cryptography

MDPI

Article

The Emerging Challenges of Wearable Biometric Cryptosystems

Khalid Al Ajlan [1,*], Tariq Alsboui [2], Omar Alshaikh [2], Isa Inuwa-Dute [2], Saad Khan [2] and Simon Parkinson [2]

[1] Royal Academy of Police, Ministry of Interior, Manama 33305, Bahrain
[2] Department of Computer Science, University of Huddersfield, Huddersfield HD1 3DH, UK; t.alsboui@hud.ac.uk (T.A.); omar.alshaikh@hud.ac.uk (O.A.); i.inuwa-dutse@hud.ac.uk (I.I.-D.); saad.khan@hud.ac.uk (S.K.); s.parkinson@hud.ac.uk (S.P.)
* Correspondence: u2187796@unimail.hud.ac.uk

Abstract: Cryptographic key generation and data encryption and decryption using wearable biometric technologies is an emerging research area with significant potential for authentication and communication security. The research area is rapidly developing, and a comprehensive review of recently published literature is necessary to establish emerging challenges. This research article aims to critically investigate and synthesize current research using biometric cryptosystems that use behavior or medico-chemical characteristics, ranging from gate analysis to gaze tracking. The study will summarize the state of knowledge, identify critical research gaps, and provide insight into promising future implications and applications that can enable the realization of user-specific and resilient solutions for authentication and secure communication demands.

Keywords: biometrics; cryptographic key generation; cancellable key; secure data transmission; wearable technologies

1. Introduction

In the digital age, cyber-attacks pose a serious risk to the confidentiality, availability, and integrity of sensitive data [1–3]. Robust and cutting-edge security techniques are required to counteract these cyber-attacks [4–6]. In recent years, cryptography has become an essential tool to protect communication and prevent unauthorized access to sensitive data [7]. The use of wearable biometric technologies to encrypt and decrypt data based on physiological or behavioural characteristics is a promising solution [8–10]. This is because the generation, management, and distribution of cryptographic keys present significant challenges when considering the increasing number of cyber-attacks. During secure data transmission, cryptographic keys protect confidential data from unintended access. Traditional key management methods are prone to cyber-attacks, and any weakness in generation and distribution can compromise security. The keys are generated with the help of complex algorithms and random number generators to maintain secure communication [11]. Although these methods are secure in theory, their implementation can be exploited by adversaries. Traditional key exchange mechanisms use digital channels that are susceptible to interception, manipulation, and impersonation, making the transmission of cryptographic keys risky.

In the field of cryptography, it is standard practice that knowledge of how encryption and decryption algorithms work is in the public domain. For example, the RSA algorithm is a form of encryption and decryption that uses public–private key pairs [12]. However, the effectiveness and dependability of cryptographic systems are highly dependent on the secrecy of the decryption keys. There are two distinct categories in cryptography: symmetric and asymmetric. Symmetric encryption uses the same key to encrypt and decrypt data, whereas asymmetric encryption uses two different keys for the same purpose. Weaknesses can exist in both approaches. For example, cryptographic key storage requires strong access control mechanisms [13], and key revocation is complex [14]. To increase

check for updates

Citation: Ajlan, K.A.; Alsboui, T.; Alshaikh, O.; Inuwa-Dute, I.; Khan, S.; Parkinson, S. The Emerging Challenges of Wearable Biometric Cryptosystems. *Cryptography* **2024**, *8*, 27. https://doi.org/10.3390/cryptography8030027

Academic Editors: Aleksandr Ometov and Joaquín Torres-Sospedra

Received: 16 April 2024
Revised: 19 June 2024
Accepted: 20 June 2024
Published: 21 June 2024

the security of a network, practical systems, such as the Transport Layer Security (TLS) protocol, use asymmetric key cryptography to transmit session keys securely. Subsequently, the session key is used in symmetric cryptography, allowing the security of interchangeable messages during the session [15]. In an increasingly interconnected world, the proliferation of devices and platforms complicates the security of vital information. Accessibility and security are difficult to balance with traditional methods of key administration. The distribution of secure keys is also challenging [16].

Key management approaches have long been in development. For example, both the widely used AES and RSA algorithms are in the public domain, and the security of encryption is based on the strength of the cryptographic key. If the key to cryptography is stolen or obtained by an unauthorized third party, the intruder can easily decrypt the ciphertext. Authentication in cryptography can be either knowledge-based (using something like a password, for instance) or token-based (using a smart card). In other words, a user is considered authentic if they possess either the secret key or the token and can access the confidential message. If the key is sufficiently large, such as the key of the AES algorithm (128, 162, or 256 bits), it will be challenging for users to memorize [17]. The alternative is for users to store it somewhere, for example, on a hardware token, a smart card, or on a computer with controlled access to the secret key using a different authentication system, for example, one that is password-based, which introduces a new layer of potential security risk. In addition, tokens or smart cards can be lost or stolen, and passwords can be guessed using dictionary attacks.

Wearable biometric technologies may provide a solution to the aforementioned cryptographic problems [18,19]. By integrating human physiological or behavioral characteristics with cryptographic processes, wearable biometric technologies could solve the challenges of key generation, management, and distribution [20]. Biometric characteristics such as fingerprints, iris patterns, and behavioral characteristics add security to the generation of cryptographic keys, making them difficult to replicate or impersonate [21]. In general, biometrics can be integrated into cryptography in one of three ways: key release, key binding, or key generation. Using the key release mode completely separates the key release mechanism from the biometric template matching process [22]. In the smart card, token, or computer where they are both stored, the biometric template and the cryptographic key are kept as separate entities. The biometric information that has been stored and the biometric information that has been requested are compared. The key will be released if the user's biometric characteristics are successfully matched. The biometric template is stored in crypto-biometric systems, even though they are once again vulnerable to attack.

Researchers have advocated the use of the user's biometric characteristics to manage cryptographic keys as an alternative to the procedures for key management described previously. According to a recent study [23], it is possible to accurately measure and identify a person based on their physiological or behavioral characteristics, which are considered biometric. Because of this, biometrics have the potential to distinguish between an authentic individual and a fraudulent impostor. Therefore, biometrics are being incorporated into cryptography to improve the security of more traditional forms of cryptography. As a result, numerous researchers are developing biometric-based cryptography (crypto-biometric) systems [24–27]. In these systems, biometrics ensure authentication, while conventional cryptography ensures information security. Traditional cryptography's authentication component has been replaced with biometric-based authentication to eliminate the need to memorize cryptographic keys without compromising the strength of the cryptographic key.

Techniques such as cancelable biometrics and cryptographic key binding are proposed to intrinsically link cryptographic keys to biometrics and handle issues such as biometric variance. Cancelable biometrics refers to the transformation of the original biometric template using one-way functions to create a distorted version [28,29]. This preserves user privacy, as the original template cannot be reconstructed. The cancelable template can also be renewed if compromised, providing revocability. Therefore, cancelable biometrics are designed to solve the problem in which biological characteristics cannot be cancelled or reissued. In cryptographic key binding, biometric characteristics are extracted and directly bound to a cryptographic key using techniques known as fuzzy commitment or fuzzy vault [30,31]. The key is intrinsically connected to biometric data but cannot be inverted to retrieve the original template. It is securely bound to the biometric template, which requires successful biometric authentication and direct access to the template for release. These binding techniques offer advantages, such as avoiding raw template storage. However, research challenges related to the handling of noise in biometrics, security analyses against emerging attacks, and the constraints posed by wearable devices continue to arise in the field of cybersecurity [32,33].

This research article provides a comprehensive investigation of the potential behind the use of wearable biometric technologies for the generation of secure cryptographic keys and the encryption or decryption of data. The analysis will synthesize and critically evaluate current research on techniques such as fuzzy commitment and cancelable biometrics that intrinsically bind cryptographic keys to biometric templates, evaluating strengths, limitations, and open challenges. Key focus areas will include handling biometric variance, optimization of wearable constraints, expansion beyond fixed modalities, formal security analysis against emerging attacks, and revocability mechanisms. To the best of our knowledge, there is an absence of studies with this specific focus. The main aim of this research is to critically investigate and synthesize current research on wearable biometric cryptosystems, identifying challenges and future implications for authentication and secure communications. In this work, the following list of objectives is investigated:

- Critically review intrinsic binding techniques, modalities, and algorithms proposed in the existing literature.
- Identify limitations and gaps with respect to the direct implementation of wearables.
- Analyze security, accuracy, revocability, privacy protections, and wearable constraints.
- Recommend grouped techniques and optimized combinations tailored for wearable devices.
- Highlight promising research avenues that can address gaps through specific implementations.
- Summarize the findings and limitations to progress from conceptual research to deployable wearable biometric cryptosystems.
- Highlight promising research avenues that can address gaps through specific implementations tailored for wearable devices and constraints.
- Summarize the findings of the current state, limitations, and future directions to progress from conceptual research to deployable wearable biometric cryptosystems.

The article provides a significant and innovative contribution to the field of cybersecurity. It addresses the critical and complex issue of cryptographic key generation, management, and distribution in the context of wearable biometric technologies. The novelty of the research lies in its comprehensive review of current literature and the synthesis of knowledge to identify gaps and future implications in biometric cryptosystems. By focusing on user-specific, resilient solutions for authentication and secure communications, the article paves the way for developing more robust security systems that integrate human physiological or behavioral characteristics with cryptographic processes. This approach is particularly relevant in an era where cyberattacks pose a serious risk to data confidentiality and integrity, making the research both timely and crucial for advancing security measures in wearable technology applications.

The article provides the two following major contributions:

- It provides a comprehensive review into current research on wearable biometric cryptosystems.
- It identifies key research challenges, offering insight into promising future implications and applications.

The paper is structured as follows: in Section 2, the methodology followed in performing this survey is presented. The main literature review is presented in Section 3, followed by a discussion of key identified works in Section 4, which includes a summary of key challenges. Finally, the conclusion is presented in Section 5, which also briefly presents future work.

2. Methodology

As previously established, multi-user cryptography requires dedicated key management systems [34,35]. However, there are many fundamental challenges with key generation and management. For example, developing mechanisms in which the key can be revoked [36], maintaining confidentiality [37,38], handling noise and incompleteness [39], and biometric information should not be invertible from the key [40].

In recent years, many pertinent studies have been published in the area of the use of biometrics in cryptosystems. These start from influential work published by Uludag et al. (2002) [41] to recent and highly relevant studies in 2023 [42,43]. However, to the best of the authors' knowledge, there are no surveys seeking to understand the role of wearable biometric cryptosystems. There are many key works investigating the use of wearable biometrics in security applications [10], user authentication [44], and real-life integration [45]. However, these works do not provide detailed information on how wearable biometrics can be used in cryptosystems. Considering the increasing update of wearable biometrics and the pervasive use of cryptosystems, it is necessary to gain an understanding of how they can work together and what challenges need addressing. The timing is critical to ensure that current and future works in this field are adequately informed and aligned.

The aim is to critically investigate and synthesize current research using wearable biometric technologies for the generation of cryptographic keys. The scope of this review of the literature focuses on the analysis of existing techniques that intrinsically bind cryptographic keys to biometric templates captured via wearable devices. It synthesizes studies on the use of voice, sleep patterns, gait dynamics, and other wearable modalities for cryptographic key generation in terms of encryption or decryption. The review specifically assesses the strengths, limitations, and challenges surrounding security, including accuracy, revocability, privacy, wearable constraints, and large-scale testing.

A systematic approach has been adopted to carry out this research. This was carried out by investigating the use of wearable biometric technologies for cryptographic key generation and encryption or decryption. The review focuses on viability, security, privacy, challenges, and future directions. The choice of reputable academic journal articles has been carefully carried out to support the thesis and published studies. Academic databases such as IEEE Xplore, ACM Digital Library, ScienceDirect, Scopus, and Google Scholar were also used. A search strategy was developed to retrieve relevant studies, including a search string with the following keyword search string for Google Scholar "wearable" AND "biometrics" AND "cryptography" AND "key generation" OR "encryption" OR "cancelable templates" and more. Figure 1 shows a taxonomy of all biometrics that can be used as wearable biometrics. The figure is based on previously published surveys on biometric modalities and was also used as a guide in this survey to perform a systematic literature search. This was created based on influential prior works [10,44,46] and example individual works discovered for each type, as cited in the illustration. Identified papers were screened to ensure that they have been peer-reviewed and published within the last 10 years. The excluded criteria include articles that have not been peer-reviewed, papers published in languages other than English, or white papers or presentations. The full texts of selected studies underwent a thorough content analysis to extract relevant data on techniques, modalities, security evaluations, wearable devices, limitations, and more. Studies were critically assessed before key themes and knowledge gaps were identified through thematic analysis. The findings are structured around topics such as binding mechanisms, revocability, wearable constraints, privacy preservation, and others. The conclusion was formulated to summarize the current state of knowledge, the limitations of the existing literature, and potential future research avenues to address gaps based on systematic analysis. In this article, a total of 1760 articles were identified using the search criteria, and after applying exclusion criteria, 78 were reviewed and kept as part of this study.

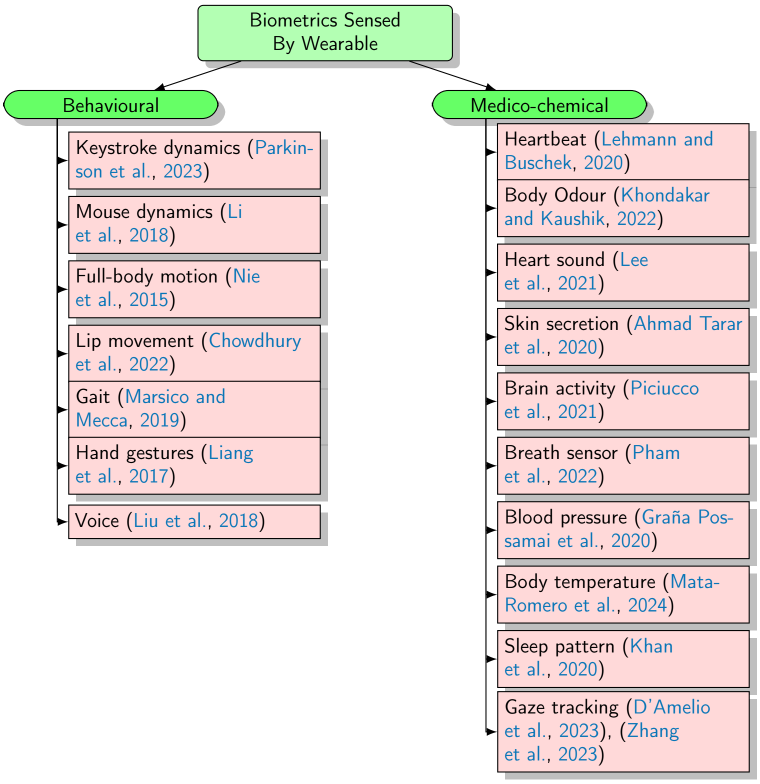
Biometrics Sensed By Wearable
Behavioural
Keystroke dynamics (Parkinson et al., 2023)
Mouse dynamics (Li et al., 2018)
Full-body motion (Nie et al., 2015)
Lip movement (Chowdhury et al., 2022)
Gait (Marsico and Mecca, 2019)
Hand gestures (Liang et al., 2017)
Voice (Liu et al., 2018)
Medico-chemical
Heartbeat (Lehmann and Buschek, 2020)
Body Odour (Khondakar and Kaushik, 2022)
Heart sound (Lee et al., 2021)
Skin secretion (Ahmad Tarar et al., 2020)
Brain activity (Piciucco et al., 2021)
Breath sensor (Pham et al., 2022)
Blood pressure (Graña Possamai et al., 2020)
Body temperature (Mata-Romero et al., 2024)
Sleep pattern (Khan et al., 2020)
Gaze tracking (D'Amelio et al., 2023), (Zhang et al., 2023)

Figure 1. List of all biometric types to guide the literature search for biometrics. The following surveys were influential in identifying applicable biometrics [10,33,44–62].

3. Review

In recent years, there has been increasing research interest in the use of biometric characteristics to improve the security of cryptosystems [43,63]. These attributes consist of fingerprints, iris scans, and facial recognition. Unlike conventional passwords, which can easily be cracked or stolen, biometric characteristics are unique to each individual and cannot be easily replicated [33,64]. In a recent study [65], biometric characteristics were incorporated into a variety of construction strategies. They discovered that such incorporation can increase the resistance of cryptographic systems to intrusion attempts; however, they also identified that creating a suitable biometric encryption key is the most challenging aspect of biometric encryption.

Several strategies have been proposed to address key challenges in biometric systems, including increasing the randomness of iris codes, adding synthetic points to real biometric points, employing biometric images rather than direct features, and storing parameters representing wearable characteristics. However, each of these strategies has its advantages and disadvantages, which means that there is no clear approach that is most suitable for adoption [43]. To address this issue, researchers have proposed the use of multimodal biometrics to overcome challenges such as the resistance of cryptosystems to attacks. For instance, voice biometric characteristics have been demonstrated to be useful for single- and multi-factor biometric cryptosystems due to the impossibility of guessing their values. Using biometric speech signals, it is possible to generate random encryption keys with a high level of entropy and resistance to hacking that can then be used to extract various properties for use in encryption applications [66].

To create cryptographic keys using biometric information, the work incorporates biometric features, cryptography, and numerous data concealment techniques. Few published works have successfully addressed each of the aforementioned concerns; however, several works have already been published that address individual concerns. Despite the numerous methods that have been developed and tested to determine their level of safety, there is no formal study that provides a comprehensive examination of all available approaches. In conclusion, the incorporation of biometric characteristics into cryptographic protocols has the potential to significantly strengthen the overall level of security of the system. However, additional research is necessary to develop efficient methods to incorporate biometric characteristics into encryption keys and to evaluate the level of security provided by these methods.

In this literature review, the discussion of identified works has been classified into the following five subsections: (1) cryptographic key generation using biometrics, (2) cancelable templates in biometrics, (3) cryptographic key binding techniques, (4) encryption and decryption during data transmission, and (5) cryptographic biometric key generation using wearable technologies. In the remainder of this section, a detailed survey of related work in each category is provided.

3.1. Cryptographic Key Generation Using Biometrics

Recent studies have proposed various techniques to generate cryptographic keys from biometric modalities such as face, fingerprint, and EEG signals [67–70]. These techniques typically involve extracting features from biometric data using methods such as PCA, Gabor filters, ICA, or deep CNNs. Biometric features are then used to generate keys through techniques such as aligning minutiae points, Diffie–Hellman exchange, or XOR operations. The reported key sizes range from 140 to 1024 bits. Matching algorithms include minutiae matching, key matching, and threshold-based matching. Some schemes allow for the renewal of compromised keys through revocation or by changing parameters. The key strengths of biometric cryptosystems include strong encryption, high randomness, irreversibility, and renewalability. However, limitations such as slower authentication, high error rates, and trade-offs between security and usability have also been reported. Overall, biometric cryptosystem key generation shows promising outcomes, but further research is required to optimize its security, accuracy, and usability. Another similar work [71] presents a system for cryptographic key generation using EEG signals. In contrast to existing studies, the developed approach uses raw EEG data without feature extraction, generating covariance matrices and geometric mean. Cryptographic keys are generated from user samples without changing the system configuration. The evaluation using publicly available datasets shows a high genuine acceptance rate (GAR).

A study [72] proposed a fingerprint biometrics-based key generation approach using minutiae distances and a two-layer error correction technique. Their method quantized the relative distances between the minutiae into bit strings for key generation rather than exposing the fingerprint templates. Experiments in real fingerprint databases showed high key regeneration rates of up to 99.73%, robust fault tolerance, and security against brute-force attacks. However, the challenges with fingerprint extraction, limited security analysis, and fixed key sizes were key limitations. Another study [73] developed a framework for generating cryptographic keys from facial biometrics. They proposed equalized local binary patterns (ELBP) for robust facial feature extraction and a three-bit quantization technique to handle variations. Their approach did not require storing templates or keys, which mitigated challenges associated with key storage. Simulation studies demonstrated high recognition rates on standard face data sets. Statistical tests also showed strong randomness, security, and privacy for the generated keys, but they had slightly lower accuracy compared to deep learning methods, which was a trade-off. Another work [74] proposed an asymmetric cryptosystem using fingerprint biometrics and phase retrieval algorithms. Optically generated fingerprint keys were used for encryption and decryption, along with random phase masks. This technique intrinsically links keys to biometrics for added security. The results show accurate decryption and resilience against different attacks initiated by unauthorized users. However, security analyses were limited, and the revocability of biometric keys was not addressed. Another study [75] proposed the generation of cryptographic keys using biometric data. It used deep learning models to extract biometric features from facial images [76] and code-based cryptographic extractors to process the extracted facial features. The optimized algorithm parameters yielded a lower error rate, making the keys suitable for biometric authentication.

An article reviewed various biometric template protection schemes, including key binding techniques such as fuzzy commitment and fuzzy vault [77]. This intrinsically bound the keys to the biometrics using error correction to handle biometric variance. They noted research gaps regarding resilience against sophisticated attacks. However, it is important to note that the paper did not offer an extensive quantitative security analysis of the various biometric cryptographic techniques. Another article [78] proposed a novel two-factor authentication (2FA) approach by combining fingerprints and passwords to generate stable RSA key pairs without storing private keys. Their method encoded minutiae distances in grey code instead of binary code to minimize key-string mismatches from biometric variance. Reed–Solomon coding then corrected errors for consistent key regeneration. It should be noted that the use of 2FA improves security over biometrics alone. Both studies demonstrate that the intrinsic linking of cryptographic keys with biometrics provides security benefits over traditional methods. The security assessments of biometric cryptographic techniques are limited, with a lack of rigorous cryptanalysis and evaluations against sophisticated attacks. More comprehensive security evaluations involving mathematical proofs, cryptanalysis, and testing against various attack scenarios would strengthen security claims. The use of 2FA further strengthens security and differentiates their approach. These studies reveal that biometrics holds promise for robust key generation. However, focused research is still needed on customized techniques that utilize suitable wearable modalities and cancelable templates that preserve privacy and formally assess security against sophisticated attacks such as reconstruction, spoofing, and usability optimization.

In another recent study, a novel approach was proposed to generate a symmetric cryptographic key using cancelable fingerprint templates of both the sender and the receiver [38]. Their approach transformed original fingerprint templates into cancelable templates using a one-way, non-invertible function. This preserved the privacy of the fingerprint. The cancelable templates were then securely exchanged between parties. A master template was created when the two templates were merged. Finally, a 128-bit cryptographic key was derived from this master template. A key finding worth noting in such a study was that linking the cryptographic key with the unique biometrics of both users improves security and intrinsically binds the key to the identities of the users. It eliminates the key storage and distribution challenges of traditional cryptography. The use of cancelable templates also enables template renewal if compromised. However, the security analysis presented in this study has some key limitations, as it does not thoroughly evaluate resilience against attacks. In addition, the approach focuses primarily on fingerprint biometrics and symmetric key generation. This research highlights the potential of biometrics to improve systems by establishing a direct connection between keys and users. However, more research is required to explore the applicability of techniques to the modalities to conduct a formal assessment of security measures and extend their implementation to asymmetric cryptography.

Two studies by Sarkar et al. (2018) [77] and Salman et al. (2020) [79] proposed methods to generate cryptographic keys from biometric data using techniques such as fingerprint minutiae and multibiometrics. Sarkar focused on generating asymmetric keys for the ElGamal cryptosystem using cancelable fingerprint templates. They extracted minutiae points from fingerprints, shuffled the coordinate vectors, XORed them to obtain a cancelable template, extracted 1024 bits, and used this to generate a large prime number as the private key. Their method aimed to intrinsically link keys to the user's biometric characteristics while preserving fingerprint privacy through cancelable templates. However, they did not provide a comprehensive security analysis. Salman also extracted features from multi-modal biometrics (eye and ear) and used the meerkat clan algorithm, a swarm intelligence technique, to generate symmetric cryptographic keys. Their results showed that the eye features generated more random keys than the ear features. Their approach produced strong and unique keys efficiently. However, again, the security analysis was limited; only a small dataset was used. Both studies highlight the potential of biometrics to link keys to users to enhance security and avoid problems such as forgotten passwords. However, there are limitations regarding formal security evaluations, handling noisy data, revocability of compromised biometrics, and testing on larger samples. There is also a lack of research on techniques optimized specifically for wearable devices and modalities such as electrocardiograms.

Biometrics offer a strong security advantage by inherently associating keys with their users. Techniques such as fuzzy commitment in biometric binding provide the additional benefit of revocability and eliminate the need to store raw templates [21]. The combination of biometrics with passwords or tokens improves security through multi-factor authentication [32]. However, the challenge lies in the variability of biometrics, making it difficult to consistently generate keys [80], as well as the lack of in-depth security analysis against advanced threats [68,78]. Furthermore, reliance on specific modalities such as fingerprints or ECGs limits its applicability [81]. To enhance the generation of the biometric cryptographic key, researchers should explore techniques such as quantization, grey coding, or error correction codes to extract stable keys from noisy biometric signals [68], introduce cancelable biometrics to enable template renewal in case of compromise [78], and consider emerging wearable-friendly modalities such as EEGs, EMGs, skin conductance to overcome limitations associated with specific modalities [81].

3.2. Cancelable Templates in Biometrics

According to a recent study [82], cancelable templates ensure security and inherent revocability. They create a problem when a person uses the same biometric for multiple applications. A person can only possess a limited number of biometric characteristics; if one application is compromised, all applications will be compromised. This is due to the inability to alter or delete a specific biometric characteristic. A secured biometric system uses cancelable biometrics to mitigate the effects of this problem. Cancelable biometric techniques can store and employ biometric information to protect against attackers. A recent study [83] presented a comprehensive benchmark of several cancelable biometric systems. Their experiments show that all the evaluated cancelable biometric schemes achieve high recognition performance, close to perfect unlinkability, but varying irreversibility, demonstrating their usefulness.

The generation and protection of large cryptographic keys is one of the most significant challenges posed by traditional cryptography. The keys are not directly associated with the user, so it can be challenging to memorize them. To solve this problem, a study [28] proposed a method to generate symmetric cryptographic keys that make use of cancelable biometric templates of the individual. This method binds the cryptographic key to the user's unique biometric characteristics. The key is generated using the biometric templates of both the sender and the recipient, which are located in their respective locations. Since the cryptographic key is generated dynamically for each communication session, the owner does not need to memorize it, instead of having to memorize it or find a safe place to store it. Biometric templates that can be canceled are used to protect the biometric identities and confidentiality of users. Because the original biometric template is transformed in a way that only goes in one direction when creating these templates, it is not possible to revert to the original template once the cancelable template has been used. This makes it possible to easily revoke the use of compromised cancelable biometrics and replace them with new ones. Using cancelable biometric templates, this solution provides an approach that is both secure and straightforward to implement for the generation of symmetric cryptographic keys. In addition, this method eliminates the problems associated with key storage and distribution that conventional cryptography faces. This is accomplished by linking the cryptographic key to the user's biometric characteristics.

Using cancelable biometrics allows for the protection of biometric templates. Cancelable biometrics is a method used to protect biometric templates by generating an irreversible and renewable identifier using transformation functions such as a hash and user-specific parameters such as a password or token [84]. Authentication requires the inclusion of user-specific parameters and biometric images. Therefore, it is necessary to employ a method that requires authentication from two distinct sources. On the contrary, the use of a user-specific parameter directly contradicts the assumption that biometric systems are independent of memory and ownership. Consequently, biometric encryption systems must allow one factor to be canceled. Indexing-first-order hashing (IFO hashing) [85] is a potential biometric technique that can be canceled with a single factor. IFO is a precise, non-invertible, renewable, and non-linkable one-factor locality-sensing hash function. It is used primarily to protect templates.

This paper presents a biometric-based medical image encryption technique that can be canceled across multiple modalities. Using the unique characteristics of biometrics while preserving the secrecy of biometric characteristics, IFO hashing and AES-CBC are essential for the system's security. Alternative algorithms for the generation of biometric templates could be substituted for the current method to speed up the process. The use of loss-less compression schemes, such as UNIX compress, has been suggested as a way to improve the security of the scheme [86]. Alternatively, the second round of AES-CBC could be replaced with AES-CCM, which offers the benefit of incorporating inherent authentication capabilities. In the final step, the cancelable template is generated by calculating the distance and sorting the resulting data. Consequently, this procedure involves calculating the distance between the points using an appropriate distance metric and then arranging the results in a predetermined order, thereby creating the cancelable template [87]. This transformation is secure against an invertible attack by the model, but the use of the same transformation function does not reveal the revocability of biometrics.

Another paper [88] presents a cancelable biometric authentication system using a combination of the hyperchaotic technique and the Fibonacci Q matrix. The system was validated through authentication and security measurements. Five biometric patterns were tested, providing high authentication performance, high entropy, NPCR, and UACI values, and protection against several attacks. Cancelable biometrics are primarily based on digital (soft) templates. An interesting paper [89] proposes cancelable biometrics with physical template (CanBiPT), which uses a printed sticker to wear in a specific region of the face. The sticker generates an image with an individual's features, which are used for authentication and recognition. Different physical templates can be formed by changing regions or appearance. The method's feasibility and effectiveness are demonstrated through public dataset experiments.

Cancelable templates in biometrics offer enhanced privacy through one-way transformations [28], provide the valuable features of renewability and revocability in the event of compromise, while avoiding the need to store raw templates by binding [85]. However, these benefits are often limited to specific modalities such as fingerprints, and there is a scarcity of extensive large-scale tests, highlighting the necessity of security evaluations against advanced attacks [90].

To enhance cancelable templates in biometrics, researchers should broaden their applications of modalities such as voice, iris scans, and ECG signals beyond fingerprints, conduct testing on more extensive proprietary and public biometric datasets while assessing consistency and accuracy across diverse samples, perform formal analyses against common attacks, including brute force and spoofing, and engage in cryptanalysis to validate the strength of cryptographic systems.

3.3. Cryptographic Key Binding Techniques

A study [90] proposed an innovative iris-based binding scheme that relied on a technique known as indexing-first-order hashing. In simple terms, this technique transforms biometric templates (such as iris scans) into cancelable forms. In the case of indexing-first-order hashing, this transformation promotes the encoding of bits in cryptographic keys. What is particularly noteworthy about this approach is its ability to achieve high key regeneration rates without relying on error-correcting codes, which can impose restrictions on key size. However, it is important to note that this method presented minimal security analysis and that the issue of revocability in the case of compromised biometrics was not thoroughly addressed. Another study [91] introduced objective functions to bind keys to iris and fingerprint data by minimizing functions to create helper data to aid in retrieval. The analysis of benchmark data sets demonstrated high genuine acceptance rates and low false acceptance for keys up to 2048 bits despite the existing noise in biometric data. Furthermore, security evaluations exhibited robustness against brute-force and correlation attacks. However, a limitation was handling biometric variance and developing specialised techniques optimized for wearable technologies.

Another study [92] introduced a cancelable biometrics vault framework that incorporates a technique called BioEncoding to bind cryptographic keys. BioEncoding is a cryptographic method that involves encoding biometric data in a way that maintains accuracy while enhancing security. In this context, it is applied to the binding of keys to biometric information. The framework also incorporates chaffing and winnowing principles, which are cryptographic techniques aimed at confusing potential attackers. One notable advantage of this system is its ability to maintain high accuracy regardless of key size, unlike systems that are constrained by the capabilities of error correction codes. Furthermore, the system demonstrates robustness against privacy leakage attacks, making it computationally infeasible to reconstruct biometric data. However, it is essential to note that relying on the specific BioEncoding scheme could limit its wider applicability. A key advantage is maintaining high accuracy regardless of key size, unlike systems bound by error-correcting code capabilities. The system also shows robustness to privacy leakage attacks with computational infeasibility to reconstruct biometrics. However, relying on the specific BioEncoding scheme could constrain its wider applicability.

Another study [21] proposed a novel hybrid optimization approach using deer hunting and chicken swarm algorithms to select the optimal iris characteristics to bind symmetric keys. Their method showed higher accuracy than other whale and grey wolf optimization algorithms. The study aimed to securely bind secret keys to user characteristics extracted from iris biometric data. Gabor filters encoded iris features, which were optimized using hybrid algorithms to identify optimal features for key binding. These were used to train a neural network for user authentication. RSA encryption bound the keys to optimal features through XOR operation. Experiments with different key lengths demonstrated the proposed model's accuracy: higher than whale and grey wolf optimization, respectively. The study further stated that combining optimization techniques improved results in metrics such as specificity, precision, and FDR versus without optimization and individual algorithms. However, security analysis was limited as the binding technique focused only on iris biometrics and symmetric keys. Biometric variance, special wearable techniques, privacy preservation, and resilience against sophisticated attacks were not addressed. The study revealed the potential of novel nature-inspired hybrid algorithms to extract optimal biometric features for robust cryptographic key binding. However, there are significant research gaps regarding formal security evaluations, revocability, noise handling, and the development of customizable techniques for diverse applications such as wearables. Also, a recent survey article [93] reviewed various biometric-based cryptography key-binding techniques (e.g., using fingerprint and iris images) to determine their limitations. The main issue found was the large key size, which reduces the performance of the system.

According to another study [94], cryptographic key binding is an essential biometric security concept. It is essential to ensure secure data transfer between wearable technologies. The linking of cryptographic keys with unique biometric data is the most fundamental aspect of cryptographic key binding [91]. Examples include fingerprints, facial characteristics, and iris patterns. This binding process enhances security by establishing a strong link between an individual's physiological or behavioral characteristics and the cryptographic keys used for data encryption and decryption during transmission. These keys are used for encryption and decryption during data transmission. Through the establishment of this link, it is possible to significantly improve both the integrity of biometric data and the confidentiality of transmitted data [95].

The key binding process is based on varying methodologies and rules. In the first step, known as biometric feature extraction, unique characteristics are extracted from raw biometric data [96]. After transforming these features into numerical representations known as feature vectors, which serve as the basis for subsequent cryptographic key derivation [97], subsequent cryptographic key derivation is possible. To convert these feature vectors into cryptographic keys, one-way functions that are frequently implemented using cryptographic hash functions are used [94,98]. This transformation is designed to be irreversible. Therefore, the original biometric information cannot be reconstructed using the generated keys.

According to another study [99], the generation of session-specific keys increases security by associating each data transfer session with a unique key. This provides additional protection. Although cryptographic key binding offers numerous advantages, it also raises many challenges and concerns that must be considered. Robustness is an essential aspect of binding techniques because of their ability to withstand attacks and other forms of attempted manipulation. Different biometric features require specialized approaches to successfully bind keys [30]. Compatibility is an additional issue that must be addressed [94,100].

There are numerous advantages to using cryptographic key binding. This method increases security by tightly coupling biometric characteristics with cryptographic keys. Consequently, the technique reduces the likelihood of successful traditional standard attacks, such as password cracking. However, the system has some limitations and weak points. The accuracy of binding can be affected by forged or noisy biometric data, and it remains challenging to find a balance between usability and security [91]. Case studies based on the real world and research findings [101] further illustrate the applicability of cryptographic key binding. These studies illustrate the incorporation of the binding technique into a variety of applications and scenarios that involve wearable technologies, highlighting the importance of the technique in ensuring the secure transfer of data.

In comparison to other approaches to key generation and binding, cryptographic key binding is an industry leader. Its reliance on biometric characteristics provides a higher level of security than conventional methods that rely on passwords [102]. Its unique advantages should be carefully considered when evaluating its suitability for various contexts. As the field evolves, there are several emerging trends and challenges to consider. Multimodal biometrics and dynamic binding are two emerging potential trends with the possibility of shaping the future of cryptographic key binding [103]. However, some research obstacles remain, including the need to make the system more resistant to sophisticated attacks and further improve the usability of the binding procedure [104]. According to a study [105], cryptographic key binding techniques are essential to ensure the security of data transmission between various wearable technologies. By binding cryptographic keys to unique biometric data, this method ensures a strong link between a person's characteristics and their cryptographic keys. As a result, it increases the level of security and privacy in wearable technology-based data communication [106].

Cryptographic key binding techniques offer the advantage of tightly linking keys with biometrics, an inherent association that enhances security [91]. Furthermore, they maintain accuracy regardless of key size, distinguishing them from ECC-based methods [92], and hybrid optimization techniques improve the selection of biometric features [21]. However, their applicability depends on specific algorithms, such as BioEncoding [92]. Their robustness against attacks and biometric variations also requires validation [91]. Additionally, these techniques are mainly applied to single modalities, such as iris scans [21]. To improve cryptographic key binding techniques, researchers should work on generalizing these methods to make them independent of particular algorithms and capable of accommodating diverse binding techniques [92]. Developing flexible frameworks that can incorporate various binding techniques is crucial [92], exploring multimodal approaches that fuse multiple biometrics and customising algorithms to suit different wear-friendly modalities [21].

3.4. Lightweight Encryption and Decryption

A critical aspect of developing robust wearable biometric cryptosystems is identifying algorithms that provide strong security while maintaining the speed and security of wearable technologies. This section reviews existing encryption techniques for secure data transmission to determine the most appropriate solutions that can be integrated into the biometric key generation methods for wearables documented earlier. By analyzing the strengths and weaknesses of current encryption approaches, this section aims to determine the most promising technique that can be tailored and combined with wearable biometrics to deliver optimized confidentiality assurances for data communication. Table 1 provides summary information on the papers discussed in this section.

Several studies have investigated encryption and decryption techniques to ensure secure data transmission and prevent unauthorized access to sensitive information. A study [107] proposed a hybrid cryptography approach that combined AES, DES, and RSA encryption to provide multilayered security for files stored in the cloud. Their method divides a file into three segments, each encrypted with a different algorithm, and hides the keys in an image via least significant bit (LSB) steganography. Their results show improved security against brute-force attacks compared to single encryption methods. However, the increased complexity requires more computational resources. Several studies examined the integration of symmetric and asymmetric cryptographic algorithms to leverage their respective strengths. Another study [108] developed a hybrid AES–RSA algorithm that was faster and provided better performance than AES or RSA alone, demonstrating the performance benefits of a hybrid approach to network security. Another work [109] implemented a double encryption technique using sequential AES and RSA algorithms for cloud storage. This multilayered encryption improved security while maintaining efficient performance for encryption decryption and ciphertext sizes.

Another work [110] also proposed a hybrid symmetric–asymmetric scheme that combined the DES and RSA algorithms. Their multilevel encryption and decryption model for cloud security showed reduced upload and download times compared to existing methods. However, they did not provide a comprehensive security analysis of the hybrid approach. A similar work [111] developed a hybrid AES–ECC–SHA256 technique focused on enhancing confidentiality, integrity, and authentication. Although it was faster and more effective for text, it was relatively slower for image encryption. Another study [112] proposed a hybrid cryptography algorithm that combined Hill cipher and elliptic curve cryptography (ECC) for image encryption. Hill cipher provides high-speed encryption but is susceptible to known plaintext attacks. ECC offers high security but slower performance. The hybrid method applies Hill cipher first for fast encryption and then ECC to enhance security. The results showed that the hybrid algorithm was faster than ECC alone and was also more secure against attacks compared to Hill cipher. However, the use of fixed keys is a limitation.

A recent study developed a hybrid technique using AES encryption integrated with LSB steganography [113]. AES provides strong security for encrypting image data. Steganography using the LSB algorithm hides encrypted data within the placed cover image for covert transmission. The results demonstrated that the hybrid approach enabled secure, imperceptible transmission of encrypted images. The double protection of encryption and data-hiding enhances confidentiality. In contrast, the method is time-intensive and may not adequately protect against advanced steganalysis.

One study compared classical cryptography techniques, such as AES and DES, to quantum cryptography for image encryption and decryption [114]. Their key findings were that quantum cryptography offers the highest security and is resistant to attacks but is currently limited by distance and implementation challenges. Another work [115] proposed a hybrid cryptography algorithm that combines symmetric (AES and Blowfish) and asymmetric (RSA) techniques for cloud security. Their hybrid AES–Blowfish–RSA approach provided greater security than AES or RSA alone. However, the performance of image encryption was slower, thus resulting in the existence of another limitation. Another study [116] proposed a secure, efficient, and super-fast algorithm for real-time image encryption applications. It uses three logistic maps and a SHA-512 secret key to generate initial values for the Chen system, which is a chaotic image encryption technique [117] based on a block cipher and uses a chaotic map to generate secret keys or sequences, enhancing security by diffusing pixels or bits. The algorithm achieves faster encryption and decryption with fewer runs of chaotic maps and less memory. Simulation results confirm its efficiency and security. Another paper [118] presented a plaintext dynamics-based image-encryption algorithm that uses row-column shuffling and diffusion, reducing encryption rounds and increasing efficiency. It is based on a time-delayed nonlinear combinatorial hyperchaotic map (TD-NCHM) with a wide hyperchaotic interval. The algorithm is sensitive to keystreams and withstands brute-force cracking, differential attacks, chosen-plaintext, and chosen-ciphertext attacks.

Another study [119] proposed an improved hybrid cryptography model that combines symmetric AES, asymmetric RSA, and key exchange via a public key server for IoT data security. The importance of securing IoT data cannot be overstated, as these interconnected devices play a crucial role in our daily lives and various industries, ranging from healthcare and transportation to smart cities and agriculture. As IoT continues to proliferate, innovative security measures are essential to safeguard sensitive information, protect privacy, and ensure the reliability and integrity of IoT networks and applications. Their approach divides data into segments encrypted by different algorithms and shows improved resilience against brute-force attacks versus single methods. However, increased complexity may require more resources. The study demonstrates the potential of multilayered encryption to balance security and performance. A similar work [120] developed a framework integrating homomorphic and Blowfish encryption with fragmentation to secure outsourced medical data in several multi-cloud environments. Their two-tier architecture reduced vendor lock-in risks and provided confidentiality and availability guarantees. Performance analyses showed lower space and time complexity versus alternatives. The hybrid technique enabled secure computation of the encrypted data. However, managing keys across diverse domains remains a critical challenge.

Another article [121] proposed an RSA-based approach for access control over shareable healthcare data, generating keys from the fusion of provider and patient passwords. Their method divided users into personal and public domains with the intent of reducing the management complexity for owners. The experimental results demonstrated enhanced privacy with lower complexity compared to other existing schemes. However, security evaluations were limited, and revocability was not addressed. Another article [122] proposed the optimization of streamlined encryption using the genetic algorithm (GA), termed stream cipher randomization. It aims to maintain data encryption security by increasing the complexity of the key used. It hides statistical properties for the input message and increases key diffusion to eliminate the likelihood of using statistical analysis and cryptanalysis techniques. The method outperforms state-of-the-art methods in terms of execution time and encryption round key size.

A hybrid algorithm was also proposed that combines AES, RSA, and Twofish to improve Bluetooth security [123]. The triple encryption approach on a shared 128-bit key improved robustness compared to the single AES-128 algorithm used in Bluetooth. However, increasing complexity may affect performance and efficiency. The study demonstrated the potential of multilayered encryption to strengthen security. Another study [124] developed an identity-based encryption technique using bilinear pairings to enable fuzzy user data sharing in cloud computing. Their method divided users into personal and public domains, with the aim of reducing the complexity of key management. The security analyses proved resilience against chosen ciphertext attacks. However, assessments were limited, and revocability was unaddressed. A research work [125] proposed an asymmetric technique using RSA plus SHA-2 hashing and AES in counter mode for image encryption. Multiple performance analyses showed a high level of security and efficiency; however, security evaluations focused on statistical attacks with limited cryptanalytic testing.

Based on the comparative analysis of encryption techniques for wearable devices, the lightweight ECC-based cryptography approach demonstrates the greatest potential [126]. Its combination of high cryptographic strength, low power needs, efficient performance in embedded systems, and its ability to generate keys intrinsically linked to wearable biometric signals make it well suited for integration. ECC-enabled encryption optimized for wearable environments and biometrically bound keys can provide robust user-specific security protection for data transmission that augments wearable cryptosystems. Another paper [127] proposed an ECC-based three-factor authentication and key agreement scheme for wireless sensor networks (WSNs). It aimed to enhance security performance by combining biometrics, smart cards, and password authentication technology. The scheme's security and efficiency were tested via formal and informal analysis, making it suitable for resource-constrained WSNs. Another paper [128] presented a novel area-delay optimized finite field multiplier, reducing hardware resource consumption and minimizing latency. It is used to develop an ECC parallel processor, which is highly efficient, robust against power analysis attacks, and suitable for several critical applications. Although further research is still required, the analysis indicates that ECC is the most viable encryption technique that can be customized and deployed on resource-constrained wearable platforms to provide strong confidentiality in addition to biometric authentication mechanisms.

Table 1. Summary and comparison of existing methods of encryption and decryption during data transmission.

Study	Method	Algorithms	Speed	Security	Strength	Weaknesses
Bharathi et al. (2021) [107]	Hybrid cryptography	AES, DES, RSA + LSB steganography	Faster than single encryption	High security	Strong against brute force attacks	Requires more computation than single encryption
Chaloop and Abdullah (2021) [108]	Hybrid cryptography	AES + RSA	Higher throughput than AES or RSA alone	High security	Hybrid combines symmetric and asymmetric with the strength of AES speed and RSA security	Slower than standalone AES
Jaspin et al. (2021) [109]	Double encryption	AES + RSA	Very fast encryption and decryption compared to DES, Blowfish, RC5, 3DES	High-security level	Maintains data confidentiality and integrity, smaller ciphertext size	High computation complexity, Key management overhead
Kumar et al. (2021) [129]	Hybrid cryptography for cloud security	DES + RSA	Reduced encryption/decryption time	Increased data security	Combination of symmetric (DES) and asymmetric (RSA) algorithms provides strong security	Only tested on text files, not other file formats
William et al. (2022) [111]	Hybrid cryptography	AES, ECC, SHA-256	Faster for text but slower for images vs. AES alone	High security using a combination of symmetric, asymmetric, and hash algorithms	Leverages strengths of AES, ECC, and SHA256 algorithms; provides confidentiality, authentication, integrity	Slower image encryption/decryption speed

Table 1. *Cont.*

Study	Method	Algorithms	Speed	Security	Strength	Weaknesses
(Timothy & Santra, 2017) [115]	Hybrid cryptography algorithm for cloud computing security	Blowfish (symmetric), RSA (asymmetric), SHA-2 (hash	Not evaluated	High security for data transmission and storage	Combination of symmetric and asymmetric algorithms SHA-2 provides integrity verification	Specific performance metrics not analyzed; overhead of using multiple algorithms not discussed.
(Pawar & Harkut, 2018) [114]	Survey and comparison of classical and quantum cryptography for image encryption and decryption	Symmetric cryptography, asymmetric cryptography, BB84 protocol, quantum key distribution	Quantum is faster than classical	Quantum cryptography provides more security than classical	Quantum resistant to attacks, based on laws of physics, hard to crack	Expensive, short communication distance, low bit rate
(Almaiah et al. 2020) [112]	Hybrid cryptography	ECC + Hill cipher	Faster than the original Hill cipher	High security	Strong encryption keys generated; every ASCII character can be encrypted	Relatively new approach, needs more analysis.
(Yahaya & Ajibola, 2019) [113]	Hybrid cryptography and steganography	AES + LSB steganography	Not evaluated	High security	Double protection with encryption and hiding	Not evaluated
(Sharma et al. 2022) [121]	Proposed an information leakage prevention scheme (ILPS) using RSA encryption for secure sharing of sensitive health information (SHI) in big data	Improved RSA algorithm for key generation and encryption/decryption	Faster encryption and decryption times compared to AES, DES, RSA	Semantically secure against insider/outsider attacks; provides confidentiality against unauthorized access	Logically divides system into public and personal domains for access control; requires both doctor and patient passwords for decryption key; patient has full control over their SHI data	Relies on RSA which can have scalability issues for large datasets Key management complexity increases with a large number of users
(Bhandari & V B, 2019) [119]	Proposed an enhanced encryption technique for IoT data transmission	Elliptic curve cryptography (ECC) for key pair generation, elliptic curve Diffie–Hellman (ECDH) for shared key agreement, advanced encryption standard (AES) for encryption/decryption	Should be fast due to the use of symmetric encryption (AES) after an initial asymmetric key exchange	High security due to a combination of asymmetric and symmetric encryption	Strong encryption and authentication using a combination of multiple algorithms	Relies on the security of the public key server, which could be a central point of failure if compromised
(Seth et al. 2022) [120]	Proposed a hybrid architecture with client-side and server-side encryption for secure data storage in multi-cloud environments	Paillier homomorphic encryption at the client side, Blowfish encryption at the server side, data fragmentation, integrity checking using hashing	Encryption and decryption faster with compression using Blowfish	Provides confidentiality, integrity, and availability protections against various attacks	Uses two encryption techniques for stronger security; fragmentation improves security and load balancing; multi-cloud storage improves availability	Increased latency compared to single cloud; computationally intensive encryption algorithms; dependent on third-party auditor for integrity checks
Albahar et al. (2018) [123]	Proposed a hybrid cryptosystem	AES, RSA, Twofish	Not assessed	Improved robustness vs. single AES-128 algorithm	Multilayered encryption improves security	Increased complexity may impact efficiency.

Table 1. *Cont.*

Study	Method	Algorithms	Speed	Security	Strength	Weaknesses
Meshram et al. (2019) [124]	Developed identity-based encryption technique	Uses bilinear pairings	Comparable to the ElGamal cryptosystem	Proven secure against chosen ciphertext attacks	Divides users into domains to reduce key management complexity	Evaluations limited; revocability unaddressed
Gafsi et al. (2019) [125]	Proposed asymmetric technique	RSA, SHA-2, AES counter mode	Fast compared to related schemes	Statistical analysis showed high security	AES in counter mode provides speed and security	Limited cryptanalytic testing, focused on statistical attacks

There is a wide range of cryptographic solutions, and focused research is still needed to evaluate techniques developed and/or optimized for modern interconnected environments and wearable devices, considering emerging attacks. The reviewed studies provide insight into the strengths and limitations of current and widespread encryption methods for secure data transmission.

Employing multilayered encryption enhances security [107]. The synergy of symmetric and asymmetric cryptography brings performance benefits [108]. Moreover, quantum cryptography fortifies security resilience [114]. However, it is important to note that this approach can introduce increased complexity, which could affect its operational efficiency [123]. Challenges in managing keys, especially in multi-user systems, pose significant obstacles [124], and the scope of security evaluations may currently be limited [125]. To enhance encryption and decryption during data transmission, researchers should prioritize optimization of encryption algorithms to mitigate adverse effects on data transmission efficiency [123]. Additionally, the development of efficient key management solutions customized to multi-user environments is crucial [124]. Furthermore, researchers should expand the scope of security evaluations to include a wider range of potential threats and vulnerabilities [125].

3.5. Cryptographic Biometric Key Generation from Wearable Technologies

The generation of cryptographic biometric keys uses unique human characteristics to improve the security of cryptographic systems. Biometric characteristics such as fingerprints, iris scans, and facial characteristics can be closely related to cryptographic keys to add an additional layer of protection compared to conventional passwords or token-based approaches [68]. Wearable technologies offer promising capabilities for biometric key generation due to their proximity to the body and their ability to capture physiological and behavioral data. However, research focused specifically on the use of wearable technology is not yet fully covered [18].

The generation of cryptographic biometric keys using wearable technologies is an emerging research area with significant potential to improve the security and user authentication for on-body networks and other devices. Two previous studies demonstrated promising techniques that use gait biometrics to intrinsically bind keys to their users. Both works extract features from accelerometer data during walking [101,130], which helps to generate symmetric cryptographic keys shared between wearable devices on the same body.

In one study, blind source separation by independent component analysis (ICA) is used to isolate gait signals from noise caused by swing motions of the arm [130]. This enables robust key generation by wrist devices. They use binary quantization and privacy amplification to convert signals into high-entropy binary keys. Later, in another study [101], the authors improved this approach to increase bit rates. They also incorporated error correction codes into the reconciliation stage to improve matchmaking between independently generated keys. In both studies, the intrinsic link between unique gait patterns and cryptographic keys was shown to provide security benefits over conventional password- or token-based approaches. The cancelable nature of biometric templates preserves user privacy. Experimental results demonstrate high key agreement rates of up to 100% between legitimate body devices, even from different locations such as the hand, wrist, and body (waist). Statistical tests proved strong randomness for the generated keys. However, limitations are still present concerning formal security analysis, the evaluation of resilience to sophisticated reconstruction or spoofing attacks, the handling of biometric variance, and the management of revocability if templates are compromised. Techniques focus narrowly on gait biometrics and symmetric key generation. Despite that, expansion beyond the allocated constraints is needed. Customizing algorithms specifically for wearable modalities and architectures could improve efficiency and interoperability. These studies provide an initial proof of concept, but rigorous real-world security assessments in adversarial settings would further verify robustness. However, these works reveal promising directions for the generation of biometric cryptographic keys in wearables. They offer user-specific, secure alternatives to conventional key distribution and storage. Ongoing research can be built on these techniques to address current limitations, including assessing security against emerging threats. Tailoring cryptosystems and cancelable templates for wearable biometrics and using multimodal approaches are potential avenues for future exploration. This could enable wearable-based authentication and secure communication without relying on external infrastructure.

Another study provides a comprehensive review of the literature on iris recognition for biometric identification and cryptography [131]. Iris patterns contain a high degree of randomness and distinctiveness, which makes them suitable for binding cryptographic keys. The study discusses several key research areas, including mobility, methods, big data, open-source systems, and challenges. With the proliferation of smartphones and devices, more personalized authentication, such as iris scanning, is needed to address emerging security risks. Cryptographic key generation based on iris templates is proposed to strengthen the encryption process. The author also notes the parallelism between biometric systems and large data in handling large enrolment databases. Open-source iris recognition platforms can enable collaborative advancement and benchmarking. A primary challenge highlighted is the accurate extraction of templates from noisy iris images.

Recent studies have explored techniques to generate cryptographic keys from biometric data captured via wearables. Recent research developed a gait recognition model called ABLSTM to extract gait characteristics from IMU sensor data [132]. To protect the privacy of extracted features, they proposed the stochastic orthogonal transformation (SOT) encryption scheme, which was proven to be secure against chosen plaintext attacks. Their biometric-based encryption (BBE) scheme enables secure communication using gait features as encryption keys after successful user authentication. A recent work [133] developed a stable, flexible, and convenient bio-key using electrocardiograms (ECGs). It minimizes ECG variability issues (e.g., related heart rate and psychological states) using normalization, clustering-based finalization, and fuzzy extractor. The method generates bio-keys with randomness and stability, achieving a maximum entropy of 0.99 and an authentication accuracy of 96%. This research establishes a foundation for encryption key-based personal authentication and can be expanded to other biometric systems.

An approach has also been proposed for grouping and sharing key information between multiple body wearable devices using accelerometer data and gait biometrics [134]. Their method involves smartphones to dynamically generate a secret key during the user's routine, considering their activities using an RMS-based sample selection from the accelerometer data. Gait biometrics are then used to securely distribute the key to other devices using a fuzzy vault construct. A key finding across both studies is that cryptographic binding and generation techniques intrinsically link keys to biometrics (e.g., gait patterns) and provide security benefits over conventional password- or token-based approaches. However, there are limitations to formally evaluating robustness against sophisticated reconstruction, spoofing, and side-channel attacks. The handling of biometric variance and noise also remains a challenge. Additionally, research gaps remain in the development of customized techniques optimized for wearable modalities and constrained environments.

Another work [135] proposed ECG heart (EbH) for the generation of symmetric encryption keys by extracting feature vectors from consecutive ECG samples from a wearable sensor, comparing them with a user ECG model to create seeds, and then deriving the keys through key expansion. Tests conducted on 24 h of ECG data from 199 individuals revealed that EbH generated mainly distinct keys (95. 97%) and was consistent over time. However, the limitations were minimal security analysis and constraints to ECG and symmetric ciphers. The use of PPG-KeyGen has been proposed for the generation of keys from photolithysmogram (PPG) signals using Galois LFSR with successive IBI sequences or AES seeded with IBI sequences [80]. Analyses of the PPG data revealed improved randomness and a 49.67% average Hamming distance between the subjects' keys versus 47.56% for standalone IBI techniques. Limitations included small sample size and limited security evaluations. Another work [136] proposed a biometric security model for wearable healthcare using ECG IPI features to create 128-bit keys. The experiments demonstrated high randomness, passing NIST tests, and a 47.6% average Hamming distance between keys. The limitations, again, included minimal assessments.

Recent interest in intelligent wearable technology has increased in the field of medicine, specifically in the form of wearable computers and other types of computers worn on the human body. Currently, available devices allow people of all ages, including children, the disabled, the elderly, and even adults, to monitor their health in a manner that is not only comfortable but also convenient. However, as the use of these devices becomes more widespread, so do concerns about the privacy and security of the data generated by their users. In one study [137], researchers described technologically advanced wearable sensors that are capable of intelligently monitoring an individual's health and transmitting data securely. They proposed the combination of encryption keys and biometric sensors to secure the communication channel between wearable devices and healthcare providers. This was carried out to prevent unauthorized access to the data transmitted through this channel. When it comes to the safety of wearable technology, protecting sensitive medical data from unauthorized access is one of the greatest obstacles to overcome. The researchers proposed a number of distinct actions that can be taken to protect the privacy of individual data and information to address the problem described in the previous paragraph. These include key encryption sensors, in which data are captured at receiving ends using a key generation method, biometric sensors, in which patients must match their thumbprint to a database to sign in and submit information, and other similar technologies. The authors evaluated the functionality of their wearable medical devices at a hospital in the Indian state of Rajasthan's Neemrana city. They concluded that the use of encrypted communication and biometric sensors was an effective way to protect the privacy of both the patient and the communication channel. This was the case because both the patient and the communication channel were able to remain anonymous. Distant patients could receive updates from their physicians, and as a result, the confidentiality of their messages was maintained.

Wearable computing and other forms of intelligent wearable technology have the potential to significantly improve the delivery of medical care. This could be accomplished through a variety of methods. It is essential to prioritize the privacy and security of users' data to foster trust and encourage a greater number of people to use these services. Inadequate comprehensive security evaluations, lack of revocation mechanisms, limited modalities, and standardized methods are identified as the most significant gaps. Most studies use small sample sizes. Adaptive research is required using robust techniques that are resistant to emerging sophisticated attacks, revocability, privacy preservation, and usability optimized for novel wearable modalities.

Recent interest in intelligent wearable technology has increased in the field of medicine, specifically in the form of wearable computers and other types of computers worn on the human body. Currently, available devices allow people of all ages, including children, the disabled, the elderly, and even adults, to monitor their health in a manner that is not only comfortable but also convenient. However, as the use of these devices becomes more widespread, so do concerns about the privacy and security of the data generated by their users.

The use of gait biometrics inherent to users is a notable strength of cryptographic biometric key generation in wearables [101]. Implementing cancelable templates also brings the advantage of revocability [132] and eliminates the need for external infrastructure, improving practicality [134]. However, it is crucial to recognize that formal security cryptanalysis is currently lacking [80], and the method often focuses on limited modalities such as ECG or PPG signals [136]. Furthermore, there is a clear need for optimized protocols that consider the unique constraints and limitations associated with wearable devices [135]. To improve the generation of biometric cryptographic keys on wearables, researchers should prioritize performing thorough cryptanalysis to evaluate the security of wearable-based key generation methods [80]. Expanding the applicability of these techniques to a wider spectrum of biometric modalities is essential [136].

4. Discussion

This research delves into the use of wearable biometric technologies for the generation and decryption of cryptographic keys and data, unveiling several key themes focused on harnessing unique physiological and behavioural characteristics to establish robust and secure user-specific keys. Although there are promising techniques for the use of wearable biometrics in cryptographic systems, there is still a significant gap in the implementation of a comprehensive and synergistic approach that combines the most robust methods into a customized solution for wearable devices [32,80].

Intrinsic binding techniques, such as fuzzy commitment, show potential in tightly linking keys to biometrics, yet the challenge of handling noise and variance persists [78]. The use of error-correcting codes promises to address inconsistencies but can impose limitations on key sizes [72]. Cancelable templates provide the advantage of template renewability and revocability in case of compromise while also avoiding the storage processing of raw biometric data. However, current techniques lack sufficient security analysis, particularly with respect to side-channel attacks and optimization of the constraints posed by wearable devices [77].

Diverse encryption techniques exhibit varying strengths and weaknesses, encompassing efficiency, constraints, and security evaluations. However, there is a need for focused research to develop wearable-optimized methods, accommodate multimedia data, and mitigate emerging threats [125]. Furthermore, the proposed protocols for the generation of wearable keys, encryption and decryption, are promising but have limitations regarding constraints, supported modalities, resilience against attacks, adherence to standards, and robustness testing in the real world [135,136].

A fundamental benefit highlighted in this research is the intrinsic link of cryptographic keys to individual biometric data, such as fingerprints, iris scans, or gait patterns, which offers distinct security advantages over traditional password- or token-based systems. Techniques such as fuzzy commitment, fuzzy vault, and cancelable biometrics, as presented in Table 2, propose keys that are tightly irreversibly bound to biometrics, eliminating the need for raw template storage [68,92]. This inherent connection between a user's identity and their cryptographic key enhances the level of security and seamlessly matches the key with the individual. However, the persistent challenge lies in managing inherent noise and variance in biometric data, which require custom methods to extract stable cryptographic keys from noisy input captured by such wearable sensors [78].

Another key focus is the preservation of the privacy of biometric data used in cryptographic processes, achieved through cancelable biometrics, one-way transformations, and the avoidance of raw template storage [68,81]. Analyzing the security and revocability of systems in the event of template compromise is equally essential. However, as indicated in Table 2, many studies demonstrate proof of concepts with minimal security analysis against sophisticated attacks such as reconstruction or spoofing [68,78]. Furthermore, as summarized in Table 1, while there are many encryption and decryption methods, there is a need for focused research in the development and evaluation of customized techniques optimized for modern interconnected environments, wearable devices, multimedia data, and emerging attack vectors. Comprehensive cryptographic evaluations during the design phase and testing with larger sample sizes will contribute to validating their robustness and reliability [68,80].

The generation of strong cryptographic keys on resource-constrained wearable devices presents a unique set of challenges compared to traditional systems. Lightweight protocols and algorithms that optimize limited computational power, battery life, storage, and bandwidth are imperative [77,96]. However, striking the right balance between efficiency requirements and security strength remains an ongoing research equation. In addition, most techniques tend to focus only on fixed modalities, such as ECG, PPG, fingerprints, or gait patterns. Expanding beyond these limits through custom algorithms that cater to diverse wearable modalities can fortify the security procedure [134]. The exploration of multi-modal approaches is also warranted. However, tailored techniques that are aligned with the ergonomics of each modality are essential for usability.

Moreover, there is a noticeable absence of common standards, interoperable techniques, or benchmarks between different wearable platforms, user groups, and manufacturers [136]. Establishing standard modalities, evaluation criteria, and data sets would facilitate rigorous comparative evaluations of biometric encryption techniques in wearables, helping to encourage their adoption and consumption. Custom techniques, optimized for specific devices or biometrics, pose challenges in interoperability.

In conclusion, while wearable biometrics have immense potential to generate robust user-specific cryptographic keys that are inherently resistant to physical theft, significant research gaps in the areas of resilience against sophisticated attacks, revocability, noise in biometric data, constraints within wearable environments, and the need for interoperability standards persist [68,77]. Dedicated research efforts that focus on cryptanalysis, lightweight optimization, novel modalities, and large-scale testing are imperative. Multidisciplinary efforts encompassing biometrics, cryptography, and machine learning can advance this emerging field and pave the way for the creation of practical and secure solutions [134,138]. Wearable biometric cryptosystems have the potential to revolutionize authentication and communication security for on-body networks, capitalizing on the widespread prevalence of biometrics. However, systematic research that addresses the identified limitations is crucial to applying this vision. A review of the literature provided invaluable information on the current landscape, strengths, and weaknesses while guiding promising directions in future investigations.

Table 2. Summary and comparison of existing methods of biometrics cryptographic key generation.

Study	Methodology	Key Generation	Biometric Modalities	Key Size	Matching Algorithm	Renewability	Strengths	Weaknesses
(Wang et al. 2021) [72]	Generated intervals and two-layer error correction	Fingerprint minutiae distances	Fingerprint	120–168 bits	Hamming distance threshold	Yes, cancelable template	High key regeneration rate, privacy protection, fault tolerance	Fingerprint extraction challenges, limited security analysis
(Anees & Chen, 2018) [73]	Equalized LBP feature quantization	Facial features	Face	256 bits	-	Yes	No templates stored caters for variations, enhanced security	Slightly lower recognition rate, higher complexity
(Verma et al. 2019) [74]	phase retrieval and PTFT	Fingerprint hologram	Fingerprint	Binary key	Correlation coefficient	Yes	Asymmetric encryption, authenticity verification, robust against attacks	-

Table 2. *Cont.*

Study	Methodology	Key Generation	Biometric Modalities	Key Size	Matching Algorithm	Renewability	Strengths	Weaknesses
(Sarkar & Singh, 2017) [20]	RSA key generation using cancelable fingerprint templates	Asymmetric (public/private keys)	Fingerprint	1024 bits	Not specified	Yes, cancelable templates are renewable	Links key to biometrics for added security—cancelable templates provide renewability	Unclear if keys are consistent across captures—security analysis not comprehensive
(Suresh et al. 2022) [78]	RSA key pair generation using fingerprint and password	Asymmetric (public/private keys)	Fingerprint + Password	2048 bits	Reed–Solomon code	No, but the private key is not stored so not needed	Two-factor authentication (fingerprint + password) Grey code handles intra-user variability	Fingerprint template still exposed during enrollment; limited biometric modalities
(Salman et al. 2020) [79]	Meerkat algorithm for key generation from multi-biometric template	Symmetric key from minutiae points of eye and ear	Eye outer edges, Ear	128 bits	-	Renewable by updating the cancelable template	Strong and unique keys from biometrics using Meerkat; faster and accurate key generation	Only evaluated on a small dataset; Security analysis lacking
(Sarkar & Singh, 2018) [77]	Cancelable fingerprint template of sender and receiver combined to generate a symmetric key	Symmetric key from cancelable fingerprint templates	Fingerprint minutiae	128 bits	-	Renewable by updating cancelable template parameters	Links key to biometrics; preserves fingerprint privacy; no key storage needed	Limited security analysis; needs more evaluation
(Sarkar et al. 2018) [81]	Shuffling and bitwise XOR of minutiae coordinates to get a cancelable template, then prime number generation for asymmetric key	Asymmetric (private, public) key from cancelable fingerprint template	Fingerprint minutiae	1024 bits	-	Renewable by updating the shuffle key	Maintains biometric privacy via cancelable templates; easy revocation and re-issuance	Security analysis lacking; robustness needs thorough assessment; robustness needs thorough assessment
Aanjanadevi et al. (2019) [67]	PCA for feature extraction, RSA for encryption/decryption	From facial features	Face	Not specified	Not specified	Not discussed	Strong encryption using biometrics	Privacy and security not fully analyzed
Sarkar & Singh (2020) [68]	Gabor filter for feature extraction, fuzzy vault	Align fingerprint minutiae with random chaff points	Fingerprint	140 bits	Fingerprint minutiae matching	Revocable and renewable keys	Revocable and renewable keys	Slower authentication due to fingerprint alignment
Tuiri et al. (2019) [69]	ICA for EEG processing, Diffie–Hellman and AES for key generation/encryption	Diffie–Hellman exchange and AES based on EEG features	EEG	230 bits	Key match for Diffie–Hellman and AES keys	New keys generated by changing parameters	Random and irreversible keys, high security	High FRR rates

Table 2. *Cont.*

Study	Methodology	Key Generation	Biometric Modalities	Key Size	Matching Algorithm	Renewability	Strengths	Weaknesses
Wang et al. (2020) [70]	Deep CNN for feature extraction, XOR operation for key generation	XOR operation on deep CNN facial features	Face	1024 bits	Threshold-based key match	New keys generated by changing parameters	High randomness, security, and renewability	Threshold selection affects FAR/FRR tradeoff

Summary of Challenges with Wearable Technologies Key Generation

As discussed, key generation and management using wearable devices presents several unique challenges that need to be addressed. Based on the literature review, some of the main challenges are as follows:

Biometric Variance and Noise —Biometric data collected by wearables, such as fingerprints, iris scans, and facial patterns, can be noisy and vary between captures [36,68,78]. This variability can affect the accuracy of the binding techniques and cryptographic key generation, which are based on precise biometric data. Potential solutions include the use of techniques such as quantization, grey code, and error correction codes to handle biometric variance [72,73,78]. Unlike conventional passwords or tokens, which remain consistent, the biometric data captured by wearable sensors can be noisy or exhibit variations between captures [68]. This inconsistency makes it challenging to consistently extract the same cryptographic key from biometric inputs such as ECG or gait signals [80]. Therefore, techniques must be developed to handle intra-user variability and generate stable keys from wearable biometrics [78].

To overcome these challenges, the use of robust feature extraction techniques that are less sensitive to noise should be further investigated. This means that the research community should place added emphasis on addressing challenges with noise as well as achieving good results in empirical studies. This could be achieved by intentionally using noisy samples when testing to gain a more comprehensive understanding. It is also necessary to establish adaptive thresholds for biometric matching to handle variations in data quality. Many biometric technologies use fixed thresholds established during empirical testing, which, when deployed in different environments, may no longer be optimal. In addition, there is a need to consider multimodal fusion by combining different biometric modalities to improve accuracy. As identified in this article, the use of multimodal biometric systems is a way to improve their capabilities, and their integration into cryptosystems should be further considered. Finally, providing real-time quality feedback during data capture and applying noise reduction algorithms could also provide a useful solution. If the system is likely to provide diminished results due to noise, then it is a good idea to inform the user of this so that they can understand why the system might not perform as expected. It is important to remember that both hardware improvements and software techniques play a crucial role in mitigating this challenge.

Security and Privacy—Wearable devices are susceptible to physical compromise or side-channel attacks that could lead to the exposure of secret key material or biometric data [101]. Most studies lack formal security analysis of biometric key generation schemes customized for wearables against sophisticated forms of attacks [134]. Providing resistance to emerging threats, such as model inversion, reconstruction, and spoofing, remains a significant challenge. Preserving user privacy through cancelable biometrics is also crucial [132]. It is essential to protect the privacy of biometric data used in key generation to prevent exposure of sensitive user information [68,81]. Approaches such as cancelable biometrics, one-way transformations, and avoiding the storage of raw biometric data can help protect privacy.

As these wearable devices collect sensitive personal health data, safeguarding user information is paramount and overcoming these challenges is important. It is critical to implement robust encryption mechanisms to protect data during transmission and storage.

If data are left insecure during transfer and storage, they are susceptible to interception and potential misuse. Another key recommendation for deployment is that users must obtain clear and informed consent regarding data collection, sharing, and usage and ensure transparent privacy policies. This is necessary to ensure that both the user and the provider of the biometric system fully understand how the data will be processed. Operating in an open and transparent way is essential to gain user trust and maintain regulatory compliance. As wearable cryptosystems will inevitably involve many technology providers and stakeholders, great effort should be taken to anonymize health data before sharing them with third parties and perform regular security audits to identify vulnerabilities. It is also important to enable users to control the preferences of data sharing through custom privacy settings. Not only is this a necessary legal requirement, but it also instills user trust if they have control over how their data are shared and managed. Adopting a holistic approach that combines technical measures, legal compliance, and user awareness is essential to address security and privacy challenges in wearable technology.

Interoperability and Standardisation—The generated cryptographic keys must withstand various attacks, such as brute force, reconstruction, and spoofing attempts. There is a need for formal security analysis during the design of these techniques [68,78]. Techniques to improve resilience include multimodal biometrics, dynamic key binding, and incorporating factors such as passwords [78,103]. Furthermore, there seems to be a lack of common standards or methods for a biometric-based key generation across different wearable platforms, users, and manufacturers [136]. The cybersecurity landscape faces an unprecedented surge in attacks. Adversaries exploit zero-day vulnerabilities, employ disruptive wipers, and utilize emerging server-based attack mechanisms (such as ransomware), amplifying the complexity of cyber threats. In cyber security defence, it is evident that more artificial intelligence (AI) systems are emerging as viable solutions to protect and defend [2,139]. However, The use of AI systems to better protect cryptosystems is an avenue of research that is still to be fully explored. It is of key importance that detection and defence mechanisms are further considered, as it is inevitable that any deployed system will be attacked. Detecting and defending against attacks is important to gain an understanding of how the system is maintaining resilience.

When addressing this challenge, it is important to establish context-specific quality standards for wearables. By ensuring, developing, and adopting wearable cryptosystems, these standards should account for variations in data accuracy, reliability, and robustness in diverse environments while increasing system interoperability. Ensuring that wearable devices can seamlessly be integrated into other health systems and platforms is key to their long-term adoption. Users are more likely to adopt new technology if it is used across a range of technologies that they interact with in their daily lives, such as vehicles, IoT devices, etc. Interoperability allows data exchange and collaboration in different environments and can help promote equitable access to wearable technology. Other ways to help provide equitable access include addressing disparities related to affordability, availability, and distribution, especially in under-represented regions or populations. However, it is important to emphasize that promoting diverse system updates means that the system must be developed and tested using representative datasets. This requires the validation of wearable performance in diverse user demographics, environmental conditions, and health contexts, taking into account factors such as age, sex, ethnicity, and levels of physical activity. It is possible that the wearable devices can seamlessly be integrated into other health systems and platforms.

Ease of Use and Ergonomics—The biometric capture process for key generation should be seamless and ensure usability, especially for mobile devices [68]. Modalities that align with natural user interactions are ideal. On-device processing avoids the need for additional complex hardware [81].

When addressing these challenges, there is a need to prioritize user requirements throughout the design process. This involves users in usability testing and feedback sessions to ensure that the wearables are intuitive and comfortable. As part of this consideration, it is necessary to optimize wearable form factors for comfort, fit, and minimal interference with daily activities. This is to ensure that wearable devices themselves do not cause usability and wear challenges. The majority of wearable biometrics examined in this article can be sensed by devices that have become pervasive (e.g., smart watches), and using these devices can really help make the biometric system easy to use and ergonomically acceptable. Best practices in terms of system design will need to be followed to simplify user interaction. This is because it is necessary to streamline user interfaces to minimize cognitive load and ensure that the system can be easily operated while the user is going about his/her daily life or interacting with other systems. This means adhering to widely regarded good design principles, such as clear menus, intuitive gestures, and straightforward controls, improves usability.

Limited Modalities and Testing—Most existing techniques are limited to specific biometrics such as ECG, PPG, or gait. Expanding to new suitable wearable modalities, such as EEG, EMG, body temperature, or skin conductance, could improve key generation [134]. Multimodal approaches should also be explored to improve capability. Furthermore, many studies demonstrate proof of concept on small proprietary data sets with limited subjects. Rigorously evaluating the robustness, repeatability, and reliability of biometric key generation techniques in larger, diverse populations is important [80]. Further, there are several challenges [10] associated with integrating biometric sensors into wearable devices, such as high power consumption and low quality or inaccurate biometric measurements.

To overcome this challenge, it is a good idea, where possible, to explore diversifying sensing modalities and introducing quality standards, as previously mentioned. This could be achieved by including additional sensors, such as chemical sensors, bio patches, or electronic skin. The combination of data from multiple sensors may improve accuracy and reliability; however, this is still to be established, and further research is required. Although there is extensive work demonstrating that multimodal biometric systems can improve the accuracy of cryptosystems, there is an absence of studies that demonstrate that multimodal sensing using wearable devices can improve the capabilities and usability of wearable cryptosystems. More research is required to explore and establish whether fusion techniques can compensate for limitations in individual modalities and whether developing wearables that sense different biometric characteristics and activities can improve capability and usability. Once again, interoperability should be considered to ensure that wearable devices can integrate seamlessly with other health systems and platforms.

Wearable devices collect personal data, including that of biometric characteristics, which must be protected through various mechanisms, such as encryption and authentication. At the same time, improving the functionality of the wearable device with minimal power consumption and improved sensor accuracy is required for a seamless and intuitive experience. Hence, there is a need for the optimization of wearable environments and maximization of functionality while preserving security.

Future solutions should focus on formal security analysis against sophisticated reconstruction, model inversion, and spoofing attacks. This involves implementing access control measures, such as authentication and encryption, to restrict access to the model and its predictions, as well as to avoid spoofing attacks. Input validation is also crucial to prevent malicious data from being provided to the system. In addition, regular retraining of the model by incorporating new data can prevent outdated information from being leaked and correct any inaccuracies in the predictions.

Cancelable biometrics and multi factor authentication should be used to enhance privacy and resilience. The existing literature presents several solutions for transforming biometric data into a cancelable form, thereby preventing direct storage of an individual's biometric features. This also reduces the risks of biometric data theft by preventing attackers from reverse engineering templates, ensuring system resilience. Multi-factor authentication offers multiple layers of protection, providing backup authentication mechanisms, making it harder for unauthorized users to gain access even if one layer is compromised.

Tailored techniques are needed that are capable of extracting consistent and stable keys from noisy physiological signals. This requires thoroughly tested methodologies that work accurately in different environments and conditions. It is also necessary to have interoperable algorithms that work across various modalities, manufacturers, and developers. Differences in encoding methods and data formats (for example, the biometric templates) can seriously hinder seamless integration and data sharing. Addressing this challenge using standardized techniques will enhance usability and applicability.

Evaluation of larger, diverse datasets rather than small samples will help validate their robustness and enhance security. This is necessary to improve generalization, increase the pool of potential features to reduce the likelihood of collisions, address biometric drift, and simulate real-world scenarios to determine applicability.

Focused research in these areas can significantly improve the reliability and security of biometric key generation in wearables and facilitate the widespread adoption of secured solutions.

5. Conclusions and Future Work

In conclusion, this comprehensive review of the literature has shed light on the intriguing possibilities and challenges surrounding the use of wearable biometric technologies for the generation and management of cryptographic keys. The key takeaways from this analysis paint a picture of a promising but evolving landscape.

One of the standout advantages of this approach is the inherent connection between cryptographic keys and a user's unique physiological or behavioral characteristics. This innovative approach significantly improves security, surpassing traditional password- or token-based systems that are vulnerable to theft or loss. The introduction of techniques such as fuzzy commitment, fuzzy vault, and cancelable biometrics offers exciting avenues to securely attach keys to biometric templates. However, taming the noise and variance in biometric data collected through wearable sensors remains a formidable challenge. Tailor-made techniques are imperative to extract stable cryptographic keys from these inherently noisy inputs.

In addition, crucial emphasis is placed on safeguarding the privacy of biometric data. Cancelable biometrics, one-way transformations, and avoidance of raw template storage are the keys to this effort. However, it is essential to acknowledge that while initial proofs of concept have been demonstrated, formal cryptanalysis to assess resilience against advanced attacks is still limited. A robust security evaluation in more extensive and diverse datasets is imperative to fully validate the strength and dependability of these methods. The practicality of implementing wearable biometric cryptosystems within resource-constrained wearable environments introduces another layer of complexity. These systems must be optimized for limited computational power, battery life, storage capacity, and bandwidth without compromising security. Furthermore, the potential expansion of biometric modalities beyond traditional ones, such as fingerprints, iris scans, and gait, to include novel wearable-friendly biometrics such as EEG, EMG, and skin conductivity holds the promise of further strengthening security.

In the future, there are several promising directions to build on the findings of this literature survey and address existing research challenges. First, conducting comprehensive security evaluations against advanced attacks such as reconstruction, model inversion, and presentation attacks is essential to fully assess the resilience of proposed cryptosystems. Incorporating artificial intelligence techniques can enhance continuous authentication capabilities. It is critical to develop cancelable biometric schemes tailored specifically for wearable modalities, allowing template renewal if compromised and preserving user privacy by avoiding the exposure of raw biometric data. In addition, specialized feature extraction and binding techniques need to be designed to generate stable keys that are resistant to noise and physiological signal variance. Resolving inconsistencies in biometric data captured via wearable sensors remains a persistent challenge. Exploring emerging modalities suitable for wearables, such as EEG, EMG, skin temperature, and conductivity, and combining multiple modalities could improve the security and accuracy of biometric authentication. Many current techniques are limited to a narrow set of biometrics, so adapting algorithms and templates for diverse wearable sensing is crucial. Developing lightweight, optimized protocols that balance efficiency within the resource constraints of wearables without excessively compromising security is also a priority. Standard benchmarks, modalities, and evaluation criteria would facilitate comparative evaluations of techniques in different studies. Rigorously evaluating performance, security, and usability in larger and more diverse populations that reflect real-world conditions is essential to validate robustness.

In summary, while wearable biometrics represent a promising avenue for user-specific key generation, several substantial gaps and challenges persist. These include concerns regarding attack resilience, revocability, handling biometric noise, constraints on wearable platforms, interoperability, standards, and the need for rigorous security assessments. Addressing these limitations will require targeted research efforts focused on cryptanalysis, cancelable templates, stable feature extraction, lightweight optimisations, expanded modalities, and large-scale testing initiatives. With diligent efforts to bridge these gaps, wearable biometric cryptosystems have significant potential to evolve into secure and deployable solutions, ultimately enhancing communication security in our interconnected world.

Author Contributions: Conceptualization, K.A.A.; methodology, K.A.A., T.A., O.A., I.I.-D., S.K. and S.P.; investigation, K.A.A.; data curation, K.A.A.; writing—original draft preparation, K.A.A., T.A., O.A., I.I.-D., S.K. and S.P.; writing—review and editing, K.A.A., T.A., O.A., I.I.-D., S.K. and S.P.; supervision, S.P.; project administration, K.A.A., S.K. and S.P. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: No new data was created.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Cremer, F.; Sheehan, B.; Fortmann, M.; Kia, A.N.; Mullins, M.; Murphy, F.; Materne, S. Cyber risk and cybersecurity: A systematic review of data availability. *Geneva Pap. Risk Insur.-Issues Pract.* **2022**, *47*, 698–736. [CrossRef] [PubMed]
2. Parkinson, S.; Khan, S. Identifying irregularities in security event logs through an object-based Chi-squared test of independence. *J. Inf. Secur. Appl.* **2018**, *40*, 52–62. [CrossRef]
3. Mubarak, R.; Alsboui, T.; Alshaikh, O.; Inuwa-Dutse, I.; Khan, S.; Parkinson, S. A Survey on the Detection and Impacts of Deepfakes in Visual, Audio, and Textual Formats. *IEEE Access* **2023**, *11*, 144497–144529. [CrossRef]
4. Humayun, M.; Niazi, M.; Jhanjhi, N.; Alshayeb, M.; Mahmood, S. Cyber security threats and vulnerabilities: A systematic mapping study. *Arab. J. Sci. Eng.* **2020**, *45*, 3171–3189. [CrossRef]
5. Khan, S.; Parkinson, S.; Murphy, C. Context-based irregular activity detection in event logs for forensic investigations: An itemset mining approach. *Expert Syst. Appl.* **2023**, *233*, 120991. [CrossRef]
6. Azad, M.A.; Bag, S.; Parkinson, S.; Hao, F. TrustVote: Privacy-Preserving Node Ranking in Vehicular Networks. *IEEE Internet Things J.* **2019**, *6*, 5878–5891. [CrossRef]
7. Susmitha, C.; Srineeharika, S.; Laasya, K.S.; Kannaiah, S.K.; Bulla, S. Hybrid Cryptography for Secure File Storage. In Proceedings of the 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 23–25 February 2023; pp. 1151–1156.
8. Bertino, E. Data security and privacy: Concepts, approaches, and research directions. In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; Volume 1, pp. 400–407.
9. Parkinson, S.; Khan, S.; Badea, A.M.; Crampton, A.; Liu, N.; Xu, Q. An empirical analysis of keystroke dynamics in passwords: A longitudinal study. *IET Biom.* **2023**, *12*, 25–37. [CrossRef]
10. Khan, S.; Parkinson, S.; Grant, L.; Liu, N.; Mcguire, S. Biometric systems utilising health data from wearable devices: Applications and future challenges in computer security. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–29. [CrossRef]
11. Ahmad, S.; Mehfuz, S.; Beg, J. Hybrid cryptographic approach to enhance the mode of key management system in cloud environment. *J. Supercomput.* **2023**, *79*, 7377–7413. [CrossRef]
12. Zhang, Q. An overview and analysis of hybrid encryption: The combination of symmetric encryption and asymmetric encryption. In Proceedings of the 2021 2nd International Conference on Computing and Data Science (CDS), Stanford, CA, USA, 28–29 January 2021; pp. 616–622.

13. Parkinson, S.; Khan, S. A survey on empirical security analysis of access-control systems: A real-world perspective. *ACM Comput. Surv.* **2022**, *55*, 1–28. [CrossRef]
14. Ji, Z.; Zhang, Y.; He, Z.; Lin, K.; Li, B.; Yeoh, P.L.; Yin, H. Vulnerabilities of physical layer secret key generation against environment reconstruction based attacks. *IEEE Wirel. Commun. Lett.* **2020**, *9*, 693–697. [CrossRef]
15. Henriques, M.S.; Vernekar, N.K. Using symmetric and asymmetric cryptography to secure communication between devices in IoT. In Proceedings of the 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, India, 19–20 May 2017; pp. 1–4.
16. Kim, J.; Nepal, S. A cryptographically enforced access control with a flexible user revocation on untrusted cloud storage. *Data Sci. Eng.* **2016**, *1*, 149–160. [CrossRef]
17. Dammak, M.; Boudia, O.R.M.; Messous, M.A.; Senouci, S.M.; Gransart, C. Token-based lightweight authentication to secure IoT networks. In Proceedings of the 2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 11–14 January 2019; pp. 1–4.
18. Shaheed, K.; Mao, A.; Qureshi, I.; Kumar, M.; Abbas, Q.; Ullah, I.; Zhang, X. A systematic review on physiological-based biometric recognition systems: Current and future trends. In *Arch. Computat. Methods Eng.* **2021**, *28*, 4917–4960. [CrossRef]
19. Kakkad, V.; Patel, M.; Shah, M. Biometric authentication and image encryption for image security in cloud framework. *Multiscale Multidiscip. Model. Exp. Des.* **2019**, *2*, 233–248. [CrossRef]
20. Sarkar, A.; Singh, B.K.; Bhaumik, U. RSA key generation from cancelable fingerprint biometrics. In Proceedings of the 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 17–18 August 2017; pp. 1–6.
21. Suresh, P.; Radhika, K. Nature inspired hybrid algorithms for binding shared key with user trait. *Int. J. Appl. Pattern Recognit.* **2021**, *6*, 217–231. [CrossRef]
22. Sardar, A.; Umer, S.; Rout, R.K.; Khan, M.K. A secure and efficient biometric template protection scheme for palmprint recognition system. *IEEE Trans. Artif. Intell.* **2022**, *4*, 1051–1063. [CrossRef]
23. Panchal, G.; Samanta, D.; Barman, S. Biometric-based cryptography for digital content protection without any key storage. *Multimed. Tools Appl.* **2019**, *78*, 26979–27000. [CrossRef]
24. Khan, S.H.; Akbar, M.A.; Shahzad, F.; Farooq, M.; Khan, Z. Secure biometric template generation for multi-factor authentication. *Pattern Recognit.* **2015**, *48*, 458–472. [CrossRef]
25. Ballard, L.; Kamara, S.; Reiter, M.K. The Practical Subtleties of Biometric Key Generation. In Proceedings of the USENIX Security Symposium, San Jose, CA, USA, 28 July–1 August 2008; pp. 61–74.
26. Chang, Y.J.; Zhang, W.; Chen, T. Biometrics-based cryptographic key generation. In Proceedings of the 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No. 04TH8763), Taipei, China, 27–30 June 2004; Volume 3, pp. 2203–2206.
27. Suleski, T.; Ahmed, M.; Yang, W.; Wang, E. A review of multi-factor authentication in the Internet of Healthcare Things. *Digit. Health* **2023**, *9*, 20552076231177144. [CrossRef]
28. Sarkar, A.; Singh, B.K. Cancelable biometric based key generation for symmetric cryptography. In Proceedings of the 2017 International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 10–11 March 2017; pp. 404–409.
29. Rao, S.R.P.; Jyothi, K. Secret Key Generation using Genetic Algorithm for the Hybrid Blowfish Encryption and Substitution Ciphers. In Proceedings of the 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 8 September 2022; pp. 1–5.
30. Gomez-Barrero, M.; Maiorana, E.; Galbally, J.; Campisi, P.; Fierrez, J. Multi-biometric template protection based on homomorphic encryption. *Pattern Recognit.* **2017**, *67*, 149–163. [CrossRef]
31. Crihan, G.; Dumitriu, L.; Crăciun, M.V. Preliminary Experiments of a Real-World Authentication Mechanism Based on Facial Recognition and Fully Homomorphic Encryption. *Appl. Sci.* **2024**, *14*, 718. [CrossRef]
32. Sarkar, A.; Singh, B.K. A review on performance, security and various biometric template protection schemes for biometric authentication systems. *Multimed. Tools Appl.* **2020**, *79*, 27721–27776. [CrossRef]
33. Khan, S.; Parkinson, S.; Liu, N.; Grant, L. Low-cost fitness and activity trackers for biometric authentication. *J. Cybersecur.* **2020**, *6*, tyaa021. [CrossRef]
34. Rezai, A.; Keshavarzi, P.; Moravej, Z. Key management issue in SCADA networks: A review. *Eng. Sci. Technol. Int. J.* **2017**, *20*, 354–363. [CrossRef]
35. Slimani, D.; Merazka, F. Encryption of speech signal with multiple secret keys. *Procedia Comput. Sci.* **2018**, *128*, 79–88. [CrossRef]
36. Dwivedi, R.; Dey, S.; Sharma, M.A.; Goel, A. A fingerprint based crypto-biometric system for secure communication. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 1495–1509. [CrossRef]
37. Tran, Q.N.; Turnbull, B.P.; Hu, J. Biometrics and privacy-preservation: How do they evolve? *IEEE Open J. Comput. Soc.* **2021**, *2*, 179–191. [CrossRef]
38. Sarkar, A.; Singh, B.K. A multi-instance cancelable fingerprint biometric based secure session key agreement protocol employing elliptic curve cryptography and a double hash function. *Multimed. Tools Appl.* **2021**, *80*, 799–829. [CrossRef]
39. Sarier, N.D. Multimodal biometric identity based encryption. *Future Gener. Comput. Syst.* **2018**, *80*, 112–125. [CrossRef]
40. Sardar, A.; Umer, S.; Pero, C.; Nappi, M. A novel cancelable facehashing technique based on non-invertible transformation with encryption and decryption template. *IEEE Access* **2020**, *8*, 105263–105277. [CrossRef]

41. Uludag, U.; Pankanti, S.; Prabhakar, S.; Jain, A.K. Biometric cryptosystems: Issues and challenges. *Proc. IEEE* **2004**, *92*, 948–960. [CrossRef]
42. Sharma, S.; Saini, A.; Chaudhury, S. A survey on biometric cryptosystems and their applications. *Comput. Secur.* **2023**, *134*, 103458. [CrossRef]
43. Kaur, P.; Kumar, N.; Singh, M. Biometric cryptosystems: A comprehensive survey. *Multimed. Tools Appl.* **2023**, *82*, 16635–16690. [CrossRef]
44. Liu, S.; Shao, W.; Li, T.; Xu, W.; Song, L. Recent advances in biometrics-based user authentication for wearable devices: A contemporary survey. *Digit. Signal Process.* **2022**, *125*, 103120. [CrossRef]
45. Piciucco, E.; Di Lascio, E.; Maiorana, E.; Santini, S.; Campisi, P. Biometric recognition using wearable devices in real-life settings. *Pattern Recognit. Lett.* **2021**, *146*, 260–266. [CrossRef]
46. Blasco, J.; Chen, T.M.; Tapiador, J.; Peris-Lopez, P. A survey of wearable biometric recognition systems. *ACM Comput. Surv. (CSUR)* **2016**, *49*, 1–35. [CrossRef]
47. Parkinson, S.; Khan, S.; Liu, N.; Xu, Q. Repetition and Template Generalisability for Instance-Based Keystroke Biometric Systems. In Proceedings of the 2023 IEEE 3rd International Conference on Computer Communication and Artificial Intelligence (CCAI), Taiyuan, China, 26–28 May 2023; pp. 272–277.
48. Li, B.; Wang, W.; Gao, Y.; Phoha, V.V.; Jin, Z. Hand in motion: Enhanced authentication through wrist and mouse movement. In Proceedings of the 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, 22–25 October 2018; pp. 1–9.
49. Nie, Z.; Liu, Y.; Duan, C.; Ruan, Z.; Li, J.; Wang, L. Wearable biometric authentication based on human body communication. In Proceedings of the 2015 IEEE 12th International Conference on Wearable and Implantable Body Sensor Networks (BSN), Cambridge, MA, USA, 9–12 June 2015; pp. 1–5.
50. Chowdhury, D.P.; Kumari, R.; Bakshi, S.; Sahoo, M.N.; Das, A. Lip as biometric and beyond: A survey. *Multimed. Tools Appl.* **2022**, *81*, 3831–3865. [CrossRef]
51. Marsico, M.D.; Mecca, A. A survey on gait recognition via wearable sensors. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 1–39. [CrossRef]
52. Liang, G.C.; Xu, X.Y.; Yu, J.D. User-authentication on wearable devices based on punch gesture biometrics. In *Proceedings of the ITM Web of Conferences*; EDP Sciences: Les Ulis, France, 2017; Volume 11, p. 01003.
53. Liu, R.; Cornelius, C.; Rawassizadeh, R.; Peterson, R.; Kotz, D. Vocal resonance: Using internal body voice for wearable authentication. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2018**, *2*, 1–23. [CrossRef]
54. Lehmann, F.; Buschek, D. Heartbeats in the wild: A field study exploring ECG biometrics in everyday life. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 25–30 April 2020; pp. 1–14.
55. Khondakar, K.R.; Kaushik, A. Role of wearable sensing technology to manage long COVID. *Biosensors* **2022**, *13*, 62. [CrossRef]
56. Lee, S.H.; Kim, Y.S.; Yeo, W.H. Soft wearable patch for continuous cardiac biometric security. *Eng. Proc.* **2021**, *10*, 73. [CrossRef]
57. Ahmad Tarar, A.; Mohammad, U.; K. Srivastava, S. Wearable skin sensors and their challenges: A review of transdermal, optical, and mechanical sensors. *Biosensors* **2020**, *10*, 56. [CrossRef] [PubMed]
58. Pham, C.; Bui, M.H.; Tran, V.A.; Vu, A.D.; Tran, C. Personalized breath-based biometric authentication with wearable multimodality. *IEEE Sens. J.* **2022**, *23*, 536–543. [CrossRef]
59. Graña Possamai, C.; Ravaud, P.; Ghosn, L.; Tran, V.T. Use of wearable biometric monitoring devices to measure outcomes in randomized clinical trials: A methodological systematic review. *BMC Med.* **2020**, *18*, 310. [CrossRef]
60. Mata-Romero, M.E.; Simental-Martínez, O.A.; Guerrero-Osuna, H.A.; Luque-Vega, L.F.; Lopez-Neri, E.; Ornelas-Vargas, G.; Castañeda-Miranda, R.; Martínez-Blanco, M.d.R.; Nava-Pintor, J.A.; García-Vázquez, F. A Low-Cost Wearable Device to Estimate Body Temperature Based on Wrist Temperature. *Sensors* **2024**, *24*, 1944. [CrossRef] [PubMed]
61. D'Amelio, A.; Patania, S.; Bursic, S.; Cuculo, V.; Boccignone, G. Using gaze for behavioural biometrics. *Sensors* **2023**, *23*, 1262. [CrossRef] [PubMed]
62. Zhang, R.; Xu, Q.; Wang, S.; Parkinson, S.; Schoeffmann, K. Information Difference of Transfer Entropies between Head Motion and Eye Movement Indicates a Proxy of Driving. *Entropy* **2023**, *26*, 3. [CrossRef]
63. Jin, Z.; Teoh, A.B.J.; Goi, B.M.; Tay, Y.H. Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognit.* **2016**, *56*, 50–62. [CrossRef]
64. Parkinson, S.; Khan, S.; Crampton, A.; Xu, Q.; Xie, W.; Liu, N.; Dakin, K. Password policy characteristics and keystroke biometric authentication. *IET Biom.* **2021**, *10*, 163–178. [CrossRef]
65. Sadkhan, E.S.B.; Al-Shukur, B.K.; Mattar, A.K. Survey of biometrie based key generation to enhance security of cryptosystems. In Proceedings of the 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), Baghdad, Iraq, 9–10 May 2016; pp. 1–6.
66. Nagakrishnan, R.; Revathi, A. A robust cryptosystem to enhance the security in speech based person authentication. *Multimed. Tools Appl.* **2020**, *79*, 20795–20819. [CrossRef]
67. Aanjanadevi, S.; Palanisamy, V.; Aanjankumar, S. An Improved Method for Generating Biometric-Cryptographic System from Face Feature. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 1076–1079.

68. Sarkar, A.; Singh, B.K. A novel session key generation and secure communication establishment protocol using fingerprint biometrics. In *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*; Springer: Cham, Switzerland, 2020; pp. 777–805.
69. Tuiri, S.E.; Sabil, N.; Benamar, N.; Kerrache, C.A.; Koziel, G. An EEG based key generation cryptosystem using diffie-hellman and AES. In Proceedings of the 2019 2nd IEEE Middle East and North Africa COMMunications Conference (MENACOMM), Manama, Bahrain, 19–21 November 2019; pp. 1–6.
70. Wang, Y.; Li, B.; Zhang, Y.; Wu, J.; Yuan, P.; Liu, G. A biometric key generation mechanism for authentication based on face image. In Proceedings of the 2020 IEEE 5th International Conference on Signal and Image Processing (ICSIP), Nanjing, China, 23–25 October 2020; pp. 231–235.
71. Abdel-Ghaffar, E.A.; Daoudi, M. Personal authentication and cryptographic key generation based on electroencephalographic signals. *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 101541. [CrossRef]
72. Wang, P.; You, L.; Hu, G.; Hu, L.; Jian, Z.; Xing, C. Biometric key generation based on generated intervals and two-layer error correcting technique. *Pattern Recognit.* **2021**, *111*, 107733. [CrossRef]
73. Anees, A.; Chen, Y.P.P. Discriminative binary feature learning and quantization in biometric key generation. *Pattern Recognit.* **2018**, *77*, 289–305. [CrossRef]
74. Verma, G.; Liao, M.; Lu, D.; He, W.; Peng, X.; Sinha, A. An optical asymmetric encryption scheme with biometric keys. *Opt. Lasers Eng.* **2019**, *116*, 32–40. [CrossRef]
75. Kuznetsov, O.; Zakharov, D.; Frontoni, E. Deep learning-based biometric cryptographic key generation with post-quantum security. *Multimed. Tools Appl.* **2023**, *83*, 56909–56938. [CrossRef]
76. Roopak, M.; Khan, S.; Parkinson, S.; Armitage, R. Comparison of deep learning classification models for facial image age estimation in digital forensic investigations. *Forensic Sci. Int. Digit. Investig.* **2023**, *47*, 301637. [CrossRef]
77. Sarkar, A.; Singh, B.K. Cryptographic key generation from cancelable fingerprint templates. In Proceedings of the 2018 4th International Conference on recent Advances in Information Technology (RAIT), Dhanbad, India, 15–17 March 2018; pp. 1–6.
78. Suresh, K.; Pal, R.; Balasundaram, S. Two-factor-based RSA key generation from fingerprint biometrics and password for secure communication. *Complex Intell. Syst.* **2022**, *8*, 3247–3261. [CrossRef]
79. Salman, D.D.; Azeez, R.A.; Hossen, A.M.J. Key generation from multibiometric system using meerkat algorithm. *Eng. Technol. J.* **2020**, *38*, 115–127. [CrossRef]
80. Moosavi, S.R. PPG-KeyGen: Using photoplethysmogram for key generation in wearable devices. *Procedia Comput. Sci.* **2021**, *184*, 291–298. [CrossRef]
81. Sarkar, A.; Singh, B.K.; Bhaumik, U. Cryptographic key generation scheme from cancellable biometrics. In *Progress in Computing, Analytics and Networking: Proceedings of ICCAN 2017*; Springer: Singapore, 2018; pp. 265–272.
82. Kaur, H.; Khanna, P. PolyCodes: Generating cancelable biometric features using polynomial transformation. *Multimed. Tools Appl.* **2020**, *79*, 20729–20752. [CrossRef]
83. Shahreza, H.O.; Melzi, P.; Osorio-Roig, D.; Rathgeb, C.; Busch, C.; Marcel, S.; Tolosana, R.; Vera-Rodriguez, R. Benchmarking of cancelable biometrics for deep templates. *arXiv* **2023**, arXiv:2302.13286.
84. Alam, M.T.; Li, H.; Chowdhury, M. Cancellable multi-modal biometrie authentication for cloud based mobilityfirst like environment. In Proceedings of the 2016 IEEE 11th Conference on Industrial Electronics and Applications (ICIEA), Hefei, China, 5–7 June 2016; pp. 510–515.
85. Kim, J.; Teoh, A.B.J. One-factor cancellable biometrics based on indexing-first-order hashing for fingerprint authentication. In Proceedings of the 2018 24th International Conference on Pattern Recognition (ICPR), Beijing, China, 20–24 August 2018; pp. 3108–3113.
86. Carey, A.N.; Zhan, J. A cancelable multi-modal biometric based encryption scheme for medical images. In Proceedings of the 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA 10–13 December 2020; pp. 3711–3720.
87. Ghouzali, S.; Nafea, O.; Wadood, A.; Hussain, M. Cancelable multimodal biometrics based on chaotic maps. *Appl. Sci.* **2021**, *11*, 8573. [CrossRef]
88. Hossam Eldein Mohamed, F.A.; El-Shafai, W. Cancelable biometric authentication system based on hyperchaotic technique and fibonacci Q-Matrix. *Multimed. Tools Appl.* **2024**. [CrossRef]
89. Liu, H.; Gao, Y.; Liu, C.; Sun, J.; Guo, X.; Zhang, H.; Wan, W. CanBiPT: Cancelable biometrics with physical template. *Pattern Recognit. Lett.* **2023**, *172*, 213–220. [CrossRef]
90. Chai, T.Y.; Goi, B.M.; Tay, Y.H.; Jin, Z. A new design for alignment-free chaffed cancelable iris key binding scheme. *Symmetry* **2019**, *11*, 164. [CrossRef]
91. Asthana, R.; Walia, G.S.; Gupta, A. A novel biometric crypto system based on cryptographic key binding with user biometrics. *Multimed. Syst.* **2021**, *27*, 877–891. [CrossRef]
92. Ouda, O.; Nandakumar, K.; Ross, A. Cancelable biometrics vault: A secure key-binding biometric cryptosystem based on chaffing and winnowing. In Proceedings of the 2020 25th International Conference on Pattern Recognition (ICPR), Milan, Italy, 10–15 January 2021; pp. 8735–8742.
93. Tantubay, N.; Bharti, J. A Survey of Biometric Key-Binding Biocrypto-System Using Different Techniques. *Int. J. Emer. Tech.* **2020**, *11*, 421–432.

94. Riccio, D.; Galdi, C.; Manzo, R. Biometric/cryptographic keys binding based on function minimization. In Proceedings of the 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), Naples, Italy, 28 November–1 December 2016; pp. 144–150.
95. Zainulina, E.; Matveev, I. Binding Cryptographic Keys into Biometric Data: Optimization. *J. Comput. Syst. Sci. Int.* **2020**, *59*, 699–711. [CrossRef]
96. Gupta, S.; Buriro, A.; Crispo, B. A chimerical dataset combining physiological and behavioral biometric traits for reliable user authentication on smart devices and ecosystems. *Data Brief* **2020**, *28*, 104924. [CrossRef]
97. Revadigar, G.; Javali, C.; Xu, W.; Hu, W.; Jha, S. Secure key generation and distribution protocol for wearable devices. In Proceedings of the 2016 IEEE International Conference on Pervasive Computing and Communication Workshops (PerCom Workshops), Sydney, NSW, Australia, 14–18 March 2016; pp. 1–4.
98. Al-Odat, Z.A.; Al-Qtiemat, E.M.; Khan, S.U. An efficient lightweight cryptography hash function for big data and iot applications. In Proceedings of the 2020 IEEE Cloud Summit, Harrisburg, PA, USA, 21–22 October 2020; pp. 66–71.
99. Amin, R.; Islam, S.H.; Biswas, G.; Khan, M.K.; Leng, L.; Kumar, N. Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks. *Comput. Netw.* **2016**, *101*, 42–62. [CrossRef]
100. Gilkalaye, B.P.; Rattani, A.; Derakhshani, R. Euclidean-distance based fuzzy commitment scheme for biometric template security. In Proceedings of the 2019 7th International Workshop on Biometrics and Forensics (IWBF), Cancun, Mexico, 2–3 May 2019; pp. 1–6.
101. Xu, W.; Javali, C.; Revadigar, G.; Luo, C.; Bergmann, N.; Hu, W. Gait-key: A gait-based shared secret key generation protocol for wearable devices. *ACM Trans. Sens. Netw. (TOSN)* **2017**, *13*, 1–27. [CrossRef]
102. Lutsenko, M.; Kuznetsov, A.; Kiian, A.; Smirnov, O.; Kuznetsova, T. Biometric cryptosystems: Overview, state-of-the-art and perspective directions. In *Advances in Information and Communication Technology and Systems*; Springer: Cham, Switzerland, 2019; pp. 66–84.
103. Yang, W.; Wang, S.; Sahri, N.M.; Karie, N.M.; Ahmed, M.; Valli, C. Biometrics for internet-of-things security: A review. *Sensors* **2021**, *21*, 6163. [CrossRef] [PubMed]
104. Al-Saggaf, A.A. Key binding biometrics-based remote user authentication scheme using smart cards. *IET Biom.* **2018**, *7*, 278–284. [CrossRef]
105. Jiang, Q.; Chen, Z.; Ma, J.; Ma, X.; Shen, J.; Wu, D. Optimized fuzzy commitment based key agreement protocol for wireless body area network. *IEEE Trans. Emerg. Top. Comput.* **2019**, *9*, 839–853. [CrossRef]
106. Dwivedi, R.; Dey, S.; Singh, R.; Prasad, A. A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping. *Comput. Secur.* **2017**, *65*, 373–386. [CrossRef]
107. Bharathi, P.; Annam, G.; Kandi, J.B.; Duggana, V.K.; Anjali, T. Secure file storage using hybrid cryptography. In Proceedings of the 2021 6th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 8–10 July 2021; pp. 1–6.
108. Chaloop, S.G.; Abdullah, M.Z. Enhancing Hybrid Security Approach Using AES And RSA Algorithms. *J. Eng. Sustain. Dev.* **2021**, *25*, 58–66. [CrossRef]
109. Jaspin, K.; Selvan, S.; Sahana, S.; Thanmai, G. Efficient and secure file transfer in cloud through double encryption using AES and RSA Algorithm. In Proceedings of the 2021 international conference on emerging smart computing and informatics (ESCI), Pune, India, 5–7 March 2021; pp. 791–796.
110. Kumar, S.; Karnani, G.; Gaur, M.S.; Mishra, A. Cloud security using hybrid cryptography algorithms. In Proceedings of the 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, UK, 28–30 April 2021; pp. 599–604.
111. William, P.; Choubey, A.; Chhabra, G.; Bhattacharya, R.; Vengatesan, K.; Choubey, S. Assessment of hybrid cryptographic algorithm for secure sharing of textual and pictorial content. In Proceedings of the 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 16–18 March 2022; pp. 918–922.
112. Almaiah, M.A.; Dawahdeh, Z.; Almomani, O.; Alsaaidah, A.; Al-Khasawneh, A.; Khawatreh, S. A new hybrid text encryption approach over mobile ad hoc network. *Int. J. Electr. Comput. Eng. (IJECE)* **2020**, *10*, 6461–6471. [CrossRef]
113. Yahaya, M.M.; Ajibola, A. Cryptosystem for secure data transmission using Advance Encryption Standard (AES) and Steganography. *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. (IJSRCSEIT)* **2019**, *5*, 317–322. [CrossRef]
114. Pawar, H.R.; Harkut, D.G. Classical and quantum cryptography for image encryption & decryption. In Proceedings of the 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE), San Salvador, El Salvador, 22–24 August 2018; pp. 1–4.
115. Timothy, D.P.; Santra, A.K. A hybrid cryptography algorithm for cloud computing security. In Proceedings of the 2017 International Conference on Microelectronic Devices, Circuits and Systems (ICMDCS), Vellore, India, 10–12 August 2017; pp. 1–5.
116. Rezaei, B.; Mobasseri, M.; Enayatifar, R. A secure, efficient and super-fast chaos-based image encryption algorithm for real-time applications. *J. Real-Time Image Process.* **2023**, *20*, 30. [CrossRef]
117. Zhang, B.; Liu, L. Chaos-based image encryption: Review, application, and challenges. *Mathematics* **2023**, *11*, 2585. [CrossRef]
118. Shen, Y.; Huang, J.; Chen, L.; Wen, T.; Li, T.; Zhang, G. Fast and secure image encryption algorithm with simultaneous shuffling and diffusion based on a time-delayed combinatorial hyperchaos map. *Entropy* **2023**, *25*, 753. [CrossRef] [PubMed]
119. Bhandari, R.; Kirubanand, V. Enhanced encryption technique for secure iot data transmission. *Int. J. Electr. Comput. Eng.* **2019**, *9*, 3732. [CrossRef]

120. Seth, B.; Dalal, S.; Jaglan, V.; Le, D.N.; Mohan, S.; Srivastava, G. Integrating encryption techniques for secure data storage in the cloud. *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4108. [CrossRef]
121. Sharma, K.; Agrawal, A.; Pandey, D.; Khan, R.A.; Dinkar, S.K. RSA based encryption approach for preserving confidentiality of big data. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 2088–2097. [CrossRef]
122. Shawkat, S.A.; Tagougui, N.; Kherallah, M. Optimization-based pseudo random key generation for fast encryption scheme. *Bull. Electr. Eng. Inform.* **2023**, *12*, 1007–1018. [CrossRef]
123. Albahar, M.A.; Olawumi, O.; Haataja, K.; Toivanen, P. Novel hybrid encryption algorithm based on aes, RSA, and twofish for bluetooth encryption. *J. Inf. Secur.* **2018**, *9*, 168–176. [CrossRef]
124. Meshram, C.; Lee, C.C.; Meshram, S.G.; Khan, M.K. An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment. *Soft Comput.* **2019**, *23*, 13127–13138. [CrossRef]
125. Gafsi, M.; Ajili, S.; Hajjaji, M.A.; Malek, J.; Mtibaa, A. High securing cryptography system for digital image transmission. In Proceedings of the 8th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT'18), Hammamet, Tunisia, 20–22 December 2022; Springer: Cham, Switzerland, 2020; Volume 1, pp. 311–322.
126. Kumar, D.; Grover, H.S.; Adarsh. A secure authentication protocol for wearable devices environment using ECC. *J. Inf. Secur. Appl.* **2019**, *47*, 8–15. [CrossRef]
127. Huang, W. ECC-based three-factor authentication and key agreement scheme for wireless sensor networks. *Sci. Rep.* **2024**, *14*, 1787. [CrossRef]
128. Javeed, K.; El-Mursy, A.; Gregg, D. Ec-crypto: Highly efficient area-delay optimized elliptic curve cryptography processor. *IEEE Access* **2023**, *11*, 56649–56662. [CrossRef]
129. Kaur, M.; Kumar, V. A comprehensive review on image encryption techniques. *Arch. Comput. Methods Eng.* **2020**, *27*, 15–43. [CrossRef]
130. Xu, W.; Revadigar, G.; Luo, C.; Bergmann, N.; Hu, W. Walkie-talkie: Motion-assisted automatic key generation for secure on-body device communication. In Proceedings of the 2016 15th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN), Vienna, Austria, 11–14 April 2016; pp. 1–12.
131. Mogos, G. Biometrics in cyber defense. In *Proceedings of the MATEC Web of Conferences*; EDP Sciences: Les Ulis, France, 2020; Volume 309, p. 02003.
132. Su, Y.; Li, Y.; Cao, Z. Gait-Based Privacy Protection for Smart Wearable Devices. *IEEE Internet Things J.* **2023**, *11*, 3497–3509. [CrossRef]
133. Hwang, H.B.; Lee, J.; Kwon, H.; Chung, B.; Lee, J.; Kim, I.Y. Preliminary Study of Novel Bio-Crypto Key Generation Using Clustering-Based Binarization of ECG Features. *Sensors* **2024**, *24*, 1556. [CrossRef] [PubMed]
134. Revadigar, G.; Javali, C.; Xu, W.; Vasilakos, A.V.; Hu, W.; Jha, S. Accelerometer and fuzzy vault-based secure group key generation and sharing protocol for smart wearables. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 2467–2482. [CrossRef]
135. González-Manzano, L.; de Fuentes, J.M.; Peris-Lopez, P.; Camara, C. Encryption by Heart (EbH)—Using ECG for time-invariant symmetric key generation. *Future Gener. Comput. Syst.* **2017**, *77*, 136–148. [CrossRef]
136. Pirbhulal, S.; Wu, W.; Li, G. A biometric security model for wearable healthcare. In Proceedings of the 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, 17–20 November 2018; pp. 136–143.
137. Joshi, J.; Mittal, S.; Birdi, B.; Kumar, R.; Kurian, D.S.; Mukherjee, S.; Awasthi, P. Secure and wearable computing in WBANs. In Proceedings of the 2016 International Conference on Information and Communication Technology (ICICTM), Kuala Lumpur, Malaysia, 16–17 May 2016; pp. 65–70.
138. Alshaikh, O.; Parkinson, S.; Khan, S. Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: The need for a standardised approach. *Comput. Secur.* **2024**, *139*, 103694. [CrossRef]
139. Parkinson, S.; Vallati, M.; Crampton, A.; Sohrabi, S. GraphBAD: A general technique for anomaly detection in security information and event management. *Concurr. Comput. Pract. Exp.* **2018**, *30*, e4433. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.