technologies

MDPI

Review

Integration of Biometrics and Steganography: A Comprehensive Review

Ian McAteer, Ahmed Ibrahim, Guanglou Zheng *, Wencheng Yang and Craig Valli

Security Research Institute, School of Science, Edith Cowan University, Joondalup, WA 6027, Australia; imcateer@westnet.com.au (I.M.); ahmed.ibrahim@ecu.edu.au (A.I.); w.yang@ecu.edu.au (W.Y.); c.valli@ecu.edu.au (C.V.)

* Correspondence: g.zheng@ecu.edu.au

Received: 13 February 2019; Accepted: 28 March 2019; Published: 8 April 2019

Abstract: The use of an individual's biometric characteristics to advance authentication and verification technology beyond the current dependence on passwords has been the subject of extensive research for some time. Since such physical characteristics cannot be hidden from the public eye, the security of digitised biometric data becomes paramount to avoid the risk of substitution or replay attacks. Biometric systems have readily embraced cryptography to encrypt the data extracted from the scanning of anatomical features. Significant amounts of research have also gone into the integration of biometrics with steganography to add a layer to the defence-in-depth security model, and this has the potential to augment both access control parameters and the secure transmission of sensitive biometric data. However, despite these efforts, the amalgamation of biometric and steganographic methods has failed to transition from the research lab into real-world applications. In light of this review of both academic and industry literature, we suggest that future research should focus on identifying an acceptable level steganographic embedding for biometric applications, securing exchange of steganography keys, identifying and address legal implications, and developing industry standards.

Keywords: computer security; biometrics; steganography; data security; privacy; access control

1. Introduction

Biometric authentication is a popular and reliable access control technique and has become a standard feature in smartphones [1]. These applications, and indeed any biometric-related applications, require the secure storage of biometric features in a digital database for subsequent biometric template matching [2]. The storage of such sensitive data, therefore, requires secure encryption to ensure confidentiality. During the transmission of the encrypted data, steganography can be used to further enhance the security of the biometric authentication system. Such measures can be in the form of embedding biometric data to a carrier object, such as the facial image, either related or unrelated to the individual being authenticated [3].

Biometric data, as with any individual's personal information, can be exploited by cyber criminals to conduct identity theft, and its monetary value makes it a commodity that can be traded in underground marketplaces such as the dark web. The dark web consists of a hidden network of websites which can only be accessed via certain browsers that provide anonymising features to help obfuscate user identification [4]. The most recent information available on the value of stolen personal information on the dark web shows, for example, that values range from approximately $5 for a credit card to over $1000 for an individual's complete medical history [5].

The theft of biometric data enables a cyber criminal to potentially conduct replay or substitution attacks through which he gains access to much of the personal information, e.g., the social security number, credit or debit card information, driver's license, passport number. It is therefore critical that any barriers that add to the security of an individual's sensitive data be utilised. This is the principle of the defence-in-depth information security model, where overlapping multiple controls ensure security when one layer of security fails [6], as shown in Figure 1. For example, a biometric access control system provides a security layer around protected assets. Steganography applied to the biometric data of that system provides a separate and distinct security layer.

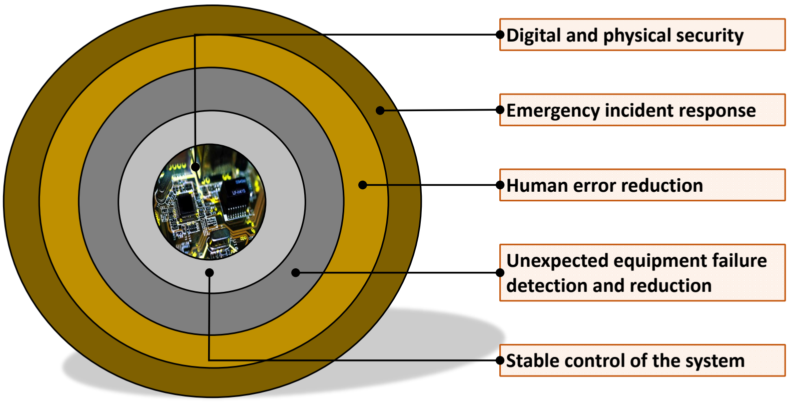
Digital and physical security
Emergency incident response
Human error reduction
Unexpected equipment failure detection and reduction
Stable control of the system

Figure 1. The defence-in-depth security model protects assets behind multiple defensive layers, each layer utilising a different strategy, so that if one layer is breached, overall security of the system is not compromised (Adapted from [6]).

There are advantages in amalgamating biometrics with steganography, such as augmenting the security of sensitive biometric information during transmission, and its adoption in real-world applications should be pursued. This paper aims to assess the current status of research in this field, determine why this work has not been embraced by industry, and assess whether the integration of biometrics and stegaography is a viable technology to strengthen layers of security.

The rest of the paper is organised as below. Sections 2 and 3 overview the principle methods used by biometrics and steganography respectively. In Section 4 we review our findings with regards to the integration of biometrics and steganography within the realms of academia and industry, discuss our subsequent interpretation of these findings. Section 5 assesses what future direction for research is required in this field, and the paper is then concluded in Section 6.

2. Biometrics

2.1. Overview

An individual's biometric characteristics can be utilised for identification and authentication purposes [7], of which there are two main categories:

(a) Physiological, which uses certain physical identifying attributes.
(b) Behavioural, which uses certain identifying attributes from an individual's movement or the manner in which they interact with peripheral devices.

Nowadays biometric technology has been widely used in different areas. For instance, it can be used to deal with challenges in the healthcare sector where doctors and patients can gain access to medical devices and systems by using their biometrics, e.g., fingerprints, instead of remembering and entering a complex password [7,8]. Meanwhile, the biometrics technology is also studied for the use of cattle identification and tracking in the agriculture sector [9,10].

The following sub-sections give a brief overview of the different biometric methods, for example, fingerprint authentication, facial recognition, and iris/retina recognition.

2.2. Fingerprint Authentication

The uniqueness of an individual's fingerprint, even between identical twins, has been exploited by law enforcement and forensic investigators for more than a century. Not only can a scan of a fingerprint be represented in an image format, but the key identifying points can be digitally captured at three levels [11].

(a) Level 1—macro details: such as friction ridge flow, pattern type (arch, loop, or whorl), and singular points.

(b) Level 2—minutiae: such as ridge ending, ridge bifurcations, independent ridge, island, ridge enclosure, spur, crossover, delta, and core.

(c) Level 3—dimensional attributes: such as ridge path deviation, ridge width, ridge shape, pores, edge contour, incipient ridges, creases, and scars.

Features from different levels can be utilised in fingerprint biometrics. Awad et al. [12,13] proposed to use singular points in fingerprint classification and compared the performance of different singular point detection methods. Among these features, minutiae points are commonly used in authentication because minutiae-based representation is efficient in terms of storage and computation [11,14].

Fingerprint authentication involves two stages: enrolment and verification [15,16]. During the enrolment stage, a fingerprint image is acquired from a sensor and is then processed in order to extract unique features. These features are regarded as a fingerprint template and stored in a secure template database. During the verification stage, the same process is followed to extract fingerprint query features. A matching process is performed by comparing the query features with the stored template and calculating a similarity score. If the score is higher than a pre-defined threshold, then the query fingerprint is considered to match the template, and the authentication result is 'success'. Otherwise, the authentication fails. Figure 2 describes steps in a fingerprint authentication process.

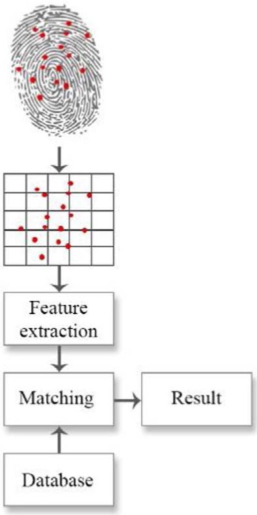

Figure 2. Fingerprint authentication involves image acquisition, image processing, feature extraction, and subsequent comparison to registered fingerprint features stored in a template database [17].

2.3. Facial Recognition

At its simplest form, facial recognition can be done manually to compare a photograph on an identity card with the face of the bearer of that card. However, the human face can also be represented digitally in the form of eigenfaces. Eigenfaces are constructed by performing principal component analysis (PCA) on a large set of facial imagery and are represented as a set of eigenvectors. They are, in effect, the sum of chosen components from a collection of standardised facial ingredients that best represent a subject's face [18].

Like fingerprint data, facial data can also be represented in both an image format and as digital data. A face-recognition system (FRS) follows a similar two-phase approach of enrolment and verification as applied in a fingerprint authentication process (see Figure 3).

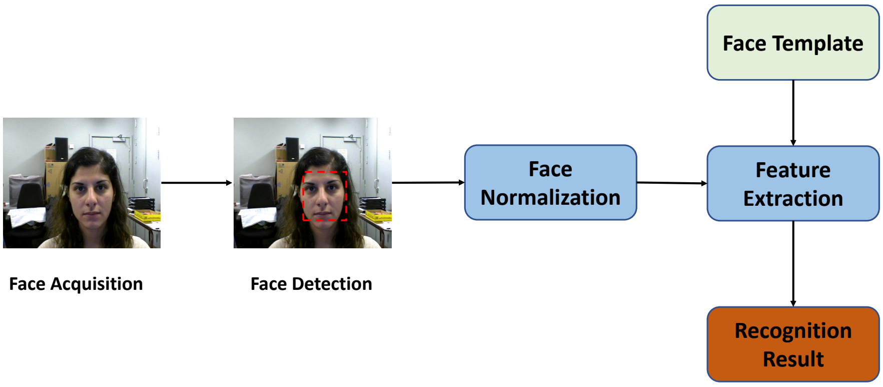

Figure 3. A face-recognition system (FRS) has seven main modules, consisting of enrolment, detection, normalisation, feature extraction, template storage, feature matching, and decision-making stages [19].

2.4. Iris and Retina Detail

The iris and retina detail in an individual's eye is as unique as their fingerprint. Both of these characteristics can be used for identification and authentication purposes, with the registration process securely encrypting the iris and retina detail as a digital code. Not only is the iris a particularly accurate biometric parameter for authentication, but its physiological characteristics can be determined as an immediate liveness check [20].

An iris and retina recognition system again follows the enrolment and verification two-phase approach as applied in fingerprint and face recognition (see Figure 4). A fresh biometric sample is processed before unique identifying features are extracted. These features are then compared to template stored in a secure database for the matching and decision-making stages.

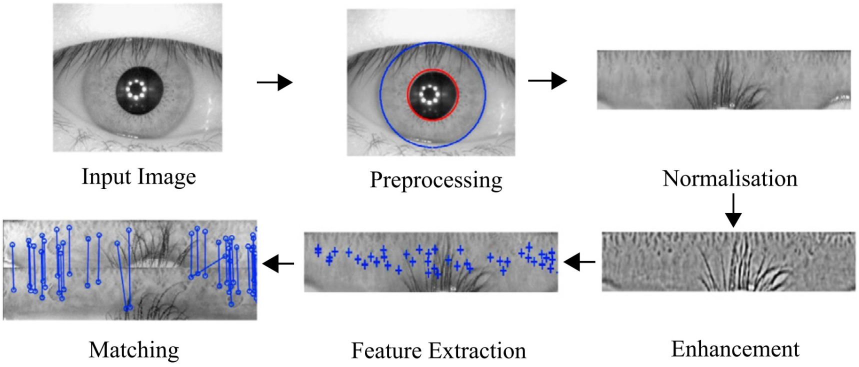

Figure 4. An iris recognition system will usually consist of eight modules, consisting of acquisition, preprocessing, normalisation, enhancement, feature extraction, template storage, feature matching, and decision-making stages [21].

2.5. Other Methods

Fingerprint [11,22], facial recognition [23], and iris [20]/retina detail are all physiological biometric parameters. Other physiological parameters available in the field of biometrics include vein recognition [24], ear recognition [25], palm print recognition [26], hand geometry [27], finger geometry [28], lip furrows [29,30], DNA [31], and odour/scent recognition [32]. Behavioural parameters that can be useful in biometric-detection of an individual include keyboard dynamics [33], gait [34], voice recognition [35], and signature [36,37].

Each of these methods again involve separate enrolment and verification phases, such as the example shown in Figure 5 which is related to keyboard dynamics. Recent advances in keyboard-dynamics research can amalgamate audio into the dynamics parameters to augment liveness checks to the authentication process [38].

The preferred choice of biometric technology is highly dependent on the application for which it is to be used. There are several parameters to consider:

- Ease of use—high for fingerprint, hand geometry, signature and voice. Low for retina scans.
- Sources of error—dirt, dryness, injury, age, glasses, lighting, hair, background noise, behavioural changes over time.
- Accuracy—highest for retina and iris scans.
- User acceptance—highest for signature and voice.
- Stability over time—highest for fingerprint, retina, and iris.
- Cost—variable depending on the level of technology employed.

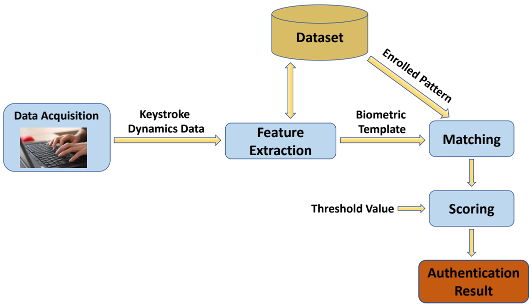

Figure 5. Keyboard dynamics involves an enrolment stage in which a support vector machine (SVM) is used for the learning step and the output is stored in a template database. A verification stage compares the results of the SVM algorithm for a new biometric capture with stored templates. If the decision shows agreement, the data from the new biometric capture replaces the stored template to cater for changes in behavioural characteristics over time [39].

2.6. *Advantages and Disadvantages of Typical Biometric Methods*

All biometric methods have advantages and disadvantages which are summarised in Table 1.

Table 1. Advantages and disadvantages of typical biometric methods [40–43].

Biometric Method	Advantages	Disadvantages
Physiological Characteristics:		
Fingerprint	• Ease of use. • User comfort. • Low cost. • Low power consumption. • Use in portable equipment (e.g., smart phones). • Characteristics remain stable over time.	• Dirt. • Cuts. • Wear and tear on ridge patterns. • Low-cost systems fooled by prosthetic or artificial fingers.
Face	• Ease of use. • No direct contact with subject. • Low cost. • High capacity (e.g., airport immigration).	• Varying light conditions. • Face angle (rotation). • Varying facial expressions. • Cultural issues (e.g., wearing of burqas).

Table 1. *Cont.*

Biometric Method	Advantages	Disadvantages
Iris	• Ease of use. • High accuracy. • Use in portable equipment (e.g., smart phones). • Characteristics remain stable over time.	• High cost. • Requires close proximity to the subject. • Varying light conditions.
Retina	• High accuracy.	• User discomfort. • High cost. • Glasses or coloured contact lenses worn by subject. • Potential variation in characteristics with changes in blood pressure.
Vein Geometry	• Ease of use. • Very low false acceptance rate. • Low risk of forgery. • Characteristics remain stable over time. • Only low image-resolution required. • Not affected by dirt, cuts, or wear and tear.	• High cost. • Requires installation of larger equipment. • Low capacity.
Ear Geometry	• Less intrusive than iris/retina recognition.	• Limited unique ear characteristics. • Low accuracy.
Palm Print	• Can be low-cost by adapting office-based scanner equipment. • Low-resolution imagery may be sufficient. • Resistance to ageing.	• Illumination variations. • Distortions due to hand movements.
Hand Geometry	• Ease of use. • User comfort.	• High cost. • Requires 3D-scan technology. • Wearing of jewellery (e.g., rings). • Changes during child/teenage years. • May be difficult to use for disabled or arthritis sufferers.
Lip Furrows	• Ease of use. • User comfort. • Characteristics remain stable over time.	• Relies on static mouth/face photos. • Varying facial expressions. • Dry/cracked lips. • Visibility of teeth may reduce accuracy. • Wearing of cosmetics (e.g., lipstick, lip balm) may cover essential features in images or smear prints.
DNA	• Unchanged over time.	• Subject compliance. • High cost. • Analysis is time-consuming.
Odour/Scent	• No worthwhile advantages.	• Insufficient technical advances in ’artificial noses’ to be viable at present. • Natural odours masked by deodorants/perfumes.
Behavioural Characteristics:		
Keyboard Dynamics	• Ease of use.	• Lengthy enrolment process. • Low accuracy negates recognition potential.

Table 1. *Cont.*

Biometric Method	Advantages	Disadvantages
Mouse Dynamics	• Ease of use.	• Lengthy enrolment process. • Affected by mouse sensitivity. • Low accuracy.
Gait	• No direct contact with subject.	• May be affected by a change of footwear, walking surface, walking direction, or clothing.
Voice	• Ease of use. • User comfort. • Suitable for disabled who may not be able to use hand/finger technologies.	• Low accuracy, particularly with background noise present. • Requires close proximity to the subject to minimise errors. • Use of prerecorded messages. • High cost.
Signature	• Ease of use. • Readily accepted.	• Can vary from one signature to the next, over longer time periods, or with changes in emotion.

2.7. Security of Biometric Authentication Systems

The majority of present-day authentication and verification systems are dependent on the 'something you have' philosophy, which requires users to remember multiple passwords or to possess tokens that, for example, generate one-time pin (OTP) numbers. Passwords, however, can be easily forgotten or can become compromised if they are written down. Tokens can be lost, so that access to the required services becomes unavailable until the token is replaced. An individual's biometric parameters, both physiological and behavioural, can uniquely identify a person using their personal characteristics so that there is no need to remember passwords or carry a token. These biometric traits do not need to be remembered and can rarely be lost (only, for example, through severe injury to fingers or eyes). While biometric user-authentication and verification is convenient to use, it does make the security of the digitised biometric data a critical matter. If this data is accessed by an adversary, it can be used to conduct attacks by various means. Akhtar (2012) [44] identifies the eight attack points which an adversary might exploit to compromise such a system as shown in Figure 6.

This use of the 'something you are' philosophy to diversify and add robustness to the user identification and authentication process requires each user's biometric parameters to be registered and securely stored in a template database.

Five main components are involved in a biometric authentication system:

(a) A biometric sensor.
(b) A biometric feature extractor.
(c) A secure database to hold registered biometric templates.
(d) A matcher to compare stored biometric information with data extracted from a new scan from the same user.
(e) A decision maker to permit or deny access based on the accuracy of the match.

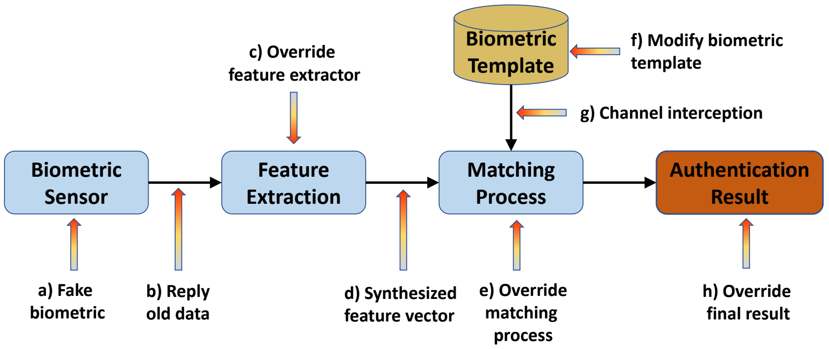

Figure 6. Biometric authentication system attack points [44].

(1) An attack on the sensor.
(2) The resubmission of previously stored data (replay attack).
(3) Override the feature extractor.
(4) The submission of false biometric feature representation (substitution attack).
(5) An attack on the matcher.
(6) The alteration of stored biometric templates (modification attack).
(7) The alteration of data in transit between template database and matcher (interception attack).
(8) Override the final accept/reject decision.

Sensitive data is subsequently at risk throughout a biometric authentication system, and the security measures implemented to protect this data must cover all contingencies. Security can be applied in three ways:

(a) Cryptography—the secure encryption of digitised data whereby the contents can only be decrypted if the recipient has the appropriate key.
(b) Watermarking—the overt embedding of, for example, a visible mark in order to provide authentication of a biometric image.
(c) Steganography—the covert embedding of, for example, digitised biometric data into a host image file so that the real purpose of the host image is obscured.

Of these cryptography and watermarking have been readily accepted by industry as proven techniques, and this will continue to be the case for all biometric authentication systems. Conversely, the use of steganography to provide additional security for biometric data in transit has struggled for even fundamental acceptance.

3. Steganography

3.1. Overview

Steganography, the process of concealing sensitive information within a host or carrier medium, has been practised in various forms for centuries [45]. Of particular interest in the context of biometric authentication is the embedding of encrypted biometric data within a host image before transmission. The host image may or may not be related to the individual whose biometric data is being hidden. For example, the use of a facial host image of the individual concerned can augment identification for access control purposes [46]. Alternatively, a completely unrelated host can be used to keep the individual's identity a secret.

Combining steganography with other security techniques, e.g., cryptography or authentication, can improve the security level of a system significantly with a minimum overhead. Challita et al. [47] and Mahale et al. [48] studied the combination of cryptography and steganography in order to achieve a higher level security for a system. Pitropakis et al. [49] proposed an authentication scheme for a cloud-based environment by using two-factor authentication credentials (username, password and a key) where the key is hidden in a stego-message.

For steganography to be successful in the context of biometric authentication, the sole requirement is that the presence of the embedded data cannot be detected. However, the image output of the steganographic process commonly referred to as a 'stego' image, must also be resistant against the embedded secret information becoming irretrievable as a result of, for example, compression, tampering, or image distortion.

The following four generic embedding techniques can be found in the literature, particularly for image steganography:

3.2. Least Significant Bit (LSB) Embedding

Each pixel of a red–green–blue (RGB) image is represented by 24 bits, which is an 8-bit binary string covering decimal values 0 to 255 for each of the three red, green, and blue channels. The least significant bit (LSB) of one of these strings is the last (or right-most) binary integer that gives the unit value [50].

Deliberate alteration of the LSB, or indeed the last two binary digits, can be used to embed secret information into that pixel without the change being detectable to the human eye viewing the image [51].

3.3. Discrete Cosine Transform (DCT) Embedding

Discrete cosine transform (DCT) is a mathematical transformation which takes an image block in a spatial domain and transforms it into a frequency domain consisting of high, medium, and low-frequency components or sub-bands. JPEG compression is an example of where DCT is used, the process being shown in Figure 7. Each of these frequency sub-bands contains redundancies into which secret information can be embedded [52].

Once the embedding is complete, an inverse DCT algorithm is applied to transform the signal coefficients back to the spatial domain [52].

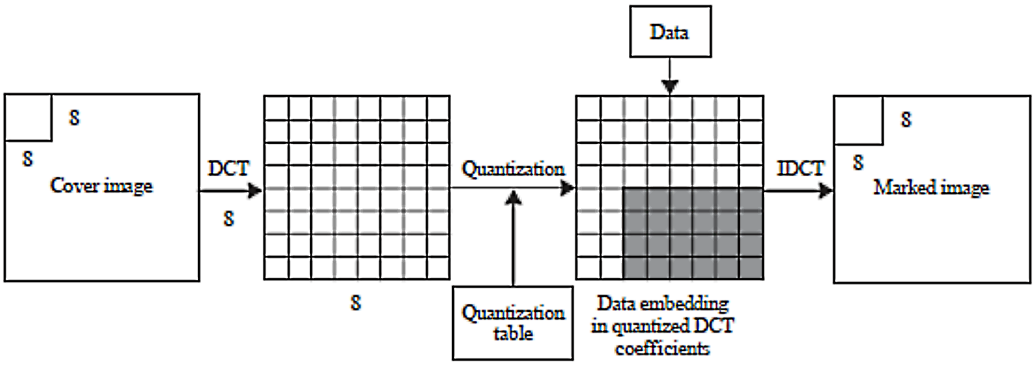

Figure 7. Discrete cosine transform (DCT)-based data-hiding using the JPEG compression model. A cover image is divided into 8 × 8-sized non-overlapping blocks, each block is applied to DCT in a raster scan order, and the transformed DCT coefficients are quantised using a quantization table. As a result of this process secret data can be embedded [53].

3.4. Discrete Wavelet Transform (DWT)

Discrete wavelet transform (DWT) is a mathematical transformation which takes an image's wavelet in the spatial domain and transforms it into the frequency domain. However, the main difference between DWT and DCT is in the high-pass bands. DWT provides lower frequency resolution, but higher spatial resolution. It, therefore, contains fewer sub-bands compared to DCT but has improved spatial resolution [54]. Figure 8 shows how decomposition of the original image through mathematical transformation occurs.

As with DCT, DWT frequency sub-bands contain redundancies for embedding secret information. An inverse DWT algorithm applied after embedding returns the properties to the spatial domain [55].

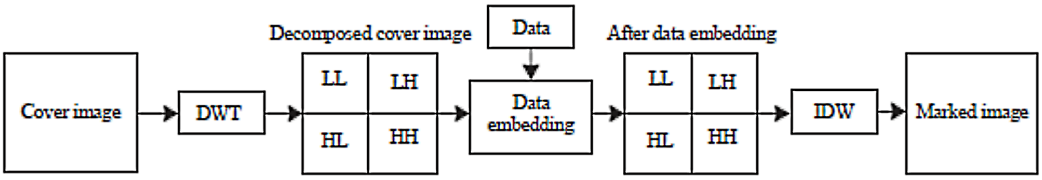

Figure 8. Discrete wavelet transform (DWT)-based data-hiding. A cover image is decomposed by a row and column operations into two low frequency (L) and high frequency (H) components. After image decomposition, the embedding algorithm is performed on the sub bands [53].

3.5. Object-Oriented Embedding (OOE)

Research into the potential embedding capacity of different images led to the concept of regions of interest (ROI) [56]. In particular, it was found that areas of skin tone in colour photographs had the highest potential embedding capacity, and this is another facet in which one aspect of biometrics, namely face recognition, and steganography converge. The percentages and relative proportions of red, green, and blue components for individual pixels can be utilised to determine whether a pixel represents skin-colour or not. Different definition parameters apply according to lighting conditions (e.g., uniform daylight, angled daylight, or flashlight illumination), and skin type (e.g., fair or dark complexion) [57].

Figure 9 shows a step-by-step approach to object-oriented embedding proposed by Cheddad et al. [58]. This process involves the following steps, which includes a skin-segmentation method researched by Zhao et al. [59]:

(A) Selection of the host image to be used.
(B) Region of interest segmentation to highlight skin-tone areas.
(C) Determination of the eye-centre locations.
(D) Separation of the eye regions.
(E) Distance transformations based on facial features, which are determined for calculations to reduce rotational-distortion errors.
(F) Construction of ellipses, with centre equidistant between the eye centres, minor axis length equal to the distance between eye centres, and the major axis length equal to twice the minor axis length.
(G) Selection of the biometric data to be embedded.
(H) Encryption of the biometric data to be embedded.
(I) Production of the stego-image consisting of the encrypted biometric data embedded into the host image.

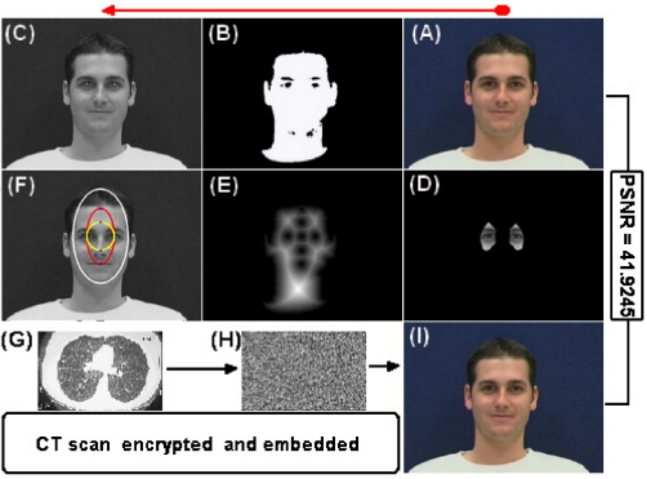

Figure 9. Object-oriented embedding. A proposed skin-based steganography system for hiding medical data in a face image: original image (**A**), skin blob of the segmented skin area (**B**), eyes' centroid detection (**C**), eye regions (**D**), distance transformation based on face features (**E**), construction of ellipses (**F**), CT scan image (**G**), CT scan encrypted (**H**) and stego-image carrying the embedded CT image (**I**) [58].

3.6. Advantages and Disadvantages of Selected Steganographic Methods

Steganographic methods have advantages and disadvantages which are are summarised in Table 2. Parameters such as ease of implementation, processing speed, embedding capacity, robustness against image modification, and security are taken into account.

Table 2. Advantages and disadvantages of some steganographic methods [60–62].

Steganographic Method	Advantages	Disadvantages
Least Significant Bit (LSB)	• Easy implementation. • Fast. • High capacity when using 4-LSB embedding.	• Vulnerable to steganalysis attacks in the spatial domain. • Loss of image quality with greater than three bits embedded per pixel.
Discrete Cosine Transform (DCT)	• Easy implementation. • Robust against cropping and compression.	• Lower embedding capacity. • Poor quality. • Low security.
Discrete Wavelet Transform (DWT)	• Highly secure. • Robust against cropping and compression.	• Complex technique requiring considerable computational resources. • Only moderate embedding capacity. • Requires considerable auxiliary data to be reversible.
Object-Oriented Embedding (OOE)	• Enhanced security. • Robust against cropping and compression.	• Dependent on embedding algorithm used.

4. Integration of Biometrics and Steganography

The integration of biometrics and steganography had been addressed by very few research papers. This subject matter is also largely absent from digital libraries, standards, and industry articles in such fields as eHealth, law enforcement, and cyber security.

From the survey of literature selected, we can broadly identify the following main categories:

(a) Types of biometric features utilised
(b) Methods of steganography employed
(c) Other methods or applications.

An overall summary of the methodologies (or sub-categories) found within these three main groups can be found in Table 3. The existence of any of the methodologies, as defined in each column, existing within each research paper, as defined in each row, was check-marked. The distribution of the total count for each sub-category within each main category is then shown in Table 4.

A graphical representation of the relative frequency that particular biometric, steganographic, and other pertinent features are shown in the Figures 10–12. Biometric feature types are dominated by fingerprint and facial data. This is likely due to these types being more accessible through online databases for research purposes. Steganographic methods are dominated by LSB, which are the techniques that have been researched the longest. Research into the more recent developments of DCT, DWT, and OOE are fairly evenly distributed. The almost ubiquitous use of cryptography for transmitting sensitive data is reflected in the distribution of other methods. The smallest portion being application-specific is reflective of the failure of the integration of biometrics and steganography to be embraced in the real-world setting.

Table 3. Features incorporated in research reviewed.

	Biometrics					**Steganography**					**Other**			
Research Paper	**Fingerprint Minutiae**	**Face Image**	**Iris or Retina Detail**	**Keyboard Dynamics**	**Skin-Tone Detection**	**LSB (Spatial Domain)**	**DCT (Spectral Domain)**	**DWT (Spectral Domain)**	**Object Oriented**	**Other or Unspecified**	**Cryptography**	**Application Specific**	**Assumes Key Pre-Sharing**	**Authentication**
Jain and Uludag (2003) [46]	✔	✔						✔					✔	✔
Ambalakat (2005) [63]	✔	✔	✔							✔			✔	✔
Ihmaidi et al. (2006) [64]	✔									✔	✔	✔	✔	✔
Cheddad et al. (2008) [56]		✔			✔	✔	✔	✔	✔				✔	
Kant et al. (2008) [65]	✔					✔					✔		✔	✔
Agrawal and Savvides (2009) [66]	✔	✔	✔				✔				✔		✔	✔
Chedded et al. (2009) [58]					✔			✔	✔				✔	
Na et al. (2010) [67]			✔				✔				✔		✔	✔
Shejul and Kulkami (2010) [54]					✔			✔	✔				✔	
Barve and et al. (2011) [68]					✔			✔	✔				✔	
Kapczyński and Banasik (2011) [51]	✔			✔		✔							✔	✔
Katiyar et al. (2011) [69]	✔					✔					✔	✔	✔	✔
Shejul and Kulkami (2011) [70]					✔			✔	✔				✔	
Sonsare and Sapkal (2011) [71]	✔	✔	✔			✔	✔				✔		✔	
Shanthini and Swamynathan (2012) [72]	✔	✔				✔					✔		✔	✔
Al-Assam et al. (2013) [73]	✔	✔	✔			✔		✔			✔		Once only	✔
Whitelam et al. (2013) [74]	✔	✔				✔					✔		✔	✔

Table 4. Distribution of categories from data compiled in Table 3.

Category	Count	Percentage
Biometrics:		
Fingerprint Minutiae	11	36.67%
Face Image	8	26.67%
Iris or Retina Detail	5	16.67%
Keyboard Dynamics	1	3.33%
Skin-Tone Detection	5	16.67%
Steganography:		
LSB (Spatial Domain)	8	30.77%
DCT (Spectral Domain)	4	15.38%
DWT (Spectral Domain)	7	26.92%
Object-Oriented	5	19.23%
Other or Unspecified	2	7.69%
Other:		
Cryptography	9	81.82%
Application-Specific	2	18.18%

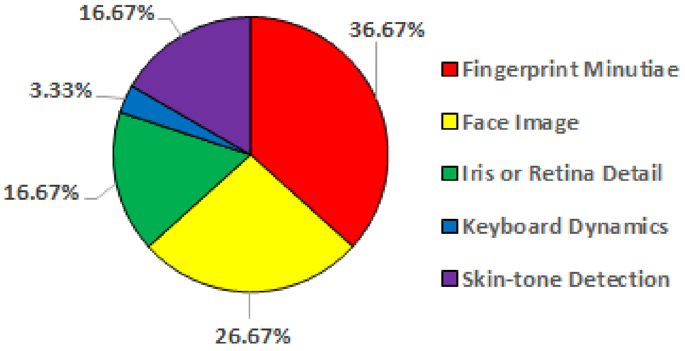

Figure 10. Distribution of biometric feature types.

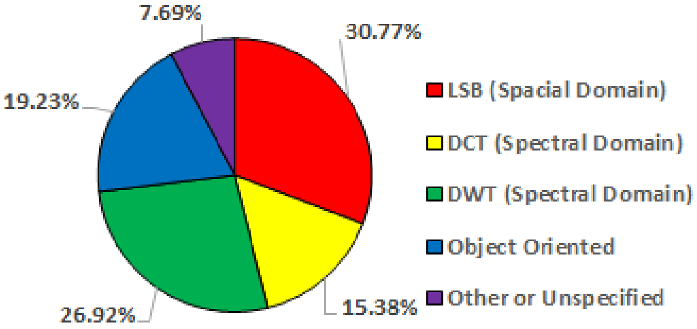

Figure 11. Distribution of steganographic methods.

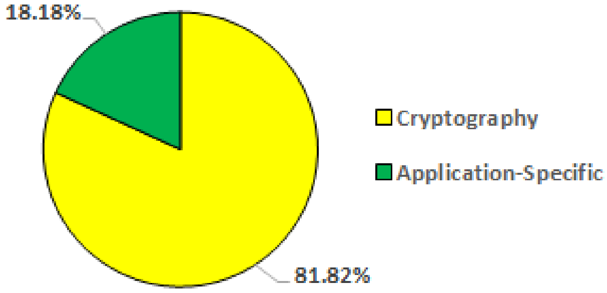

Figure 12. Distribution of other methods/applications.

Based on the literature reviewed, only two potential applications encompassing the integration biometrics and steganography have been proposed, although neither has been applied in the real-world setting:

(a) Secure online voting systems as proposed, for example, by Katiyar et al. (2011) [69]. Katiyar et al. [69] combined simultaneous cryptography and LSB steganography to propose a biometric and password security method applicable to an online voting system. Their system requires pre-existing biometric and key information at both ends of the system before voting takes place.

(b) Secure online shopping systems as proposed, for example, by Ihmaidi et al. (2006) [64]. The Ihmaidi et al. [64] paper discusses a proposed online shopping system that involves a customer receiving an online shopping card and software. The software issues a unique electronic internet shopping card (EISC) image embedded with customer information, including a fingerprint scan, and transaction details. However, there are two problems: (1) the paper does not indicate whether the card issuer or the customer supplies the fingerprint scanner, and (2) the system ties the customer to the PC to which the fingerprint scanner is connected to conduct online shopping.

Akoura Biometrics Inc., founded in 2002, devised a software product that integrated steganography and biometrics [75]. Akoura believed at that time that they were the first company to combine these methods. Its software products were inspired by corporate concerns over the regulations on the safe and secure transmission of information in the health sector (as defined by the Health Information Portability and Accountability Act (HIPAA) 1996 [76]) as well as in the financial sector (as defined by the Gramm–Leach–Bliley Act 1999 [77]).

The Akoura system [75] required senders and receivers to be registered (i.e., it relied on pre-sharing of keys). They used steganography in combination with encryption to ensure security against man-in-the-middle attacks. If all permissions were satisfied, the receiver then used his or her fingerprint to decrypt the message and extract the hidden image or document. We were unable to find other systems, particularly in the health or finance sectors.

Our intuition at this stage was that, if industry had embraced integration of steganography for its privacy preserving and security enhancing capabilities, appropriate standards or policies would address its governance, for example in eHealth. The security and privacy of medical records are paramount to eHealth. Therefore, the following health related standards and committees were investigated:

- Health Legislation Amendment (eHealth) Act 2015, No. 157, 2015, assented to 26 November 2015 [78].
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104–191, enacted on 21 August 1996 [76].

- Digital Imaging and Communications in Medicine (DICOM), the standard for the communication and management of medical imaging information and related data [79].
- Health Level Seven International, a framework (and related standards) for the exchange, integration, sharing, and retrieval of electronic health information [80].
- UN/CEFACT, the United Nations Centre for Trade Facilitation and Electronic Business [81].
- UN/EDIFACT, United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport [82].
- OASIS, "Advancing open standards for the information society" [83].
- eStandards CSA, a European consortium work-in-progress on "eHealth standards and Profiles in Action for Europe and Beyond" [84].
- CEN/TC 251, a European Committee for Standardisation (CEN) work-in-progress to standardise European Union Health Information and Communications Technology (ICT) [85].
- ISO/IEEE 11073, medical/health device communication standards enable communication between medical, health care and wellness devices and with external computer systems [86].

The search of standards for biometrics/steganography integration was further expanded to encompass information technology (IT) as a whole. There are many standards specific to the various aspects of biometrics, such as ISO/IEC-17922 (telebiometric authentication framework using biometric hardware security module), ISO/IEC-19792 (security evaluation of biometrics), ISO/IEC-24745 (biometric information protection), and ISO/IEC-24761 (authentication context for biometrics) [87]. Additionally, it is notable that there are several standards for cryptography, for example ISO/IEC-15946 (cryptographic techniques based on elliptic curves), ISO/IEC-18033 (encryption algorithms), ISO/IEC-19772 (authenticated encryption), and ISO/IEC-19790 (security requirements for cryptographic modules). However, there are no equivalents for steganography [87]. Our interpretation of this finding suggests that this may be indicative of biometrics and cryptography being considered as industry-proven, whereas steganography is being undermined by a perception that it is not a mature technology.

The websites for several biometric system manufacturers (for example, NEC NeoFace [88], UniLink [89], Damstra [90], M2Sys [91], ISCS [92]) and the website findbiometrics.com [93] were also investigated, but no reference to steganography could be found. The same outcome resulted from searching biometric access control system manufacturers (for example, HID Global [94], Germalto [95], Kisi [96], Abloy [97]).

The integration of biometrics with steganography can be achieved in two principle ways [58,63]:

(a) The embedding of digitised and encrypted biometric data into an image of the individual being authenticated to diversify access control verification.

(b) The embedding of digitised and encrypted biometric data into an image unrelated to the individual for the covert transmission of sensitive data.

Most of the research utilises fingerprint minutiae and face images (in either an image format or represented by Eigenfaces). This is mainly due to these features being the most readily available online datasets (both real and synthetic) for research purposes, such as from the Biometric System Laboratory at the University of Bologna [98], and the Pattern Recognition and Image Processing Laboratory at Michigan State University [99]. It may also be a factor that scanners for fingerprints and facial recognition tend to be cheaper than comparable hardware for other biometric inputs.

Skin-tone detection is a biometric method employed by five of the reviewed papers (see Table 3). Not only is skin tone particularly useful for embedding data using steganography, but it also has multiple applications in its own right, particularly as part of facial recognition. Cheddad et al. (2009) [58] list the following scenarios in which this technique can be applied:

- Video surveillance.

- Face and gesture recognition.
- Human-computer interaction.
- Human pose modelling.
- Image and video indexing and retrieval.
- Image editing.
- Vehicle drivers' drowsiness detection.
- Controlling users' browsing behaviour.

However, none of these applications utilise steganography. There is, however, a correlation between skin-tone detection biometrics and DWT-based steganography. This suggests that DWT is the preferred embedding method for skin-tone biometrics, as opposed to spatial-domain based steganography where residual visual artefacts are at risk as a result of embedding.

Ihmaidi et al. (2006) [64] and Katiyar et al. (2011) [69] propose application-specific usage of integrating biometrics and steganography, namely online shopping and online voting systems respectively. However, as discussed in Section 4, neither of these approaches appear to have been translated to a real-world application.

Indeed, it seems that the efforts invested in research developing the integration of biometrics with steganography have not led to a proportionate usage of the techniques in the real world. It is unclear why this should be the case. There may, of course, be a desire to keep the use of steganography secret. However, as an example, since the embedding of eHealth digital data into a cover image or the embedding of data into an eHealth cover image both have the potential to affect the integrity of the eHealth data itself adversely, then there should be accepted standards, policies or procedures in place. These do not appear to exist. The use of cryptography to encrypt data is, at least for the time being, seen as a sufficiently secure method for the transmission of sensitive information.

The research reviewed assumes that pre-sharing of a key or keys takes place between a sender and a receiver so that the receiver can extract hidden content from a stego image and decrypt the output. If the pre-shared key(s) is(are) intercepted, then subsequent transmissions will become compromised. Only Al–Assam et al. (2013) [73] propose a method using biometrics and steganography to ensure secure mutual authentication and key exchange between a sender and a receiver, but this is only true after the first communication, before which an initial one-time key K_o still needs to be shared. Despite this, the issue of pre-sharing of keys applies equally to cryptography as it does to steganography. The widespread integration of biometrics with cryptography in the real-world as opposed to the apparent lack of uptake of biometric/steganographic systems cannot be explained by issues with key-sharing alone.

5. Future Direction

In light of our review, we suggest that the current research efforts should focus on the following four key areas:

(a) Acceptable level of embedding: the capacity to embed data in a cover medium, such as a facial image, varies depending on multiple factors, such as the resolution, dimensions, and content of the host image, as well as the embedding technique employed. The tolerance for the distortions caused by embedding can therefore vary depending on the application. For example, biometrics authentication using facial images could have a higher tolerance compared to eHealth medical imagery, where the slightest foreign visual artefact could lead to a misdiagnosis.

(b) Secure steganography key exchange: one issue that still needs to be resolved is that of the initial stego key exchange, otherwise known as the prisoner's problem [100]. Various authors have tried to address this conundrum in recent years, but it remains a field of active research to this day. Nonetheless, this issue applies equally to cryptography, where a public/private key exchange is necessary to enable encryption and decryption between a sender and a receiver.

(c) Legal implications of source alteration: steganography essentially manipulates the source medium (i.e., a facial image or patient medical imagery), consequently rendering the data at the sender and receiver different. The integrity of the data is therefore altered, which raises concerns, for example, from a forensic perspective. Therefore, further research is required to determine and introduce provisions into the current legal framework to accommodate steganographic alteration of data.

(d) Industry standards: finally, existing standards need to be extended and/or new standards introduced to govern the use of steganography. Perhaps we are still far from industry adoption of steganography in real-world applications. However, the best approach is to be prepared early rather than relying on impulsive reactions as issues arise.

By expanding and intensifying research into these areas, industry will be provided with the confidence to adopt steganography in real-world applications, thereby enhancing the security and privacy of individuals and biometric systems.

6. Conclusions

Given the risk that stolen biometric information can be exploited by cyber-criminals to perform, for example, replay attacks, the security of an individual's biometric data is paramount. While the technology of biometric sensors continues to improve, such as encompassing 'liveness' checks, steganography can add a layer to the defence-in-depth model to heighten security.

Our research has identified two primary applications combining biometrics and steganography, which are access control and the transmission of sensitive eHealth/biometric data. However, neither of these applications have made the successful transition from the laboratory to the real-world setting. Proposed models for e-voting and e-shopping are included in this review, but neither of these or similar systems have been implemented as yet. In the future new applications in fields not yet envisaged may tender more readily-accepted opportunities for the integration of biometrics and steganography to be utilised.

Author Contributions: Conceptualisation, A.I., G.Z. and W.Y.; methodology, I.M.; validation, I.M., A.I., G.Z. and W.Y.; formal analysis, I.M., A.I., G.Z. and W.Y.; Investigation, I.M.; resources, C.V.; Data Curation, I.M.; writing—original draft preparation, I.M.; writing—review and editing, I.M., A.I., G.Z., W.Y., and C.V.; visualisation, I.M.; supervision, A.I., G.Z. and W.Y.; project administration, C.V.; funding acquisition, C.V., W.Y., and G.Z.

Funding: This paper was supported by the Defence Science and Technology Group (DST) of Australia through project CERA 221.

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

Abbreviations

The following abbreviations are used in this manuscript:

CEN	European Committee for Standardisation
DCT	Discrete cosine transform
DICOM	Digital Imaging and Communications in Medicine
DWT	Discrete wavelet transform
EISC	Electronic internet shopping card
FRS	Face recognition system
HIPAA	Health Information Portability and Accountability Act
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organisation for Standardisation
LSB	Least significant bit
OOE	Object-oriented embedding
OTP	One-time pin
PCA	Principal component analysis
RGB	Red–green–blue

ROI	Regions of interest
SVM	Support vector machine
UN/CEFACT	United Nations Centre for Trade Facilitation and Electronic Business
UN/EDIFACT	United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport

References

1. Meng, W.; Wong, D.S.; Furnell, S.; Zhou, J. Surveying the development of biometric user authentication on mobile phones. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1268–1293. [CrossRef]
2. Campisi, P. *Security and Privacy in Biometrics*; Springer: Berlin/Heidelberg, Germany, 2013; Volume 24.
3. Marqués, I.; Graña, M. Image security and biometrics: A review. In *International Conference on Hybrid Artificial Intelligence Systems*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 436–447.
4. Sirull, E. What Is the Dark Web? 2018. Available online: https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/ (accessed on 11 May 2018).
5. Stack, B. Here'S How Much Your Personal Information Is Selling for on The Dark Web. 2018. Available online: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (accessed on 11 May 2018).
6. Hillman, S. Physical security 101: Evolving 'defense in depth'. *InTech Magazine*, May/June 2011.
7. Zheng, G.; Yang, W.; Valli, C.; Qiao, L.; Shankaran, R.; Orgun, M.A.; Mukhopadhyay, S.C. Finger-to-Heart(F2H): Authentication for Wireless Implantable Medical Devices. *IEEE J. Biomed. Health Inform.* **2018**. [CrossRef]
8. Okoh, E.; Awad, A.I. Biometrics Applications in e-Health Security: A Preliminary Survey. In *Health Information Science*; Yin, X., Ho, K., Zeng, D., Aickelin, U., Zhou, R., Wang, H., Eds.; Springer: Cham, Switzerland, 2015; pp. 92–103.
9. Awad, A.I.; Hassanien, A.E.; Zawbaa, H.M. A Cattle Identification Approach Using Live Captured Muzzle Print Images. In *Advances in Security of Information and Communication Networks*; Awad, A.I., Hassanien, A.E., Baba, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 143–152.
10. Awad, A.I. From classical methods to animal biometrics: A review on cattle identification and tracking. *Comput. Electron. Agric.* **2016**, *123*, 423–435. [CrossRef]
11. Jain, A.K.; Feng, J.; Nandakumar, K. Fingerprint matching. *Computer* **2010**, *43*, 36–44. [CrossRef]
12. Awad, A.I.; Baba, K. Fingerprint Singularity Detection: A Comparative Study. In *Software Engineering and Computer Systems*; Mohamad Zain, J., Wan Mohd, W.M.b., El-Qawasmeh, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 122–132.
13. Awad, A.I.; Baba, K. An Application for Singular Point Location in Fingerprint Classification. In *Digital Information Processing and Communications*; Snasel, V., Platos, J., El-Qawasmeh, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 262–276.
14. Feng, J.; Jain, A.K. Fingerprint Reconstruction: From Minutiae to Phase. *IEEE Trans. Pattern Anal. Mach. Intell.* **2011**, *33*, 209–223. [CrossRef]
15. Peralta, D.; Galar, M.; Triguero, I.; Paternain, D.; García, S.; Barrenechea, E.; Benítez, J.M.; Bustince, H.; Herrera, F. A survey on fingerprint minutiae-based local matching for verification and identification: Taxonomy and experimental evaluation. *Inf. Sci.* **2015**, *315*, 67–87. [CrossRef]
16. Yang, W.; Wang, S.; Hu, J.; Zheng, G.; Valli, C. Security and Accuracy of Fingerprint-Based Biometrics: A Review. *Symmetry* **2019**, *11*, 141. [CrossRef]
17. Masdari, M.; Ahmadzadeh, S. A Survey and Taxonomy of the Authentication schemes in Telecare Medicine Information Systems. *J. Netw. Comput. Appl.* **2017**, *87*, 1–19. [CrossRef]
18. Yang, W.; Wang, S.; Zheng, G.; Chaudhry, J.; Valli, C. ECB4CI: An enhanced cancelable biometric system for securing critical infrastructures. *J. Supercomput.* **2018**, *74*, 4893–4909. [CrossRef]
19. Akhtar, Z.; Rattani, A. A Face in any Form: New Challenges and Opportunities for Face Recognition Technology. *Computer* **2017**, *50*, 80–90. [CrossRef]
20. Galbally, J.; Ortiz-Lopez, J.; Fierrez, J.; Ortega-Garcia, J. Iris liveness detection based on quality related features. In Proceedings of the 2012 5th IAPR International Conference on Biometrics (ICB), New Delhi, India, 29 March–1 April 2012; pp. 271–276.

21. Mehrotra, H.; Sa, P.K.; Majhi, B. Fast segmentation and adaptive SURF descriptor for iris recognition. *Math. Comput. Model.* **2013**, *58*, 132–146. [CrossRef]
22. Doroz, R.; Wrobel, K.; Porwik, P. An accurate fingerprint reference point determination method based on curvature estimation of separated ridges. *Int. J. Appl. Math. Comput. Sci.* **2018**, *28*, 209–225. [CrossRef]
23. Kshirsagar, V.; Baviskar, M.; Gaikwad, M. Face recognition using Eigenfaces. In Proceedings of the 2011 3rd International Conference on Computer Research and Development (ICCRD), Shanghai, China, 11–15 March 2011; Volume 2, pp. 302–306.
24. Yang, W.; Wang, S.; Hu, J.; Zheng, G.; Valli, C. A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognit.* **2018**, *78*, 242–251. [CrossRef]
25. Kumar, A.; Wu, C. Automated human identification using ear imaging. *Pattern Recognit.* **2012**, *45*, 956–968. [CrossRef]
26. Harb, A.; Abbas, M.; Cherry, A.; Jaber, H.; Ayache, M. Palm print recognition. In Proceedings of the 2015 International Conference on Advances in Biomedical Engineering (ICABME), Beirut, Lebanon, 16–18 September 2015; pp. 13–16.
27. Zhang, D.; Kanhangad, V. Hand geometry recognition. In *Encyclopedia of Cryptography and Security*; Springer: Berlin/Heidelberg, Germany, 2011; pp. 529–531.
28. Kang, B.J.; Park, K.R.; Yoo, J.H.; Kim, J.N. Multimodal biometric method that combines veins, prints, and shape of a finger. *Opt. Eng.* **2011**, *50*, 017201.
29. Wrobel, K.; Doroz, R.; Porwik, P.; Naruniec, J.; Kowalski, M. Using a Probabilistic Neural Network for lip-based biometric verification. *Eng. Appl. Artif. Intell.* **2017**, *64*, 112–127. [CrossRef]
30. Wrobel, K.; Doroz, R.; Porwik, P.; Bernas, M. Personal identification utilizing lip print furrow based patterns. A new approach. *Pattern Recognit.* **2018**, *81*, 585–600. [CrossRef]
31. Hashiyada, M. DNA biometrics. In *Biometrics*; InTech: London, UK, 2011.
32. Rashed, A.; Santos, H. Odour user interface for authentication: Possibility and acceptance: Case study. In Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong, China, 17–19 March 2010; Volume 1.
33. Bhatnagar, M.; Jain, R.K.; Khairnar, N.S. A survey on behavioral biometric techniques: Mouse vs. Keyboard dynamics. In Proceedings of the International Conference on Recent Trends in Engineering and Technology, Tamilnadu, India, 15–16 March 2013; pp. 27–30.
34. Preis, J.; Kessel, M.; Werner, M.; Linnhoff-Popien, C. Gait recognition with kinect. In Proceedings of the 1st International Workshop on Kinect in Pervasive Computing, New Castle, UK, 18–22 June 2012; pp. 1–4.
35. Rudrapal, D.; Das, S.; Debbarma, S.; Kar, N.; Debbarma, N. Voice recognition and authentication as a proficient biometric tool and its application in online exam for PH people. *Int. J. Comput. Appl.* **2012**, *39*, 6–12.
36. Kumar, P.; Singh, S.; Garg, A.; Prabhat, N. Hand written signature recognition and verification using neural network. *Int. J. Adv. Res. Comput. Sci. Softw. Eng.* **2013**, *3*, 558–565.
37. Doroz, R.; Kudlacik, P.; Porwik, P. Online signature verification modeled by stability oriented reference signatures. *Inf. Sci.* **2018**, *460–461*, 151–171. [CrossRef]
38. Pleva, M.; Bours, P.; Ondáš, S.; Juhár, J. Improving static audio keystroke analysis by score fusion of acoustic and timing data. *Multimedia Tools Appl.* **2017**, *76*, 25749–25766. [CrossRef]
39. Amin, R.; Gaber, T.; ElTaweel, G.; Hassanien, A.E. Biometric and traditional mobile authentication techniques: Overviews and open issues. In *Bio-Inspiring Cyber Security and Cloud Services: Trends and Innovations*; Springer: Berlin/Heidelberg, Germany, 2014; pp. 423–446.
40. Saini, R.; Rana, N. Comparison of various biometric methods. *Int. J. Adv. Sci. Technol.* **2014**, *2*, 2.
41. Alsaadi, I.M. Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review. *Int. J. Sci. Technol. Res.* **2015**, *4*, 285–289.
42. Tiwari, S.; Chourasia, J.; Chourasia, V.S. A review of advancements in biometric systems. *Int. J. Innov. Res. Adv. Eng.* **2015**, *2*, 187–204.
43. Buciu, I.; Gacsadi, A. Biometrics systems and technologies: A survey. *Int. J. Comput. Commun. Control* **2016**, *11*, 315–330. [CrossRef]
44. Akhtar, Z. *Security of Multimodal Biometric Systems Against Spoof Attacks*; Department of Electrical and Electronic Engineering, University of Cagliari: Cagliari, Italy, 2012; Volume 6.
45. Joseph, A.; Sundaram, V. Cryptography and steganography—A survey. *Int. J. Comput. Technol. Appl.* **2011**, *2*, 626–630.

46. Jain, A.K.; Uludag, U. Hiding biometric data. *IEEE Trans. Pattern Anal. Mach. Intell.* **2003**, *25*, 1494–1498. [CrossRef]
47. Challita, K.; Farhat, H. Combining steganography and cryptography: New directions. *Int. J. New Comput. Archit. Their Appl. (IJNCAA)* **2011**, *1*, 199–208.
48. Mahale, P.S. A survey on various patterns regarding encryption, a efficient based method regarding cryptography and steganography. *Int. J. Latest Trends Eng. Technol.* **2013**, *2*, 341–344.
49. Pitropakis, N.; Yfantopoulos, N.; Geneiatakis, D.; Lambrinoudakis, C. Towards an augmented authenticator in the Cloud. In Proceedings of the 2014 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT), Noida, India, 15–17 December 2014; pp. 296–300.
50. Akhtar, N.; Johri, P.; Khan, S. Enhancing the security and quality of LSB based image steganography. In Proceedings of the 2013 5th International Conference on Computational Intelligence and Communication Networks (CICN), Mathura, India, 27–29 September 2013; pp. 385–390.
51. Kapczyński, A.; Banasik, A. Biometric logical access control enhanced by use of steganography over secured transmission channel. In Proceedings of the 2011 IEEE 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Prague, Czech Republic, 15–17 September 2011; Volume 2, pp. 696–699.
52. Kaur, B.; Kaur, A.; Singh, J. Steganographic approach for hiding image in DCT domain. *Int. J. Adv. Eng. Technol.* **2011**, *1*, 72.
53. Shaik, A.; Thanikaiselvan, V.; Amitharajan, R. Data security through data hiding in images: A review. *J. Artif. Intell.* **2017**, *10*, 1–21.
54. Shejul, A.A.; Kulkarni, U.L. A DWT based approach for steganography using biometrics. In Proceedings of the 2010 International Conference on Data Storage and Data Engineering (DSDE), Bangalore, India, 9–10 February 2010; pp. 39–43.
55. Kumar, V.; Kumar, D. Performance evaluation of DWT based image steganography. In Proceedings of the 2010 IEEE 2nd International Advance Computing Conference (IACC), Patiala, India, 19–20 February 2010; pp. 223–228.
56. Cheddad, A.; Condell, J.; Curran, K.; Mc Kevitt, P. Biometric inspired digital image steganography. In Proceedings of the ECBS 2008, 15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems, Belfast, UK, 31 March–4 April 2008; pp. 159–168.
57. Chaves-González, J.M.; Vega-Rodríguez, M.A.; Gómez-Pulido, J.A.; Sánchez-Pérez, J.M. Detecting skin in face recognition systems: A colour spaces study. *Digit. Signal Process.* **2010**, *20*, 806–823. [CrossRef]
58. Cheddad, A.; Condell, J.; Curran, K.; Mc Kevitt, P. A skin tone detection algorithm for an adaptive approach to steganography. *Signal Process.* **2009**, *89*, 2465–2478. [CrossRef]
59. Zhao, Y.; Dai, S.; Xi, X. A Mumford-Shah level-set approach for skin segmentation using a new color space system. In Proceedings of the International Conference on Simulation and Scientific Computing, Beijing, China, 10–12 October 2008; pp. 307–310.
60. Prajapati, H.A.; Chitaliya, N.G. Secured and Robust Dual Image Steganography: A Survey. *Int. J. Innov. Res. Comput. Commun. Eng.* **2015**, *3*, 30–37. [CrossRef]
61. Goli, M.S.; Naghsh, A. A comparative study of image-in-image steganography using three methods of least significant bit, discrete wavelet transform and singular value decomposition. *Bull. De La Société R. Des Sci. De Liège* **2016**, *85*, 1465–1474.
62. Thanikaiselvan, V.; Shastri, S.; Ahmad, S. Information hiding: Steganography. In *Intelligent Techniques in Signal Processing for Multimedia Security*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 65–91.
63. Ambalakat, P. Security of Biometric Authentication Systems. 2005. Available online: https://pdfs.semanticscholar.org/e1d7/7b951c55d7d1f322d1f96942daa77ec6c4ee.pdf (accessed on 27 March 2019)
64. Ihmaidi, H.D.; Al-Jaber, A.; Hudaib, A. Securing online shopping using biometric personal authentication and steganography. In Proceedings of the 2006 2nd International Conference on Information and Communication Technologies, Damascus, Syria, 24–28 April 2006; Volume 1, pp. 233–238.
65. Kant, C.; Nath, R.; Chaudhary, S. Biometrics security using steganography. *Int. J. Secur.* **2008**, *2*, 1–5.
66. Agrawal, N.; Savvides, M. Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, Miami, FL, USA, 20–25 June 2009; pp. 85–92.

67. Na, W.; Chiya, Z.; Xia, L.; Yunjin, W. Enhancing iris-feature security with steganography. In Proceedings of the 2010 the 5th IEEE Conference on Industrial Electronics and Applications (ICIEA), Taichung, Taiwan, 15–17 June 2010; pp. 2233–2237.
68. Barve, S.; Nagaraj, U.; Gulabani, R. Efficient and secure biometric image stegnography using discrete wavelet transform. *Int. J. Comput. Sci. Commun. Netw.* **2011**, *1*, 96–99.
69. Katiyar, S.; Meka, K.R.; Barbhuiya, F.A.; Nandi, S. Online voting system powered by biometric security using steganography. In Proceedings of the 2011 Second International Conference on Emerging Applications of Information Technology (EAIT), Kolkata, India, 19–20 February 2011; pp. 288–291.
70. Shejul, A.A.; Kulkarni, U.L. A secure skin tone based steganography using wavelet transform. *Int. J. Comput. Theory Eng.* **2011**, *3*, 16. [CrossRef]
71. Sonsare, P.M.; Sapkal, S. Stegano-crypto system for enhancing biometric-feature security with RSA. In *Proceedings of the International Conference on Information and Network Technology*; IACSIT Press: Singapore, 2011; pp. 196–200.
72. Shanthini, B.; Swamynathan, S. Multimodal biometric-based secured authentication system using steganography. *J. Comput. Sci.* **2012**, *8*, 1012.
73. Al-Assam, H.; Rashid, R.; Jassim, S. Combining steganography and biometric cryptosystems for secure mutual authentication and key exchange. In Proceedings of the 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), London, UK, 9–12 December 2013; pp. 369–374.
74. Whitelam, C.; Osia, N.; Bourlai, T. Securing multimodal biometric data through watermarking and steganography. In Proceedings of the 2013 IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, USA, 12–14 November 2013; pp. 61–66.
75. French, M. Maine Startup Puts Biometric Touch on Data. 2002. Available online: https://www.bizjournals.com/boston/blog/mass-high-tech/2002/08/maine-startup-puts-biometric-touch-on-data.html (accessed on 15 May 2018).
76. 104th United States Congress. Health Insurance Protability and Accountability Act of 1996. 1996. Available online: https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm (accessed on 21 May 2018).
77. 106th United States Congress. Gramm–Leach–Bliley Act 1999. 1999. Available online: http://www.gpo.gov/fdsys/pkg/STATUTE-113/pdf/STATUTE-113-Pg1338.pdf (accessed on 21 May 2018).
78. Parliament of Australia. Health Legislation Amendment (eHealth) Act 2015. 2015. Available online: https://www.legislation.gov.au/Details/C2015A00157 (accessed on 21 May 2018).
79. National Electrical Manufacturers Association. Digital Imaging and Communications in Medicine. 2018. Available online: https://www.dicomstandard.org/current/ (accessed on 21 May 2018).
80. Health Level Seven International. Introduction to HL7 Standards. 2018. Available online: http://www.hl7.org/implement/standards/index.cfm?ref=nav (accessed on 21 May 2018).
81. United Nations Economic Commission for Europe. UN/CEFACT. 2018. Available online: https://www.unece.org/cefact.html (accessed on 21 May 2018).
82. United Nations Economic Commission for Europe. Introducing UN/EDIFACT. 2018. Available online: https://www.unece.org/cefact/edifact/welcome.html (accessed on 21 May 2018).
83. OASIS. OASIS Standards. 2018. Available online: https://www.oasis-open.org/standards (accessed on 21 May 2018).
84. eStandards. eHealth Standards and Profiles in Action for Europe and Beyond. 2018. Available online: http://www.estandards-project.eu/ (accessed on 21 May 2018).
85. European Committee for Standardization (CEN). CEN/TC 251—Health Informatics. 2018. Available online: https://standards.cen.eu/dyn/www/f?p=204:7:0::::FSP_ORG_ID:6232&cs=18CA078392807EDD402B798AAEF1644E1 (accessed on 21 May 2018).
86. ISO/IEEE. IEEE 11073 Personal Health Devices. 2018. Available online: http://11073.org/ (accessed on 21 May 2018).
87. International Organization for Standardization. Standards Catalogue 35.030—IT Security. 2018. Available online: https://www.iso.org/ics/35.030/x/ (accessed on 25 May 2018).
88. NEC Australia. NeoFace Facial Recognition—Overview. 2018. Available online: https://au.nec.com/en_AU/solutions/security-and-public-safety/biometrics/neoface-facial-recognition-overview.html (accessed on 25 May 2018).

89. UniLink. 2018. Available online: http://www.unilink.com/ (accessed on 25 May 2018).
90. Damstra Technology. Damstra. 2018. Available online: https://www.damstratechnology.com/ (accessed on 25 May 2018).
91. M2SYS Technology. M2SYS. 2018. Available online: http://www.m2sys.com/ (accessed on 25 May 2018).
92. International Security Control Solutions. ISCS. 2018. Available online: http://www.iscs.com.au/ (accessed on 25 May 2018).
93. Find Biometrics. 2018. Available online: https://findbiometrics.com/ (accessed on 25 May 2018).
94. HID Global. 2018. Available online: https://www.hidglobal.com/ (accessed on 25 May 2018).
95. Gemalto. 2018. Available online: https://www.gemalto.com/ (accessed on 25 May 2018).
96. Kisi. 2018. Available online: https://www.getkisi.com/ (accessed on 25 May 2018).
97. Abloy. 2018. Available online: https://www.abloy.com/en/abloy/abloycom/ (accessed on 25 May 2018).
98. University of Bologna. Biometric System Laboratory. Available online: http://biolab.csr.unibo.it/home.asp (accessed on 29 May 2018).
99. Michigan State University. Pattern Recognition and Image Processing Laboratory. Available online: http://www.cse.msu.edu/prip/General/ (accessed on 29 May 2018).
100. Simmons, G.J. The prisoners' problem and the subliminal channel. in *Advances in Cryptology*; Springer: Berlin/Heidelberg, Germany, 1984; pp. 51–67.