

Secure Biometric Signal Processing; A Review

¹Chukumeka Gift Iroanwusi, ²Davies Isobo Nelson, ³Aniefiok Tom Bassey

^{1&3}Department of Computer Science, Ignatius Ajuru University of Education,
Port Harcourt, Nigeria

²Department of Computer Science, Rivers State University, Port Harcourt, Nigeria

*Corresponding Author: Davies Isobo Nelson

*Corresponding Email: isobo.davies@ust.edu.ng

DOI: 10.56201/ijcsmt.vol.11.no9.2025.pg93.107

Abstract

In recent year, biometric technologies have become an integral part of modern authentication systems, offering distinct advantages such as convenience, uniqueness, and resistance to credential theft. However, as these systems are increasingly deployed in critical applications ranging from border control and e-governance to mobile security and financial transactions the security and privacy of biometric signal processing have emerged as paramount concerns. This study discussed the critical challenges faced by biometric systems, focusing on recognition accuracy, scalability, and ethical implications related to surveillance and consent. The study examines advanced security techniques, including cancelable biometrics, steganography and watermarking, homomorphic encryption, highlighting their potential to enhance the security of biometric data. Additionally, the integration of multimodal biometrics is discussed as a strategy to improve resilience against emerging threats like sensor attacks and template inversion. The study emphasizes the necessity of adopting privacy-by-design principles to mitigate unauthorized access and data breaches, ensuring user control over biometric information. Further, the findings underscore the importance of developing robust defense mechanisms that adapt to evolving security threats while preserving user privacy. By synthesizing recent advancements in secure biometric signal processing, this paper provides a comprehensive framework for enhancing security, usability, and efficiency in future biometric applications.

Key Words: *Steganography, Watermarking, Cancelable Biometrics, Homomorphic Encryption, Imperceptibility. Multibiometric*

1. Introduction

Biometric authentication systems rely on physiological and behavioral traits such as fingerprints, iris, face, voice, and gait to verify identity. At the core of these systems lies signal processing, which involves acquisition, feature extraction, enhancement, matching, and decision-making. However, since biometric signals are inherently noisy, variable, and permanent, they require specialized processing techniques that preserve both recognition accuracy and security. The fact that biometric data is public and irrevocable couple with the existence of several types of attack that are possible in a biometric system, makes the issues of security/integrity of biometric data extremely important. Traditional signal processing in biometrics focused primarily on improving recognition rates by enhancing feature robustness and minimizing intra-class variability. Yet, as biometric deployments expanded into critical applications such as border control, mobile banking, and e-health, security and privacy emerged as major concerns. Unlike passwords or tokens, biometric signals cannot be revoked if compromised. Adversaries can exploit vulnerabilities through spoofing, replay, template

inversion, or adversarial perturbations. Systems employing biometric traits for people authentication and identification are witnessing growing popularity due to their unique and indissoluble line between any individual and his/her biometric characteristics (Barni et al., 2015). The biometric characteristic of a person are unique and has the ability to recognize the person, and it can be biological or behavioral. They are used for authentication or recognition of individuals for many critical applications like border control, access control, immigration, forensic and different law enforcement (Choudhury., 2018). When employed to replace password, biometrics have the added advantage that they do not need to be memorized and are relatively hard to steal. Nonetheless, unlike conventional security mechanism such as password, biometric data are inherent parts of a person's body and cannot be replaced if they are compromised (Barni et al., 2015). The author further emphasized two problems associated with biometrics, first, that compromised biometric data can be used to have access to sensitive information and impersonate the victim for malicious purposes. And due to their uniqueness, the privacy of their owner is put at risk. Geographical position, movements, habits and even personal beliefs can be tracked by observing when and where the biometric traits of an individual are used to identify him/her.

Meitei et al. (2018), averaged that biometric can be understood as a process or the ability of a system to identify a particular person based on some unique biological features or patterns such as fingerprints, facial recognition, DNAs, voice, eye-iris and retina, palm prints, signature, etc. Compared to password or taken based authentication system, biometric system using fingerprint, iris, face, voice, etc. provides better security as people cannot lose or forget their biometric traits. However, the advanced technology of today's world makes it possible to create a loophole in prints on whatever they touch: hence one can easily steal the fingerprint and can even make artificial finger using the stolen fingerprint. The person's face can be captured by the camera even from a distance without their concern. In such situation, the security of the biometric based authentication system is at a stake (Chondhury et al., 2018).

Biometric Technology

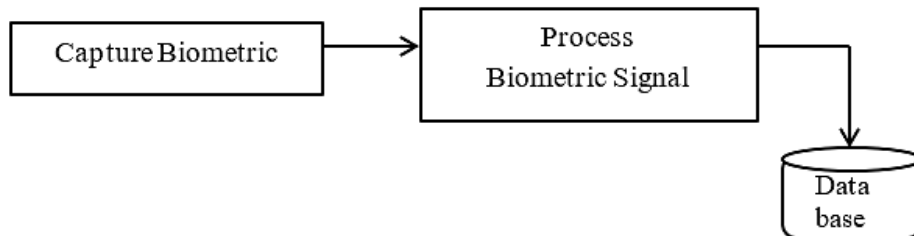
Biometric technologies are pattern recognition system that uses either image acquisition devices, such as scanners, or cameras in the case of fingerprint or iris recognition technologies, or sound or movement acquisition devices, such as microphones or plate in the case of voice recognition or signature technologies, to collect the biometric pattern or characteristics. Biometric technology refers to systems that automatically capture, analyze, and verify an individual's identity based on their unique physical or behavioral traits (Fourthline, 2025). They are designed to analyze anyone of your unique personal traits such as your voice, irises, and facial or fingerprint to prove and determine it is really you. The biometric system can be categorized into verification system and identification system. In the case of verification, the system asks the person to supply his/her biometric traits and then conduct a one-to-one comparison between queries identify and the template stored in the database. If the query feature matched the template, the person will be considered otherwise, the system will consider the person as an imposter and reject the request. The biometric feature conducts one-to-many comparisons in the case of identification, where the query will be compared with the template of all enrolled users in the database. Identification system establishes whether the person is who he/she claims to be.

NBSP (2008) averred that the characteristics of the acquired samples considered the most distinctive between users and the most stable for each user are extracted and encoded into a biometric reference or template that is a mathematical representation of a person's biometric feature. These templates are stored in a database or on a smart card or other token and used for

comparison when recognition is warranted. Biometric systems are automated by hardware and software, allowing for fast, real-time decision making in identification situations.

First is to capture the chosen biometric, 2. Process the biometric signal and extract and enroll the biometric template, 3. Store the template in a database, 4. Live scan or capture the chosen biometric, 5. Process the biometric and extract the biometric template 6. Match and compare the scanned biometric or template against stored template and provide the result of the matching score.

Enrollment: Add a biometric signal to the Database



Verification: Match against enrolled template

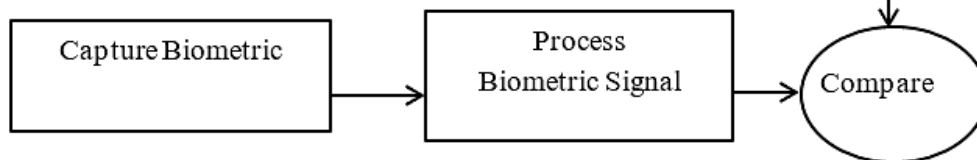


Fig. 1 Biometric system block diagram

Kaur, et al (2014) explained two phases of conventional biometric system: enrolment phase and authentication phase. In the enrolment stage, the original biometric traits is captured and saved in the database, and during the authentication stage, the system matches the stored template every time the user access the system by providing the live biometric.

While each biometric has its own strengths and weakness, for a biometric to be effective it should have the following four properties.

- i. **Universality:** All members of the population being identified should possess biometrics.
- ii. **Uniqueness:** Biometric signature should be different from all members of the population.
- iii. **Invariance:** The signature should be invariance under the conditions that it will be collected.
- iv. **Resistance:** The biometric should be resistant to potential counter measures in order to work accurately, the image biometrics system need to have the sample image of the users biometric that is stored on the database in a very clear and non-adulterated form or manner.

This section focuses on some existing and emerging biometric technology.

- i. **Face Recognition Technology:** In facial recognition biometrics, the spatial geometry like shape, size, and the structure of the face is considered as feature to recognize a person. Face recognition works by looking at features at specific nodal points on the user's face and comparing it with a database of previously recorded patterns. The nodal points are specific characteristics of the face such as the distance between eyes or the

width of the nose. The advantage of face biometric is that it is contactless and the acquisition process is simple. However, most of the times it gives inaccurate result as facial features tend to change over time due to age, expression, recording devices and other external factors (Choudhury, 2018).

- ii. **Voice Recognition:** Voice recognition uses technology to evaluate the biometrics of your voice. That includes the frequency and flow of voice, as well as your accent. Every word you speak is broken up into segment of several tones. This is then digitized and translated to create your own unique voice template. Speech recognitions and voice recognitions are not the same thing. Speech recognition recognizes only the words and focuses on translation of verbal form to a text one. Voice recognition ensures for the voice to be recognized and to identify an individual user's voice. Voice recognition is able to authenticate the speaker by analyzing the pattern and sequences of a person's voice hence capable to identify the specific person (Dakic, 2023). Voice recognition system creates personalized content, serves time, increases productivity and accessibility.

There are two distinguished types of voice recognition.

Text Dependent: depends on the specific set of words the persons says-you need step-up authentication and identity verification and in order to be activated, the user has to say the necessary phrase.

Text Independent: does not depend on a specific text yet relies on conversation speech. The authentication does not require the user to say a set of required phrases (Dakic, 2023).

- iii. **Fingerprints Based Recognition:** Fingerprint biometrics refers to the use of the unique ridge patterns and minutiae points present on an individual's fingertip for personal identification and authentication. Since no two individuals share the exact same fingerprint pattern, even identical twins, fingerprints have been widely adopted as a reliable biometric trait. Fingerprint biometric systems typically involve four main stages: image acquisition, feature extraction, template storage, and matching. The extracted features, such as ridge endings, bifurcations, and ridge flow are stored as encrypted templates rather than raw images to enhance security. Because of their uniqueness, permanence, and ease of acquisition, fingerprints are the most widely deployed biometric modality in applications ranging from mobile device authentication and border security to forensic investigations (Maltoni et al., 2019; Jain et al., 2021). Every human being possesses fingers and apparently fingerprints. Fingerprints are unique, stable and permanent to each person with his own pattern in his/her fingerprints and can be used in both verification (1;1) and identification (1;N) application. Fingerprints are either flat (capture by placing a finger directly on the scanner) or rolled (rolling the finger from one edge of the fingernail to the other). A flat fingerprint is an impression of area between the fingertip and the first knuckle, which a rolled fingerprints also includes an impression of the ridges on both sides of the finger. Fingerprint recognition is one of the most widely used biometric technologies and suitable for a large number of recognition application like payment system, crime lab and physical access system. Fingerprint base system can also be categorized into broad groups; minutiae-based matching (analyzing the local structure), direct correlation technique optical comparison and spectral ridge-pattern matching (analyzing the ridge or global structure) of the fingerprint. Fingerprint patterns are easily analyzed and compared, easy to use and cost effective."

"Fingerprints are unique to each individual, and each individual has his own pattern in his fingerprints. This type of identification has been successfully used by the police to

capture criminals and to find missing children. A fingerprint records the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. The traditional method, which is used by police, matches minutiae (Small details found in finger images such as ridge endings or bifurcations or simply details of the fingerprint). Some other approaches are pattern matching and more patterns of 3 borders. There are some verification approaches that can detect if a live finger is presented, but not all of these approaches can provide this type of information. If fingerprint-scanning techniques were to be incorporated into the flight deck to provide continuous authentication, liveness detection or testing would be a requirement for the system.”

- iv. **Iris Technology:** Iris Recognition is one of the important biometric recognition systems that identify people based on their eyes and iris. Iris recognition technology is based on the pattern resident in the iris of the eye- the colored ring surrounding the pupil. Iris recognition technology identifies people by the unique patterns in the iris using a fairly conventional charge coupled device (CCD) camera. Made from elastic connective tissue, the iris represents a richly patterned surface under the reflective cornea of the eye. The image of the iris under infra-red illumination can be quantified and used to identify an individual. Iris recognition systems use a CCD camera to capture a black-and-white, high-resolution image of iris under infra-red illumination. According to Luo et al., (2025) iris recognition is recognized as the most accurate and secure biometric identification technology playing a pivotal role in security applications such as intelligent unlocking, border control, security prevention, and criminal screening. Iris texture features provides unique high dimensional information that explains why iris recognition based verification has the lowest false acceptance rate among all types of biometric verification systems and iris base recognition system is less invasive and have the lowest false match rates. It works well in identification (one-to-many comparison) mode, and extremely accurate but won't work on some group such as the blind or people with cataracts. Applications of iris technology system include border security, ATMs, facility access control, airline passenger screening and etc.

Review of Related Work

This section discusses and reviewed related works done by other scholars.

Bayer and Rathgeb (2025), present a simple but flexible approach to increase the privacy protection of homomorphically encrypted multi-biometric reference templates while enabling adaptation to security requirements at run-time: An adaptive multi-biometric fusion with fully homomorphic encryption (AMB-FHE). AMB-FHE is benchmarked against a bimodal biometric database consisting of the CASIA iris and MCYT fingerprint datasets using deep neural networks for feature extraction. The author's contribution is easy to implement and increases the flexibility of biometric authentication while offering increased privacy protection through joint encryption of templates from multiple modalities.

Luo et al., (2025) introduce a novel deep learning framework for iris recognition that employs an attention mechanism, leveraging ResNet-50 as the foundational architecture and integrating a lightweight attention module (LAM). Within the LAM, they proposed a non-global interactive channel attention module (NGICAM) and a lightweight spatial attention module (LSAM), further optimizing the triplet loss to more effectively extract iris texture features. Their experimental results indicate that this approach yields a lower equal error rate (EER) and a higher decidability index (DI) compared to existing models, achieving the most significant EER reduction of 23.26% and an increase of up to 2.3405 in DI.

Abd El-Samie et al., (2025) use two proposed realizations of a cascaded structure to generate cancelable biometrics. The first one is based on the adaptive filter and the comb filter in consequence, while the second one is based on the comb filter and then the adaptive filter. The cascaded structure is used to generate the cancelable patterns for faces and fingerprints, and then we compare the realizations with each other. The combined filters perform the deformation process. We observe that for different comb filter orders (L), there is low correlation between the original and generated biometrics. The different filter orders tested in this study include 6, 8, 10, and 12. The proposed system is assessed using Equal Error Rate (EER), False Accept Rate (FAR), False Reject Rate (FRR), and Area under Receiver Operating Characteristic (ROC) curve. The first proposal (adaptive and then comb filter) is preferred for faces and fingerprints. There is no intersection between genuine and imposter distribution curves, and $AROC = 1$. If the filter order increases, the results get better. At order $L = 12$ in case face images, $EER = 1.2019 \times 10^{-7}$, $FAR = 2.9074 \times 10^{-9}$ and $FRR = 3.7155 \times 10^{-7}$. Buhan et al., (2010), presented the framework where results from both cryptography and signal processing can be integrated, with the goal to organize and conceptualize the existing knowledge in the area of security of biometrics and build a bridge between the formal model of cryptography and the practical view of the signal processing area.

Rane et al., (2013), presented the main concept that underlie secured biometric system and have described the principal architectures by casting them as realization of a single, general authentication framework. The researcher's objective first is to acquaint readers with the difference between secure and traditional biometric authentication; next to familiarize them with the goals, idea and performance metric common to all realizations of secure biometric and finally to introduce them to the ways in which the various realization differs.

Barni et al., (2015) presented privacy protection in biometric-based recognition system and the paper concludes that processing signals in the encrypted domain provides an elegant and provably secure mechanism to protect both the biometric data and the privacy of the individuals subject to biometric controls. It was the goal of the article to introduce the readers to the main concepts behind SPED biometric matching and to show how a clever design of the underling matching protocol many help to fill the gap between the complexity of Signal processing in the encrypted domain (SPED) protocol and the efficiency required for the development of such protocol in real system.

Jain and Kant (2015), discussed about the biometric system along with its modules and make progress towards various attacks on biometric system and found that most of the attacks makes target to the biometric templates which are stored in system database. The authors also highlight various techniques to resist attack that can be used to protect biometric templates and also discussed about generic security threats to any system. The paper also gives idea about steganography, watermarking, cancellable biometrics and biometric cryptosystems techniques to enhance the integrity of the biometric templates and found that there is no security technique which can satisfy all the aspect of an idea biometric template protection scheme. The authors concluded that there is still need to do research work in this field so that an efficient and foolproof security technique is established.

Gawande, et al., (2017) proposed two approaches of feature extraction i.e, block sum for iris and modified minute method for fingerprint, with the main aim to provide an informative analysis and solution of key issues and challenges of biometric-based security system. They also discussed different issues and challenges in designing biometric-based security system and methodologies involved in overcoming these issues. From the result, the block sum feature sets proved to be the better feature set for recognition. For fingerprint, a noval fingerprint feature set extraction algorithm, combining core and minimal points was presented and simulation

results indicated that the technique performs much better than a standard minutiae-based method and reduced feature set using DWT.

Choudhury et al., (2018) presented a review on the state-of-art and analysis of different existing method of biometric based authentication system and cancelable biometric system along with an elaborate focus on cancelable biometrics in order to show its advantages over the standard biometric through some generalized standards and guidelines acquired from the literature. In this paper, the researcher reviewed most of the traditional biometrics systems, their performances, along with their security and privacy issues which lead to the potentials cancelable biometric based system.

Taha et al., (2020) gives an overview of techniques employed in the protection of biometric information that is contained in fingerprints. The researcher also presented the benefits and drawbacks, and the use of biometric methods. The articles showcased review that covered a majority of the conventional biometric system, the respective performance, in addition to the security and privacy concern, that will be a guide to the probable biometrics hiding system. The researcher also summarized several of the most up-to-date writings on biometrics related to hiding, and did a comparison of their performances, in addition to highlighting the core advantages and disadvantage of hiding biometrics.

Prathusha et al., (2022), proposed an efficient and privacy-preserving biometric identification outsourcing scheme. The biometric data is encrypted and outsourced to the cloned server. To execute a biometric identification, the database owner encrypts the query data and submits it to the cloud. The cloud performs identification operations over encrypted database and returns the result to the database owner. A thorough security analysis indicates the proposed scheme is secured even if attackers can forge identification request and collude with the cloud. The authors concludes that he detailed analysis shows it can resist the potential attack, and through performance evaluations, the authors further demonstrated the proposed scheme meets the efficiency need well.

Challenges of Biometric System

Although biometric system are emerging and trending technology and provides a major secured system, this is not without challenges. Accuracy, scalability, security and privacy are the four main challenges of biometric system that increase the complexity and difficulties of system design.

An idea biometric system should make correct judgment on every test sample, but due to factor such as inter-class variance which is due to many external factors such as placement of finger on the sensor, applied finger pressure, skin condition and feature extraction error that lead to large intra-user variation. Intra-class similarity implies that different individuals may have extremely similar biometric features. For instance, twins usually exhibit quite identical facial appearance since they have the same genes, different representation, noise and poor sampling quality, practical biometric system cannot make correct decision sometimes. However, system accuracy can be improved by finding invariance, descriptive, discrimination and distortion tolerates features/model to represent the biometric traits.

Scalability refers to the size of the biometric database. Scalability issues will be posed if the system is incapable of an efficient response to matching requests from the extremely large-scale biometric database (Leiming and Sakamoto, 2012).

The problem of ensuring the security and integrity of the biometric data is critical. The first is that biometric features are irrevocable. Assuming a person's biometric information like fingerprint image is stolen, it is impossible to replace it like the case of stolen smart card, ID or reset a password. The second is that biometric data only provides uniqueness without providing secrecy. For instance, a person leaves his fingerprint on every surface he touches,

and face image can be observed anywhere by anyone. The fact that biometric data is public and irrevocable couple with the existence of several types of attack that are possible in a biometric system, makes the issues of security/integrity of biometric data extremely important.

Privacy and ethical issue of the biometric system is another challenge. Biometric data can be abused for unintended purpose easily. Take for instance fingerprint image stored in the database of national policy system may be used later for gaining access to your laptop computer with the embedded fingerprint reader. Ethical deployment requires transparent consent practices and the ability for individuals to opt out without penalty. OVIC (2019) listed some of the privacy issues that may arise from the use of biometrics. They are:

- i. **Function Creep.** Function creep occurs when information is used for a different purpose than it was collected for. Systems designed for access control can be repurposed for mass surveillance without user knowledge. This becomes a concern then the secondary use is not of providing their information.
- ii. **Convert-Collection.** Convert or passive collection of individuals' biometric information without their consent, participation, or knowledge is another privacy risk. For instance, facial biometric can be captured from photographs that individuals do not know are being taken and latent fingerprints can be lifted to collect biometric information long after an individual has contacted a hand surface.

Biometric Security Techniques

Studies have proven that despite the boost in user accessibility using biometric, they are still prone to several attacks (Taha, 2020). One of the main problems is that biometric signal is not secret and cannot be replaced after being compromised by a third party (Choudhury et al., 2018). Therefore, adopting methods for converting biometric features into secure signals that can be stored in the biometric database to be used for authentication is of utmost concern. Jain and Kant (2015) opined that all the techniques used for biometric template protection are known for resisting attacks. This section focuses on some of these techniques.

Information Hiding

A key factor in security biometric data is the use of information security techniques which is made up of information encryption and information hiding. Information hiding comprises of steganography and watermarking (Taha et al., 2020).

- i. **Steganography.** Steganography is a Greek word meaning "Canceled writing". Kour and Verma (2014) opined that steganography is not only the art of hiding data but also hiding the fact of transmission of secret data. Steganography hides the security data in another file in such a way that only the recipient knows the existence of messages. Mahdi et al (2019) defined steganography as the science and art of secret communications which involves the hiding of information inside another information. Compared to cryptography, steganography message are not self-revealing because data is canceled in a manner that makes its detection to the human eye difficulty. With steganography, the data is concealed in a carrier such as a video text, or audio (Hashim et al, 2018). Several steganography methods exist based on the type of carrier media, including (image, video, text and audio) steganography (Bhattacharyya et al., 2012). The carrier media on steganography is referred to as the cover object while the hidden information is referred to as the payload capacity. The cover object used depends on the volume of secret data to be embedded, while the imperceptibility of the secret message depends on the systems' robustness. Image is the commonest carrier media due to its wide usage on daily applications, as well as its high rate of redundancy. The stego image is the secreta data which is hidden in a cover image (Hashim et al., 2019).

To enhance the effectiveness of a steganography method, its security, capacity and imperceptibility-related issues must be addressed. Among these areas of concern, the imperceptibility of the system is weighty as it relates to how difficult it is to differentiate the existence/absence of a secret message. The imperceptibility of the system can only be achieved through an odd/even pixels distribution format. Another area of concern is the security which relates to the ability of a steganography system to withstand external attacks. And the issues of capacity which relates to the maximum volume of information that can be safely embedded in a cover image without much distortion and a high level of data undetectability (Haghim et al., 2019). The paper suggests an improvement on the steganography system based on the P_Even/P_Old pixel scheme, which employs a micro level encryption system and 2 control random parameters for embedding secret text with a high level of security and with neither a comprise on the stego images quality nor a secret message loss. Vatsa et al., (2005) explained that the World War 2 witnessed a form of steganography when the micro dot technique was developed by the Germans which allowed them to condense information, mostly photographs, to the size of a dot before being distributed over an unprotected channel.

Kour and Verna (2014) presented six (6) technique of steganography in their paper “Steganography Technique- A Review Paper”.

- i. **Spatial Domain Methods.** In this method the secret data is embedded directly in the intensity of pixels. It means some pixel values of the image are changed directly while hiding data.
- ii. **Spread spectrum Technique.** In this method the secret data is spread over a wide frequency bandwidth. The ratio of signal to noise in every frequency bond must be so small that it becomes difficult to detect the presence of data. Even if parts of data are removed from several bands, there would be still enough information present in other bands to recover the data. It is very robust techniques mostly used on military communication.
- iii. **Satisfied Technique.** Message is embedded in changing several properties of the cover. It involves the splitting of cover into blocks and then embedding one message bit in each block. The cover block is modified only when the size of the message bit is one otherwise no modification is required.
- iv. **Transform Domain Technique.** The secret message is embedded on the transform or frequency domain of the cover. Different algorithms and transformations are used on the image to hide message in it.
- v. **Distortion Technique.** In this technique the secret message is stored by distorting the signal. A sequence of modification is applied to the cover by the encoder. The decoder measures the differences between the original cover and the distorted cover to detect the sequence of modifications and consequently recover the secret message.
- vi. **Masking and filtering.** These techniques hide information by marking an image. Steganography only hides the information whereas watermarks becomes a portion of the image. These techniques embed the information in the more significant areas rather than hiding it to the noise level.

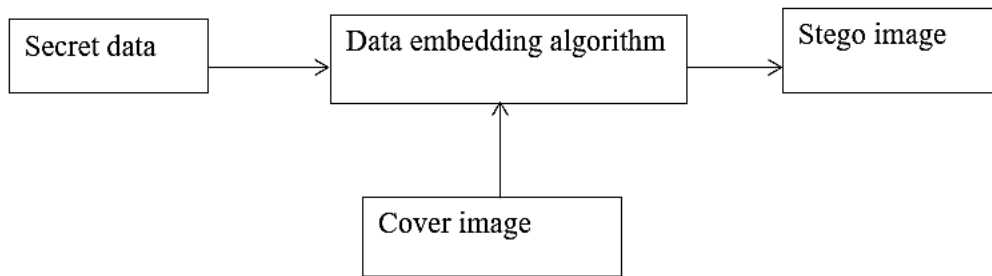


Figure 2. Block diagram of steganography.

Steganography consists of two terms that is message and cove image. Message is the secret data that needs to hide and cover image is the carrier that hides the message in it.

In steganography the process of hiding information content inside any multimedia content like image, audio, video is referred to as Embedding (Kour and Verma, 2014).

Watermarking technique

Digital watermarking or simply watermarking refers to the hiding of information of multimedia data in a host data (Taha et al., 2020). Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated in the image (Kour and Verma, 2014). Watermarking methods are classified into 2 groups based on the watermarking application domain. For the spatial domain methods, the pixel value on the image channels are changed (Taha, et al., 2019) but in the spectral-transform domain, a watermark signal is incorporated to the host image in a transform domain (Hashim et al., 2019). A combination of several conditions such as (i) The characteristics of the introduced noise by the watermarking framework and (ii) The architecture of the recognition system determines the extent the artifacts of a watermarked image can be tolerated by a recognition system (Taha et al., 2020).

Watermarking digital objects like pictures, video a software is usually achieved by embedding a special piece of information, its mark into the object so that it is difficult for an adversary to remove it without damaging the object itself, or to introduce a fresh and legible mark (Baldimtsi, et al., 2017). The requirement of digital watermarking system, whose simultaneous presence distinguishes it from the other data hiding techniques, are capacity, robustness, security, and imperceptibility (Yu et al., 2019). In practice, the requirement of imperceptibility implies that the perceptual quality of the watermarked data should be kept high.

The watermarking process is comprised of watermark insertion and watermark extraction. Image content is verified using the extracted watermark in order to detect unauthorized tampering. During watermark insertion, a watermarked image $I(i,j)$ is produced by embedding the watermark image $W(i,j)$ into source image $I(i,j)$. Each pixel in the source image is processed in turn. This process applies a watermark extraction function $WX(*)$ to the selected pixel $I(i,j)$ before testing the extracted binary watermark value $b(i,j)$ to determine if it is equal to the intended watermark value $W(i,j)$. Should the extracted and embedded watermarks be equal, the processing enters to the next pixel, but if not, the value of the selected pixel is altered until the extracted watermark value equals the desired value (Sharifara et al., 2013).

Biometric cryptosystem

A biometric cryptosystem securely binds a digital key to a user's unique biometric data, such as a fingerprint or iris, to generate or unlock cryptographic keys for authentication and security, preventing the biometric data itself or the key from being stored or reconstructed from the template. This method enhances security and privacy by eliminating the need to remember

passwords or tokens, leveraging the strengths of both biometrics and cryptography. A digital cryptographic key is generated during the enrollment process and user's biometric signal captured and converted into a digital representation (biometric template). The key is then securely "bound" or associated with the biometric template and often using a scheme like fuzzy vault. The main idea of biometric-based keys is that the biometric features perform user authentication, while a generic cryptographic system handles the other components of containment like secure communication.

Cancelable biometric

Cancelable Biometrics is aimed at enhancing Privacy Protection and Template security in existing biometric system(s). In this field, the template of a person is distorted in such a manner that the original data is not available to the intruder but still identity recognition can be performed (Rawat and Kumar, 2020). Cancelable biometrics resolves privacy-related issues, as it prevents the system from storing the original biometric traits of the user. Cancelable biometrics refers to the intentional, recursive distortions of the biometric pattern using a certain transformation, which provides a comparison of the biometric template in the transformed domain (Rathgeb et al, 2014), cited by (Choudhury et al., 2018).

The Cancelable Biometrics must possess four important characteristics; Diversity (ii) Reusability or revocability (iii) Non-invertibility (iv) performance and the template is generated using some techniques such as Hashing, Filtering, Cryptography etc. (Rawat and Kumar, 2020). The cancelable biometric is categorized into (i) Biometric salting and (ii) Non-invertible transforms. There are various methods prepared by different researchers, such as Random Projections, Bloom Filters, Bio-Hashing methods still fall under these two categories (Choudhury et al., 2018).

Multi-Biometric system

The identification of users using two or more biometric traits is done using a multi-biometric system (Taha et al., 2020). Patra (2006) cited by (Taha et al., 2020) in his study, showed that the security of multibiometric systems is higher than those of unimodal biometric systems mainly because of the existence of several data. The study discussed how an authentication process can be done based on multiple characteristics and believed that it is more difficult for an intruder to trick a system that uses multiple biometrics.

Homomorphic encryption

Homomorphic encryption is a cryptographic technique that allows computations to be performed directly on encrypted data without needing to decrypt it first. The results of these computations, when decrypted, are identical to the outcomes of operations performed on the plaintext data. According to Webster dictionary, the word homomorphism is derived from the Greek word homos meaning "same" and morphe meaning "shape". Homomorphic encryption in computer science is used in the conversion of plaintext to ciphertext. Plaintext data is encrypted into ciphertext using a homomorphic encryption algorithm. The result is decrypted to obtain the final output, equivalent to operations performed on plaintext. Plaintext is any information that a sender desires to transfer to a receiver. It can be thought of as the input to any algorithm or as information being transmitted before an algorithm encrypts it. Some examples of plaintext include email messages, word processor files, images, or ATM and credit card transaction information. This plaintext is converted to ciphertext which is data that has been encrypted and is unreadable until it has been decrypted with a key (Ogburn et al., 2013). Application of homomorphic encryption in the domain of cyber-crime prediction and control is enormous. It's used for data privacy. Organizations and individuals can share sensitive data

like user behaviors, transaction logs in encrypted form with a centralized cybercrime prediction system. The system performs computations like risk assessments on the encrypted data without exposing the plaintext to unauthorized parties. Again, cybercrime prediction and control models can be trained on encrypted data, allowing organizations and individuals to contribute to the model without exposing proprietary or personal information. Also, while ML helps create predictive models for conditions ranging from financial transactions crimes to investment outcomes, often regulations and policies prevent organizations from sharing and mining sensitive data. Fully Homomorphic Encryption FHE, enables the computation of encrypted data with ML models without revealing the information. Finally on this note, user data can be sent in encrypted form to the system for predictions. The prediction model processes the encrypted input and sends back the encrypted result, which can only be decrypted by the user.

Biometrics security threats

The template protections schemes are developed for enhancing the security of biometrics templates; however, these template protection schemes, are also vulnerable to security threats (Choudhury et al, 2018). While the biometrics system is considered to be a secure way of authentication, the imposters also created new ways to bypass the security of the biometrics system. There are eight possible threats against biometrics systems (Choudhury et al., 2018). This session discusses some of these security threats.

- i. **Attack on the sensors.** The intruders can present fake biometrics in front of the sensors (Choudhury et al., 2018). Someone can present fake biometric traits to the capturing devices to bypass the biometric system or even wear some kind of lenses to bypass iris scanner. The possible solution for this type of attack is liveness detection, multibiometric and soft biometrics (Kameldeep, 2011). Liveness detection mechanism helps to find out if the presented biometric trait is provided by the live human or it is just an artifact. Using an extra hardware or software, it is possible to detect various live signs (Choudhury et al., 2018).
- ii. **Template inversion.** Reconstruction of biometric traits from stored templates termed inverse biometrics poses serious risks. Template inversion (TI) attack against FR systems refers to an attempt by an adversary to reconstruct face images from the templates stored in the system's database (Hatef and Sebastien, 2023),
- iii. **Replay attack.** Replay attack is an attack on the communication channel between the sensors and the feature extractor module. Reusing previously captured signals. In this attack an imposter can steal the biometric data and later can present old, recorded data to bypass the feature extraction module Choudhury et al, 2018). This type of attack can be prevented by steganography, response system (Choudhury, 2018).
- iv. **Overriding feature extractor.** In this attack, the feature extractor is substituted by a Trojan horse and controlled remotely to intercept the biometric system.
- v. **Attack by synthesized feature vector.** In this attack, the route from the feature extractor to the matcher is intercepted to steal the feature vector of the authorized user. The stolen feature vector is replayed later to bypass the matcher.
- vi. **Overriding matcher.** The matcher is overridden by a Trojan horse. In this way intruder can control the matching score and can generate a high matching score to confirm authentication to the imposter (Bolle et al., 2018).
- vii. **Attack on the database.** The attacker can intervene the database where the templates are stored to compromise the biometric traits. By breaking the security of the template database, an intruder can replace the biometric trait of the illegitimate person, can modify or delete the existing in (Choudhury, 2018). To counter the attack against this

- attack, various methods for template Protection are proposed. Cancelable biometrics and Cryptosystem are such template protection scheme (Kamaldeep, 2011).
- viii. **The attack on the channel between the database and the matcher.** In this type of attack, the invaders intrude on the channel to replay old data or to modify the existing data. This attack can also be prevented by a challenge response system, watermarking and steganography technique.
- ix. **Override the final decision.** This is the attack on the application. As all the software application has bugs, an intruder can override the actual decision made by the matcher using soft biometrics, this kind of attack can be prevented (Kamaldeep, 2011).

Conclusion

Secure biometric signal processing represents a critical step toward building trustworthy, and privacy-preserving biometric systems. While advances in cryptography, template protection, and privacy-preserving machine learning provide strong foundations, significant challenges persist in balancing accuracy, efficiency, and robustness. Secure biometric signal processing (SBSP) stands at the intersection of security engineering, signal processing, and ethical governance, offering both immense opportunities and significant challenges. As biometric technologies become integral to authentication in banking, e-governance, healthcare, and digital identity systems, ensuring their security and trustworthiness is no longer optional but fundamental. This review has shown that, while biometrics offer superior uniqueness and convenience compared to traditional credentials, their permanence and sensitivity create unprecedented risks. A compromised biometric identifier cannot be revoked or replaced, making privacy protection and attack resilience central to any secure deployment. This paper discusses in details some biometric security techniques to secure the biometric signals. First, biometric systems face systemic challenges, including Accuracy, scalability, security, privacy and ethical issues all of which undermine their reliability and fairness. Second, a wide range of security-enhancing techniques such as cancelable biometrics, biometric cryptosystems, multimodal fusion, and homomorphic encryption were also discussed. Third, the spectrum of security attacks has expanded rapidly, from spoofing and replay attacks to sophisticated adversarial machine learning attacks, indicating that traditional defense mechanisms are insufficient in isolation.

Recommendation

The study recommends the following:

- i. Robust biometric template protection. Adoption of cancelable biometrics and biometric cryptosystems to ensure that compromised templates can be revoked and reissued, and the adoption of homomorphic encryption for privacy-preserving biometric matching sensitive domains like banking and healthcare.
- ii. Adoption of multimodal and adaptive systems. Encourage the integration of multimodal biometrics (e.g., fingerprint plus iris plus voice signals) to increase robustness against spoofing and reduce the probability of false acceptance. And develop adaptive signal processing frameworks that can dynamically update models when faced with new environmental conditions or adversarial attacks.
- iii. Ethical and privacy-by-design approaches. Incorporate privacy-by-design principles into biometric systems to limit function creep and unauthorized surveillance and establish clear user rights, such as the right to opt out and the right to data deletion.

REFERENCES

- BalDIMstise, F., Kiayias, A., & Samari, K. (2017). Watermarking Public-Key cryptographic functionalities and implementations. <https://www.eprint.iacr.org/2017/557.pdf>.
- Barni, M. Droandi, G., & Lazzereti, R., (2015). Privacy Protection in Biometric-Based recognition system. A marriage between cryptography and signal processing. IEEE signal processing magazine. <https://www.researchgate.net/publication>
- Choudhury, B., Patrick, T., Isaac, B. Roman, V., & Halder, M.K. (2018). A survey on biometric and cancelable biometric system. International journal of image and graphics. 18 (01).<https://www.researchgate.net/publication/322680611>
- Christian Rathgeb, Frank Breiting, Christoph Busch, Harald Baier. 2014. On Application of Bloom Filters to Iris Biometrics. IET Biometrics, 3(4). (2014) 207-218. DOI: <http://dx.doi.org/10.1049/iet-bmt.2013.0049>
- Dakic, M. (2023). What is voice recognition technology and it's benefits. <https://www.zesium.com/what-is-voice-recognition-and-its-benefits/>
- Ekong V.E (n.d.). Current trends in computing: Biometrics technologies (Lecture note). Department of computer science, University of Uyo.
- Faundez-Zanuy, M. (2022). Biometrics security technology. <https://www.arciv.org>.
- Hashim, M. M., Taha, M.S., Aman, A. H.M., Hashim, A. H. A., Rahim, M. S. M., & Islam, S. (2019). Securing medical data transmission systems based on integrating algorithm of encryption and steganography. In 2019 7th International Conference on Mechatronics Engineering (ILOM) (Pp 1-6). IEEE. <https://www.researchgate.net/publication/341775133>.
- Jain, R. & Kant, C. (2015). Attack on biometric systems: An overview. International journal of advances on scientific research 1 (7). <https://www.researchgate.net/publication/322225967>
- Kamaldeep (2011). A review of various attacks on biometric system and their known solutions. *International Journal of Computer Technology and Application*, 2(6).
- Kour, J. & Verma, D. (2014). Steganography techniques. A review paper. *International Journal of Emerging Research in Management & Technology*, 3(5). <https://www.diwa/tnts/xzle.clondfront.net/61279125..>
- Meitei, T. G., Singh, S. A., & Majunder, S. (2018). Handbook of research on information security in biomedical signal processing. <https://www.researchgate.net/publication/324517001>
- Prathusha, P., Lakshmi, K., haritha, K., divya, B. S., & Navya, B. V. (2022). An Efficient and Privacy-Preserving Biometrics Identification Scheme In Cloud Computing. *Journal of Engineering Sciences* 13(07). <https://www.jespublication.com>
- Bayer, F., & Rathgeb, C. (2025). *AMB-FHE: Adaptive multi-biometric fusion with fully homomorphic encryption*. arXiv. <https://arxiv.org/abs/2503.23949>
- Rane, S., Wange, Y., Daper S.C., & Ishwar, P. (2013). Secure biometrics; concepts, authentication architectures and challenges. IEEE signal processing magazine 30 (5). <https://www.ieeexplore.ieee.org/document/6582729>
- Rawat, M. & Kumar, N. (2020). Cancelable biometrics: A comprehensive survey artificial intelligence review 53 (1). <https://www.researchgate.net/publication/322225967>.
- Taha, M.S., Rahim, M.S.M; Zeebaree, D.Q, Hashim, M.M, Khadlid, H.N. (2020). Information hiding: A tools for securing biometric information. *Technology report of Kansai university* 62 (04):1383-1394. <https://www.researchgate/publication/341775733>.
- Vain, R. & Kant, C. (2015). Attacks on Biometric systems: an overview. *International Journal of Advance in Scientific Research*, 1(7): 283.

- https://www.researchgate.net/publication/322225967_Attacks_on_Biometric_Systems_An_Overview.
- Yu, M., Wang, Y., & Jiang, G. (2019). High dynamic range image watermarking based on tucker decomposition. IEEE Access. Pp(99).
<https://www.researchgate.net/publication/335200734>.
- Office of the Victorian Information Commissioner. (2019). Biometrics and privacy: Issues and challenges. <https://ovic.vic.gov.au/resource/biometrics-and-privacy-issues-and-challenges/>
- Jain, A. K., Nandakumar, K., & Ross, A. (2021). *50 years of biometric research: Accomplishments, challenges, and opportunities*. Pattern Recognition Letters, 147, 80–105. <https://doi.org/10.1016/j.patrec.2021.03.023>
- Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2019). *Handbook of fingerprint recognition* (2nd ed.). Springer. <https://doi.org/10.1007/978-1-4471-6874-9>