International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 10 Special Issue: | Apr 2023 www.irjet.net p-ISSN: 2395-0072

International Conference on Recent Trends in Engineering & Technology- 2023 (ICRTET-3)
Organised by: VSM College of Engineering, Ramachandrapuram

Consolidating Biometrics and Cryptography for Enhanced Security

B.PRASANNA RANI[1], J SEKHAR[2] , P.RAMYA[3]

Assistant professor, Students B.Tech Computer Science Engineering, Assistantprofessor ,V.S.M College of Engineering, Ramachandrapuram, A.P, India

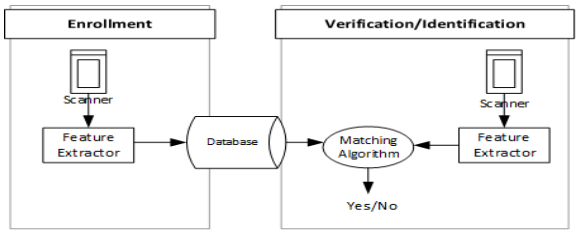
---

Abstract: The Need for Enhancing Information System Security through the Integration of Biometrics and Cryptography With the rapid advancements in information systems, ensuring the safety, integrity, and confidentiality of information has become more challenging. Despite the numerous benefits of technology, it has also introduced several security threats. Authentication, authorization, and accounting are crucial aspects of information security that require attention. Authentication, in particular, has been extensively studied, and biometric authentication is a recent method that has shown significant potential to enhance system security. However, biometric authentication alone may not always be entirely safe. This paper provides an overview of the various methods of integrating biometrics and cryptography to enhance information system security. The integration of cryptography has been shown to significantly improve access control mechanisms. The paper presents a two-way perspective on how biometrics can benefit from cryptography and vice versa. Specifically, the paper discusses how cryptography can utilize biometric data to generate more secure encryption keys that are harder to obtain or decipher. Additionally, the paper presents theoretical frameworks for measuring the performance of a biometric system, and current results on fuzzy vault techniques are surveyed and described. Overall, the paper highlights the need for integrating biometrics and cryptography to effectively secure information systems.

Index Terms: Biometrics, Cryptography, FuzzyVault

I. Introduction

In summary, this paper discusses the importance of ensuring the safety and security of information systems and the different approaches to achieving this, particularly through the integration of biometrics and cryptography. Biometrics involves using unique personal traits to authenticate users into a system, while cryptography involves altering messages to make them unreadable to unauthorized parties. The paper highlights the vulnerabilities of each approach, with key management being a major concern in cryptography and template protection being a major concern in biometrics. The paper goes on to analyze previous techniques in each of these areas and presents selected paradigms and algorithms for combining biometrics and cryptography. Finally, a performance evaluation is conducted on these paradigms and conclusions are drawn.



II. RELATED WORK

Great, let's start by analyzing previous research on biometrics in cryptography and vice versa separately.

A. Template Protection Using Cryptography

Template protection using cryptography is a crucial aspect of biometric security that involves safeguarding against confidentiality-related attacks during data storage or transmission. Simply encrypting the data with a symmetric encryption scheme is not a viable solution, as the output varies widely even when the input is similar. Shielding functions, such as δ-contracting functions, can solve the problem of noisy biometrics by using a constantvector and a biometric input vector to generate a secret key. At verification, if the difference between the new vector and the one used at enrollment is less than some δ, the contracting function returns the same value, which is compared with the one stored in the database. Cancelable biometrics is another popular technique that involves intentionally altering the

biometric using a mathematical transform, which makes it difficult for an attacker to obtain the initial data from the distorted one. Ratha et al. proposed three frequently used transformations for distorting biometric traits: cartesian, polar, and functional transformations. A recent study suggests that cancelable biometrics are less risky than encryption but are less safe than liveness detection techniques that can detect the authenticity of some biometric measurement to avoid spoofing attacks.

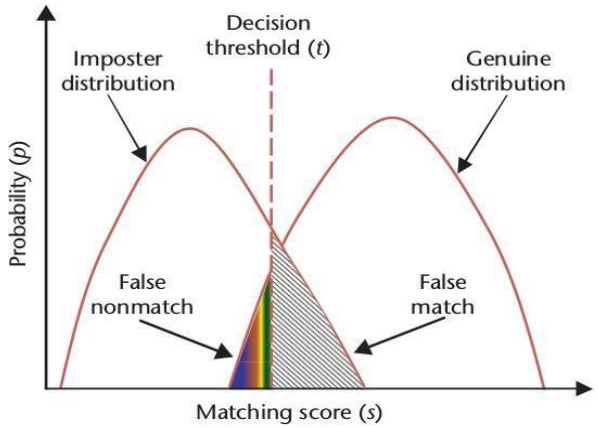
B. Enhanced Key Management Using Biometrics

Biometric cryptosystems are cryptographic systems that use biometric data to enhance their security level. They impact the first main algorithm of any cryptosystem, which is the keygeneration algorithm, by introducing biometrics to make the process of generating and managing secret keys more secure. There are two categories of securing secret keys with biometrics: biometric key-binding and biometric key-generation.

In biometric key-binding, a unique secret key is generated based on the biometrics provided at the time of enrollment. The key is stored in secured centralized databases together with the template data, but the combination is not simply stored in plain mode. Instead, some kind of undecipherable blending of the two is created. One popular key-binding scheme is called Biometric Encryption (BE), which was first introduced in 1996, and a more recent version is used for face recognition.

The Fuzzy Vault method is another method proposed for managing encryption keys inside biometric cryptosystems, which has gained probably the most popularity. The method basically chooses a codewordfrom the set of some error correcting code, and this can be perceived as the cryptographic key. At enrollment, the hash of this codeword and the difference between the biometric collected and the codeword is stored. At verification, some decoding function is used in order to obtain the new codeword. The hash of the obtained codeword is computed, and the condition for acceptance is that the hash of the initial codeword and the obtained codeword are equal.

In summary, biometric cryptosystems use biometric data to make the process of generating and managing secret keys more secure. They impact the first main algorithm of any cryptosystem, which is the key generation algorithm. Biometric key-binding and biometric key-generation are the two categories of securing secret keys with biometrics. The Fuzzy Vault method is a popular method proposed for managing encryption keys inside biometric cryptosystems.



II.PERFORMANCE EVALUATION

The passage discusses the theoretical basis of evaluating the performance of a biometric-based authenticating system. The false acceptance rate (FAR) and false reject rate (FRR) are two metrics used to evaluate the security level of the system. FAR represents the probability of the system to authenticate an intruder, while FRR represents the probability of failing to authenticate a legitimate user. Both FAR and FRR depend on the matching score and threshold values used in the system. The trade- off between security and convenience of the system is expressed through a 2D curve called the Receiver Operating Characteristic (ROC), which represents the trade-off between FAR and FRR. The closer the ROCis to the axes, the higher the quality of the system. The passage also briefly discusses some proposed fuzzy vault methods for biometric-based authentication.

Based on the information provided, it appears that thefuzzy vault method has been successfully applied to recognize both off-line and online signatures, as well as a variety of other biometric data such as fingerprints, palm prints, iris, and finger veins. The method involves gathering

discriminators points fromthe biometric data and using them to create a secure key.

The results show that the fuzzy vault algorithm can provide high levels of security, with a low FAR rate and low FRR rate. The best results were obtained when the iris was used as the method to authenticate.

Furthermore, combining multiple biometric data, such as fingerprint, iris, and finger vein, can lead to even better results in terms of FAR and FRR rates. The Hadamard and Reed-Solomon error correcting techniques developed by Hao et al. seem to be the most successful, with a FAR rate of 0 and an FRR smaller than 0.5. Overall, the fuzzy vault technique appears to be a promising method for secure biometric authentication.

IV. CONCLUSION

It is clear from the analysis presented in the paper that combining biometric and cryptographic techniques can lead to a significant improvement in the security of information systems. By using biometric data as a key or a password, the system can provide an additional layer of security that is much harder to breach than traditional password-based systems. However, it is important to note that biometric systems also have their own set of challenges and limitations, including issues related to privacy, accuracy, and spoofing attacks.

One of the most promising techniques for using biometric data in cryptographic systems is the fuzzy vault method. This method uses a mathematical framework to combine the biometric data with a secret key, producing an encrypted message that can only be decrypted using the same biometric data and key. Over the years, many studies have been conducted to evaluate the performance of fuzzy vaults, and the results have generally been quite promising. The technique has been applied to a wide range of biometric data types, including signatures, fingerprints, and iris scans, and has been shown to produce low rates of false acceptance and false rejection.

Overall, the paper provides a comprehensive overview of the state of the art in biometric and cryptographic techniques, as well as a detailed analysis of the fuzzy vault method. By presenting the theoretical basis for measuring the performance of biometric systems and highlighting the key challenges and solutions in this area, the paper offers valuable insights for researchers and practitioners alike.

V. REFERENCES

[1] Is Alice. Biometric recognition: Security and privacy concerns. IEEE Security & Privacy, 2003.

[2] Ruud M Bolle, Jonathan Connell, Sharath Pankanti, Nalini K Ratha, and Andrew W Senior. Guide to biometrics. Springer Science & Business Media, 2013.

[3] Brian Chen and Gregory W Wornell. Quantization index modulation: a class of provably good methodsfor digital watermarking and information embedding. IEEE Transactions on Information Theory, 47(4):1423–1443, 2001.

[4] Md Jahid Faruki, Ng Zhi Lun, and Syed Khaleel Ahmed. Handwritten signature verification: Online verification using a fuzzy inference system. In 2015 IEEE International Conference on Signal and Image Processing Applications (ICSIPA), pages 232–237. IEEE, 2015.

[5] Hao Feng and Chan Choong Wah. Private key generation from online handwritten signatures. Information Management & Computer Security, 10(4):159–164, 2002.

[6] Feng Hao, Ross Anderson, and John Daugman. Combining crypto with biometrics effectively. IEEE transactions on computers, 55(9):1081– 1088, 2006.

[7] Jesse Hartloff, Maxwell Bileschi, Sergey Tulyakov, Jimmy Dobler, Atri Rudra, and Venu Govindaraju. Security analysis for fingerprint fuzzy vaults. In Spie Defense, Security, and Sensing, pages 871204–871204. International Society for Optics and Photonics, 2013.

[8] Ari Juels and Madhu Sudan. A fuzzy vault scheme. Designs, Codes and Cryptography, 38(2):237–257, 2006.

[9] Kevin D Bowers, Ari. Juels and Alina Oprea, "HAIL: A High Availability and Integrity Layer for Cloud Storage", In the Proceedings of the 16th ACM Conference on Computer and Communications Security. ACM, pp. 187-198, 2009.

[10] Spillner J, Mller J and Schill A, "Creating Optimal Cloud Storage Systems", IEEE Transactions on Utility and Cloud Computing, vol. 29, issue. 4, pp. 1062-1072, June 2013.