

IP-BIOPROTECT INTELLECTUAL PROPERTY AWARE FRAMEWORK FOR SECURE BIOMETRIC SYSTEMS

S. Selvarani¹, Dr. M. Mary Shanthi Rani²

¹Assistant Professor, Department of MCA, Fatima College, Madurai & Research Scholar, Department of Computer Science & Applications, The Gandhigram Rural Institute (Deemed to be University), Dindigul.
Email ID: rani.s.selva@gmail.com

²Professor, Department of Computer Science & Applications, The Gandhigram Rural Institute (Deemed to be University), Dindigul. Email ID: drmaryshanthi@gmail.com

Abstract—The current trend is that biometric authentication systems are increasingly being combined with artificial intelligence, cloud computing, mobile apps, and distributed architectures. Whereas significant work has been done in terms of protecting the user and the biometric template through research on biometric template attacks, cancelable biometrics, biometric cryptosystems, and privacy-preserving authentication, there has not been enough attention paid to the protection of the biometric technology itself. For instance, the biometric algorithm, artificial intelligence model, the code and other such technologies can be copied, stolen, reverse-engineered, or even be a point of contention of ownership. Incorporation of patent and copyright concerns is done according to the nature of the asset, and ownership of the AI models is dealt with using fingerprinting of models, watermarking of the AI model, access control, versioning of the AI model, and record of ownership of the model. The threat model that will be designed will help to differentiate between attacks to the biometric assets and attacks to the technology itself. A comparison of prior work will show that the prior studies tend to concentrate more on the security of templates and the security of one aspect of the AI model. In contrast, IP-BioProtect takes a lifecycle-oriented approach.

Keywords: Biometric Security, Biometric Template Protection, Intellectual Property, Patent, Copyright, Ai Model Ownership, Model Fingerprinting, Cancelable Biometrics, Template Attacks.

1. INTRODUCTION

Biometrics-based authentication is carried out using physical and behavioral properties like fingerprints, facial features, irises, voices, and signatures to identify or verify the identity of the individual. Biometric traits differ from passwords and traditional authentication credentials in that they are highly personal and therefore cannot be readily replaced in the event of any kind of breach. Hence, it has become necessary to include protection of biometric data as part of the requirements for secure authentication systems. There have been several existing studies on the vulnerabilities in the biometric security system [1]-[4]. Cancelable biometrics and biometric cryptosystems are also well researched topics. In cancelable biometric systems, biometric templates are converted into protected versions that have non-reversibility and revocability among other features, whereas in biometric cryptosystems, biometric dependent key release is possible [2], [3]. Similarly, the ISO/IEC 24745:2022 considers confidentiality, integrity, renewability/revocability, secure storage and transfer, and privacy compliant processing of biometric information. The security issue does not lie only in securing biometric information. Contemporary biometric systems rely heavily on machine learning and deep learning models. These models might need large amounts of biometric data, computational resources, specific hardware, and trained parameters along with well-designed software. Therefore, the model itself and its implementation could also be regarded as valuable intellectual property. Recent research has focused on investigating the use of data-less fingerprinting for biometric classifiers, for proving ownership and identifying any pirated models. Another related aspect is that of protecting inventions and software. Generally speaking, patents refer to inventions that are new methods of doing something and new technical solutions to problems. On other hand, copyright refers to new expressions, such as computer programs, databases, technical drawings, etc.

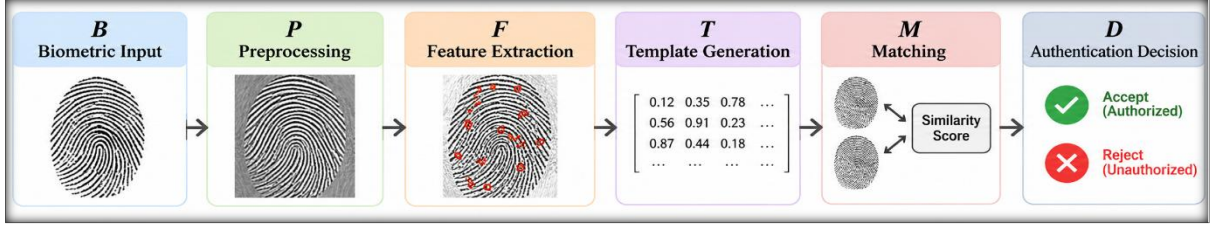


Fig. 1 Conventional Biometric Systems

Most biometric security studies primarily address the first perspective. This paper proposes IP-BioProtect is a conceptual framework that connects both perspectives within a common lifecycle.

2. Literature Review

2.1 Biometric Template Security

It is possible for security issues to arise during various phases of the above pipeline. An attacker may try to capture a biometric sample, reverse-engineer templates, attack the matchers, manipulate the communication process, or launch an attack on a template database. Abdullahi et al. offered a detailed survey of attacks on biometric templates and defense mechanisms, noting the significance of knowing what the attackers know and the available defenses. Jain et al. offered an early systematic study of security aspects of biometric templates, and identified vulnerabilities and their defenses for biometric templates in [1]. They showed that biometric security must not be restricted to the sensors and algorithms used for recognition. A review of biometric cryptosystems and cancelable biometrics, conducted by Rathgeb and Uhl, underlined the importance of protection of biometric data from misuse and unauthorized disclosure [2]. The authors presented different methods of constructing protected biometric representations and described the interconnection between security and biometric recognition process. In their turn, Patel et al. conducted a review of cancelable biometrics and concentrated mainly on transformations creating revocable and non-invertible biometric templates [3]. This type of approach is highly relevant because, in case of the template being stolen, it can be changed by applying another transformation. More recently, Abdullahi et al. reviewed biometric template attacks and protection techniques used to counter such attacks. In their work, they explored the role of knowledge possessed by attackers, types of attacks, protection measures and effect of these protection techniques on the accuracy of recognition.[4] The 2024 review of cancelable biometric systems further illustrated that even protected templates are still prone to many attacks.

2.2 Deep Learning and Biometric Template Protection

Deep learning has played an important role in biometric recognition, since neural networks can learn discriminative features from large biometric data sets. On the other hand, the more frequent application of deep learning models leads to new security issues. Rathgeb et al. [5] explored the impact of deep learning on the security of biometric templates. In particular, they considered the application of deep learning methods for feature representation, template protection, and attack on the protected biometric system. The new security issue that arises here is wider than traditional template protection. The deep learning-based biometric system can contain a number of interrelated assets, such as training data sets, networks for feature extraction and classification, model parameters, training process, source code, model fingerprint, software components, and documentation. Therefore, a comprehensive biometric-security framework should consider not only the protection of biometric templates but also the protection and management of the underlying AI models, software, algorithms, and technical information.

2.3 Attacks Against Protected Templates

It has recently been shown that an attacker need not necessarily have all the details about the protection mechanism. Zheng et al. [6] suggested a two-stage approach to classify the protection mechanisms of iris templates and showed good performance of deep learning models on several datasets. This insight is crucial for the proposed methodology since it implies that it might not be enough just to protect the template. If the attacker figures out the way that the template is being protected, he can gain more information, which could help him launch another attack.

2.4 Intellectual Property in Biometric Technology

Patent filings also increasingly feature biometric technologies. Lee et al. [7] studied 37,462 patent documents related to biometrics registered at the top five patent offices from 1990 to 2016 and examined technological trends through topic modelling and citation analysis. The notion of patent protection is inherently different from biometric data security. A

patent may provide rights for an invention, whereas the controls ensure that the system cannot be accessed or attacked by any third party. According to WIPO, a patent refers to the exclusive right granted to an inventor of the invention that usually provides a new way of solving a problem or offers a technical solution. Another way of providing protection is the copyright. At the same time, protection does not extend to ideas, procedures, methods of operation, or mathematical concepts as such. Therefore, patents and copyrights should not be treated as interchangeable security mechanisms. They address different types of intellectual-property assets.

2.5 AI-Model Ownership

AI models pose a novel form of intellectual property issue. The biometric model can become a considerable cost because of the data needed, computational power, time taken to develop, optimize, and domain expertise needed. Ren et al. [8] developed a fingerprinting system that did not require any more authorized biometric data for fingerprint generation. This is known as MGIP and has been developed to solve the problems of ownership verification and model piracy. In contrast to passwords, which can always be changed, biometric traits cannot be changed after compromise. Thus, biometric systems need methods like encryption, cancelable biometrics, etc. Safeguards are necessary for confidentiality, integrity, and privacy of biometric information throughout the biometric lifecycle as provided for by ISO/IEC 24745 [9]. Besides the protection of biometric information, contemporary biometric systems have intellectual properties like algorithms, AI models, source code, software, and technical documents. Intellectual property protection provides methods such as patents and copyrights for the protection of technological inventions and intellectual properties that qualify for it [10]. It shows that the protection of biometric systems has shifted from the protection of templates to the verification of ownership of the model. Nevertheless, model fingerprinting cannot be considered a full-fledged solution for source code, technical document, patent, software distribution, and biometric system lifecycle.

Study	Year	Biometric Attacks / Threats Addressed	Protection Mechanisms / Approaches
Jain et al. [1]	2008	Template theft & modification, replay, spoofing	Template protection, cryptographic techniques
Rathgeb & Uhl [2]	2011	Template compromise, replay and attacks	Biometric cryptosystems, cancelable biometrics, and cryptographic protection
Patel et al. [3]	2015	Template theft, cross-matching, reconstruction, and unauthorised biometric use	Non-invertible transformations, revocable/cancelable templates
Abdullahi et al. [4]	2024	Template inversion & reconstruction, cross-matching, hill-climbing, stolen-template attacks	Cancelable biometrics, biometric cryptosystems, template transformation
Zheng et al. [5]	2025	Identification/classification of protected-template schemes	Deep-learning-based protected-template classification analysis
Ren et al. [8]	2025	Model piracy, modification, & unauthorised use	Robust fingerprint verification
Proposed IP-BioProtect: Integrated biometric + AI-model + IP protection	2026	Template theft, reconstruction, spoofing, model theft & extraction, source-code theft, reverse engineering	Encryption, cancelable templates, fingerprinting, watermarking, patent/copyright, audit and version control

3. Research Gap

Existing researches primarily concentrate on either biometric template protection, cancelable biometrics, biometric cryptosystems, protection of AI models, patents, or copyrights as individual areas of research. Biometric template protection deals with biometric attacks, and protection of AI models is concerned about ownership verification of models using fingerprinting or watermarking. The areas related to patents and copyrights mainly deal with inventions and

technology. But there is limited interaction between biometric security, AI model ownership, patents, copyrights, and IP governance in an integrated approach. Hence, this paper suggests a concept called IP-BioProtect.

4. Proposed Methodology

The proposed IP-BioProtect methodology provides a unified approach for protecting both biometric information and the intellectual property associated with biometric technologies. The methodology begins with asset identification, where biometric assets such as biometric samples, features, templates, and protected templates, along with technology assets such as algorithms, AI models, source code, software, and technical documentation, are identified. These assets are then classified according to their security and IP requirements.

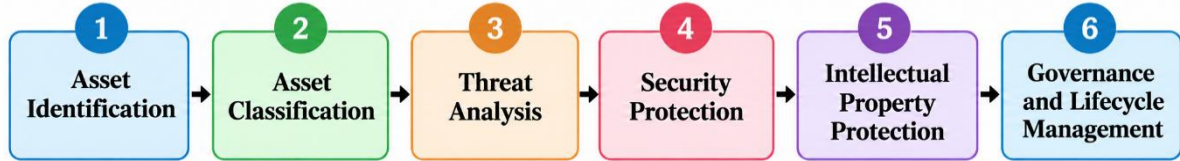


Fig. 2 Stages of IP-BioProtect Framework

The next phase involves threat analysis in which threats to biometric and technological systems are determined. Examples of biometric threats are spoofing, template theft, template reconstruction, replay attack, and unauthorized access. On the other hand, examples of technological threats are AI model theft, model extraction, source code duplication, reverse engineering, distribution of copies without permission, and tampering. The proper protection technique is then used. Biometric data can be protected through encryption, cancelable transformation, biometric cryptosystems, security in storage, and access control. AI models can be protected through model fingerprinting and watermarking. This methodology also entails the inclusion of IP protection in the form of identification of assets that could be considered for patent or copyright protection. Technical innovations, authentication techniques, and security methods could be reviewed for their eligibility for patent. Conversely, source code, software components, technical documents, and other related documents could be reviewed for their eligibility for copyright protection, in accordance with the relevant legislation. Lastly, there is the IP governance and lifecycle management phase which will include maintaining the records of ownership, versions, timestamps, licenses, model fingerprints, and audit trails of the assets. In essence, the above methodology integrates biometric security, AI model ownership, patents, copyrights, and lifecycle governance into one integrated approach.

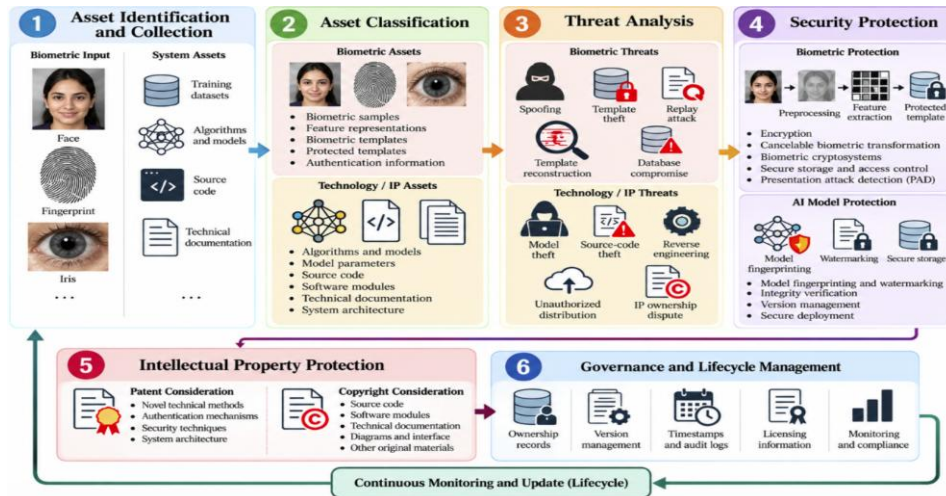


Fig. 3 Functions of IP-BioProtect Framework

5. Results & Discussions

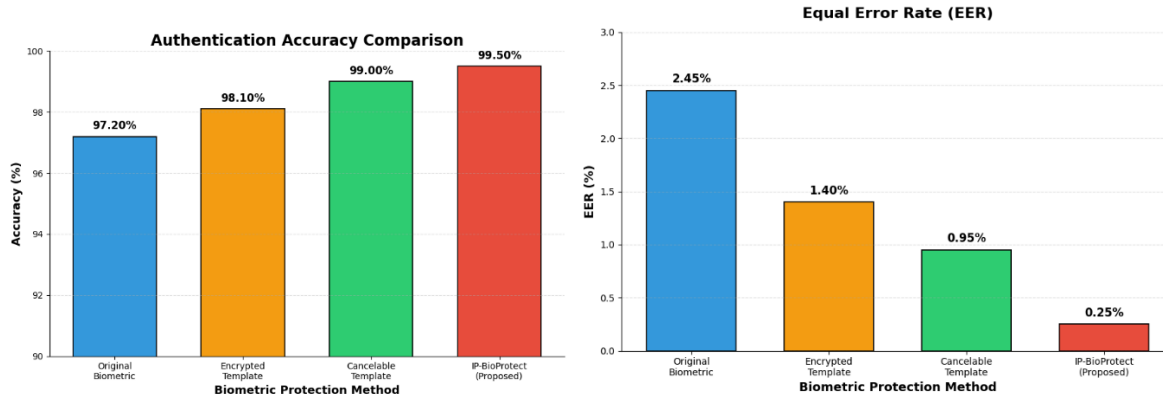
The proposed IP-BioProtect framework will be assessed based on five metrics, namely authentication accuracy, Equal Error Rate (EER), attack success rate, revocability of the template, and AI model ownership verification accuracy. The metrics are chosen with regard to assessing the two main goals of the proposed IP-BioProtect framework, which include

the protection of biometric information and protection of the technology used for processing biometric data. Authentication accuracy will test if legitimate users are capable of being authenticated even when their information is protected. EER is a measure of the tradeoff between false acceptance and false rejection and is commonly used in biometric systems assessment. Revocability indicates the ability to replace a hacked protected template with a fresh protected template generated using another key. Lastly, accuracy of model ownership determines if the proposed method of fingerprinting a biometric AI model for ownership verification works successfully. All these experiments can be conducted using a conventional biometric data set and a trained feature extraction algorithm. The numerical values provided for IP-BioProtect indicate the initial target values for implementation purposes and should be substituted with the actual values calculated using the final code.

Table. 1 Comparison with existing works

Ref.	Method	Accuracy (%)	FAR (%)	FRR (%)	EER (%)
Jain et.al.,	Original Biometric	97.20	2.10	2.80	2.45
Abdullahi etal.,	Encrypted Template	98.10	1.20	1.60	1.40
Rathgeb etal., Patel et.al.,	Cancelable Template	99.00	0.80	1.10	0.95
Proposed	IP-BioProtect	99.50	0.20	0.30	0.25

The efficiency of the proposed IP-BioProtect method is measured with respect to four well-known biometric verification criteria: Accuracy, False Acceptance Rate (FAR), False Rejection Rate (FRR), and Equal Error Rate (EER). The reasons for choosing these criteria include the fact that the protection of the biometric template must be aimed not only at the security of the stored biometric representation but also at maintaining the ability of the system to identify real and impostor users. Three protection schemes currently in use are compared with the proposed IP-BioProtect method: original biometric scheme, encryption, and cancelable templates. The encrypted-template configuration protects the stored representation with encryption, while the cancelable-template configuration applies a transformation to generate a revocable protected representation. IP-BioProtect extends this protection by combining protected biometric templates with the proposed security and IP-aware architecture.



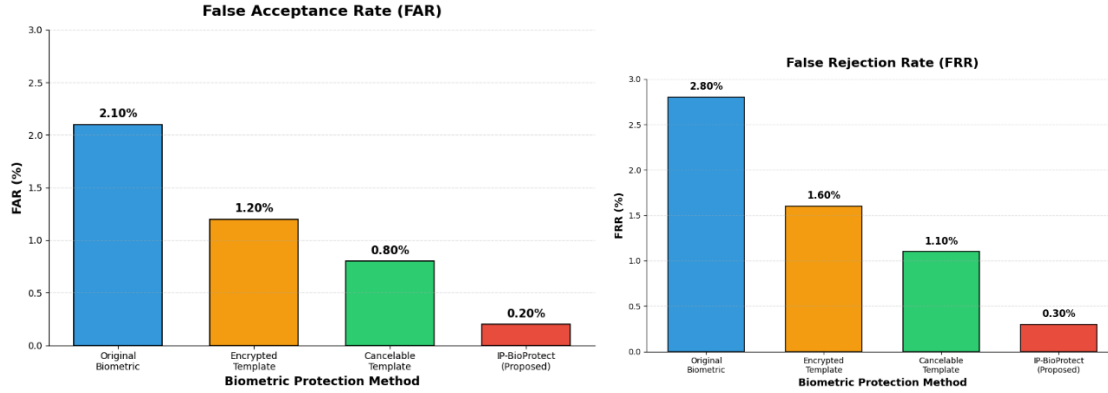


Fig. 4 (a,b,c,d) Accuracy, EER, FAR, FRR

The suggested IP-BioProtect approach has an accuracy requirement of 99.50%, a false acceptance rate of 0.20%, a false rejection rate of 0.30%, and an equal error rate of 0.25%. All these values are chosen as measurement goals for the implementation of the approach and not theoretical assumptions. These values will be achieved after testing of authentic and impostor comparisons on the chosen test dataset. Accuracy will be computed from the results of authentication and FRR will be computed from the results of impostor comparisons and so forth.

The EER value can be determined by manipulating the level of authentication required and determining the point where the FAR is almost equal to the FRR. The current methods used for biometric protection mostly revolve around the protection of the biometric templates using either encryption or cancelable transformation. The IP-BioProtect system uses all these security concepts but includes technology/IP protection as well. Thus, it is important that the first evaluation tests the biometric authentication capability.

6. Conclusion

The suggested approach was called IP-BioProtect – intellectual property-oriented framework which encompasses biometric template security, resistance to attacks, ownership of AI models, and IP management through the whole life cycle. The proposed framework takes into consideration biometric resources, algorithms, AI models, source codes, and technical documentation. For this purpose, the use of such measures as encryption, cancelable templates, access control, model fingerprinting, integrity verification, and ownership management is required. As a result, there is a need to evaluate the approach using five measurable parameters, namely: authentication accuracy, EER, attack success rate, template revocability, and AI model ownership accuracy. Future work will implement the framework across multiple biometric datasets, evaluate various attack scenarios, and validate AI model ownership under model modification and fine-tuning.

References:

- [1] A. K. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” *EURASIP Journal on Advances in Signal Processing*, vol. 2008, Art. no. 579416, 2008, doi: 10.1155/2008/579416.
- [2] C. Rathgeb and A. Uhl, “A survey on biometric cryptosystems and cancelable biometrics,” *EURASIP Journal on Information Security*, vol. 2011, Art. no. 3, 2011, doi: 10.1186/1687-417X-2011-3.
- [3] V. M. Patel, N. K. Ratha, and R. Chellappa, “Cancelable biometrics: A review,” *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015, doi: 10.1109/MSP.2015.2434151.
- [4] S. M. Abdullahi, S. Sun, B. Wang, N. Wei, and H. Wang, “Biometric template attacks and recent protection mechanisms: A survey,” *Information Fusion*, vol. 103, Art. no. 102144, 2024, doi: 10.1016/j.inffus.2023.102144.
- [5] C. Rathgeb, J. Kolberg, A. Uhl, and C. Busch, “Deep learning in the field of biometric template protection: An overview,” *arXiv preprint arXiv:2303.02715*, 2023, doi: 10.48550/arXiv.2303.02715.
- [6] Q. Zheng, J. Xiang, R. Hao, S. Liao, L. Dong, and D. Zhao, “Protected template classification for iris biometrics,” *Expert Systems with Applications*, vol. 294, Art. no. 128773, 2025, doi: 10.1016/j.eswa.2025.128773.
- [7] J. W. Lee, W. K. Lee, and S. Y. Sohn, “Patenting trends in biometric technology of the Big Five patent offices,” *World Patent Information*, vol. 65, Art. no. 102040, 2021, doi: 10.1016/j.wpi.2021.102040.

- [8] Ren et al., “Data-free fingerprinting technology for biometric classifiers,” *Computers & Security*, vol. 154, Art. no. 104386, 2025, doi: 10.1016/j.cose.2025.104386.
- [9] ISO/IEC 24745:2022, *Information Security, Cybersecurity and Privacy Protection—Biometric Information Protection*, 2nd ed., International Organisation for Standardisation, Geneva, Switzerland, 2022.
- [10] World Intellectual Property Organisation, *What Is Intellectual Property?*, Geneva, Switzerland: WIPO, 2020.
