems could occur, though, if at least one detail is altered during the fingerprint extraction stage of the authentication process. The entire produced payload is changed by any change in a single tiny point. A similarity range was established for payload comparisons in order to lessen the impact of this problem. After completing a number of test cases, which are summarized in Table III, this conclusion was reached. According to Joshi et al.'s publication, these test scenarios took into account the error range for high-performance fingerprint recognition systems, which have false positive rates of \(10^{-6}\) and false negative rates of \(10^{-4}\) [20].

Table III: Summary of Test Cases for Authentication

Test case ID	Scenario	Accuracy of authentication
001	The two payloads were the same.	100%
002	A ".0" was added at the end of one payload, which was the float version of the other.	97.44%
003	Before creating the payload, the CSPRNG value of one payload was multiplied by π.	17.65%
004	Although the hexadecimal values varied, they were all in the same range.	86.84%

The outcomes of test cases 001 and 002 were successful and as anticipated. Test case 003 revealed an unanticipated degree of inaccuracy, nevertheless. Subsequent investigation showed that a far lower CSPRNG value than the hexadecimal value was the root reason. Two approaches are suggested to deal with this problem: raising the threshold score and using a bigger CSPRNG value in comparison to the hexadecimal value, which guarantees that any variation in the CSPRNG value has a significant effect on the payload.

The user was successfully verified in test case 004, which led to a greater level of accuracy for the solution even though the hexadecimal numbers utilized were different (but within the same range). It's crucial to remember that variables like humidity and pressure on the sensor can make it difficult to consistently provide the same hexadecimal result for a single user. As a result, hexadecimal numbers within a narrow range are accepted by the solution. This suggests that the biometric process's authentication module has yielded fruitful outcomes.

C. Countering Trojan Horse Attacks

The purpose of this module is to defend against a Trojan horse attack that aims to undermine the authentication procedure. An algorithm was put in place to read a file's contents and identify any changes in order to accomplish this. The system accurately recognized two files as matching when they had the same content. Nevertheless, the program identified the change and substituted the authentic file for the altered one when two files with disparate contents were compared, so preventing the Trojan horse attack.

V. CONCLUSION AND FUTURE RESEARCH

Biometrics, which include fingerprint recognition, facial features, retinal scans, and iris identification, have emerged as a very successful authentication technique in the modern world. With a special focus on security, this study aimed to create a new and safe way to improve the current fingerprint authentication techniques. A new defense against two prevalent attacks—Tornado horse attacks and phony physical biometrics—was developed by combining technologies including steganography, neural networks, cryptography, and image processing. The study's main findings include decreased time and resource usage as well as enhanced security in general.

Enhancing the security of popular biometric authentication procedures was the main objective of this study in order to support the development of multi-factor authentication systems. Because the CSPRNG value is generated by the system in a unique way, this research reduces the possible risks associated with the compromise of biometric data by using it to construct the payload. Stated differently, this method serves as a type of multi-factor authentication that successfully adds an extra degree of protection to the biometric authentication procedure.

While there were a number of difficulties during this research, the most were resolved, and the remaining difficulties have created opportunities for additional investigation. Applying this method to other forms of static biometric identification, such facial recognition and iris authentication, is one possible direction for further study. Future researchers might, for example, investigate how to turn a person's facial traits into a distinct value that can be used for authentication in conjunction with another value generated by the system. Furthermore, when dynamic biometrics are used for authentication more frequently, future research could concentrate on figuring out related security problems and creating comparable improved defenses against the assaults.

REFERENCES

[1] "CCC | Chaos Computer Club breaks Apple TouchID", Ccc.de, 2021. [Online]. Available: https://www.ccc.de/en/updates/2013/ccc breaks-apple-touchid.

[2] "Politician's fingerprint 'cloned from photos' by hacker", BBC News, 2021. [Online]. Available: https://www.bbc.com/news/technology 30623611.

[3] L. Ghouti and A. Bouridane, "Data hiding in fingerprint images," 2006 14th European Signal Processing Conference, 2006, pp. 1-4.

[4] S. Li and A. C. Kot, "Privacy Protection of Fingerprint Database," in IEEE Signal Processing Letters, vol. 18, no. 2, pp. 115-118, Feb. 2011, doi: 10.1109/LSP.2010.2097592.

[5] M. B. Peethala and S. Kulkarni, "Integrating Biometric Cryptosystem with steganography for authentication," 2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE), 2016, pp. 28-31, doi: 10.1109/WIECON-ECE.2016.8009080.

[6] T. Matsumoto , H. Matsumoto , K. Yamada and S. Hoshino, "Impact of artificial "gummy" fingers on fingerprint systems," in IS&T/SPIE Electronic Imaging, 2002.

[7] A. Chaudhari and P. J. Deore, "Prevention of spoof attacks in fingerprinting using histogram features," 2012 Nirma University International Conference on Engineering (NUiCONE), Ahmedabad, India, 2012, pp. 1-4, doi: 10.1109/NUICONE.2012.6493244.

[8] M. Drahansky, R. Notzel, W. Funk, "Liveness detection based on fine movements of the fingerprint surface," Proc.of 2006 IEEE workshop on information assurance, IEEE 2006.

[9] Y. S. Moon, J. S. Chen, K.C. Chan, K. So., K. C. Woo, "Wavelet based fingerprint liveness detection,"Electronic letters 41(20), 1112 1113, 2005.

[10] J. Mwema, S. Kimani and M. Kimwele, "A Study of Approaches and Measures aimed at Securing Biometric Fingerprint Templates in Verification and Identification Systems," International Journal of Computer Applications Technology and Research, vol. 4, pp. 108 119, 2015.

[11] A. K. Jain, K. Nandakumar, and A. Nagar, "Fingerprint template protection: From theory to practice," in Security and Privacy in Biometrics, 2013, pp. 187–214, doi: 10.1007/978-1-4471-5230-9_8.

[12] D. Suter, A. Bab-Hadiashar , "Fingerprint Segmentation using the Phase of Multiscale Gabor Wavelets", Proceedings of the Fifth Asian Conference on Computer Vision, 2002, pp.27-32.

[13] M. Joshi and M. Bodhisatwa, "A Comprehensive Security Analysis of Match-in-database Fingerprint Biometric System," Pattern Recognition Letters, 2020, doi: 138. 10.1016/j.patrec.2020.07.024.

[14] Hong. L., Jain Anil,Yifei wan, "Fingerprint image enhancement:algorithm and performance" , IEEE tansactions on pattern

analysis and machine intelligence, vol. 20 no.8, 1998, pp.777-789.

[15] M. Khrisat, and Z. Alqadi, “Detecting, Counting Objects to Form Color Image Features,” IJARCCE 9(11), pp.69-74, 2020, doi: 10.17148/IJARCCE.2020.91112.

[16] M. Joshi, M. Bodhisatwa and D. Somnath, “Security Vulnerabilities Against Fingerprint vol. abs/1805.07116, 2018. Biometric System,” in ArXiv,

[17] A. A. Putri Ratna, P. Dewi Purnamasari, A. Shaugi and M. Salman, “Analysis and comparison of MD5 and SHA-1 algorithm implementation in Simple-O authentication based security system,” 2013 International Conference on QiR, 2013, pp. 99-104, doi: 10.1109/QiR.2013.6632545.

[18] A. S. Afre, M. Bharati and S. Tamane, “DeyPos: For multi-users environments using MD5,” 2017 1st International Conference on Intelligent Systems and Information Management (ICISIM), 2017, pp. 251-254, doi: 10.1109/ICISIM.2017.8122181.

[19] Letian Cao and Yazhou Wang, “Fingerprint image enhancement and minutiae extraction algorithm”, Linnaeus University Sweden, 2016.

[20] M. Joshi, M. Bodhisatwa and D. Somnath, "Security vulnerabilities against fingerprint biometric system," ArXiv, vol. abs/1805.07116, 2018.