A Survey on Biometrics and Cancelable Biometrics Systems

BISMITA CHOUDHURY, Swinburne University of Technology (Sarawak campus), Malaysia
PATRICK THEN, Swinburne University of Technology (Sarawak campus), Malaysia
BIJU ISSAC, School of Computing, Media and the Arts, Teesside University, UK
VALLIAPPAN RAMAN, Swinburne University of Technology (Sarawak campus), Malaysia
MANAS KUMAR HALDAR, Swinburne University of Technology (Sarawak campus), Malaysia

Abstract: Now-a-days, biometric systems have replaced the password or token based authentication system in many fields to improve the security level. However, biometric system is also vulnerable to security threats. Unlike password based system, biometric templates cannot be replaced if lost or compromised. To deal with the issue of the compromised biometric template, template protection schemes evolved to make it possible to replace the biometric template. Cancelable biometric is such a template protection scheme that replaces a biometric template when the stored template is stolen or lost. It is a feature domain transformation where a distorted version of a biometric template is generated and matched in the transformed domain. This paper presents a review on the state-of-the-art and analysis of different existing methods of biometric based authentication system and cancelable biometric systems along with an elaborate focus on cancelable biometrics in order to show its advantages over the standard biometric systems through some generalized standards and guidelines acquired from the literature. We also proposed a highly secure method for cancelable biometrics using a non-invertible function based on Discrete Cosine Transformation (DCT) and Huffman encoding. We tested and evaluated the proposed novel method for 50 users and achieved good results.

Key Words: Biometrics, Cancelable Biometrics, Security, Biometric Salting, Non-Invertible Transformation

1. INTRODUCTION

The biometric traits possessed by each individual are unique and has the potential to recognize an individual. Biometric traits can be physical and behavioral. Therefore, biometrics are used for authentication or recognition of individuals for many critical applications like border control, access control, immigration, forensic and different law enforcement. There are two phases in every conventional biometric system: enrolment phase and authentication phase. In the enrolment stage, the original biometric trait is captured and saved in the database. During the authentication stage, the system matches that stored template every time the user access the system by providing the live biometric (Kaur et al. 2014).

Compared to password or token based authentication system, biometric system using fingerprint, iris, face, voice, etc. provides better security as people cannot lose or forget their biometric trait. But, the advanced technology of today's world makes it possible to create a loophole in the biometric system. People leave their fingerprints on whatever they touch; hence one can easily steal the fingerprint and can even make an 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.

To overcome the problem of the stolen biometrics, the researchers have developed the template protection schemes. The biometric template protection schemes are mainly divided into two categories: i) Biometric Cryptosystem and ii) Cancelable Biometrics (Rathgeb et al. 2011). Figure 1 shows the different categories of the template protection scheme. The biometric cryptosystem encrypts the biometric data to store it. Then, during authentication, the stored template is decrypted to do the comparison. While cancelable biometrics matches the templates in the transmuted domain itself during the authentication phase. Cancelable biometrics provide the comparison decision in terms of Match or Non-Match. On the other hand, biometric encryption releases a cryptographic key or an encoded token. The template protection schemes are designed to follow certain criteria (Rathgeb et al. 2011):

(a) Non-invertibility: It should be unlikely to recreate the original biometric data from the transformed one.
(b) Diversity: The different versions of the transformed templates should be identical so that cross-matching is not feasible.
(c) Reusability: It should be able to produce diverse versions of protected biometric templates from the one original template.
(d) Performance: Employing template protection scheme must not reduce the overall performance of the system.

The survey is focused mainly on the conventional biometric system and cancelable biometrics. Section 2 discusses on the various biometric modalities. The functionality of the biometric system is described in Section 3. Then, Section 4 discusses the possible attacks on the biometric system and

their solutions. Cancelable biometrics and its types are briefly discussed in section 5. The state-of-the-art for cancelable biometrics is elaborated in section 6. Section 7 discusses the different security attacks on the cancelable biometrics scheme. The advantages of cancelable biometrics over the traditional biometrics system and the open problems of the cancelable biometrics are described in Section 8. A novel method for cancelable iris biometrics is discussed in Section 9, followed by the conclusion in Section 10.

2. BIOMETRIC MODALITIES

The prime advantages of using biometric traits are that biometrics cannot be forgotten, cannot get lost, it is permanent and difficult to forge. There are several different biometric traits that can be used for recognition, e.g., fingerprint, iris, voice, keystroke pattern, gait, signature, retina, vein patterns, hand geometry, brain signals (EEG), etc.

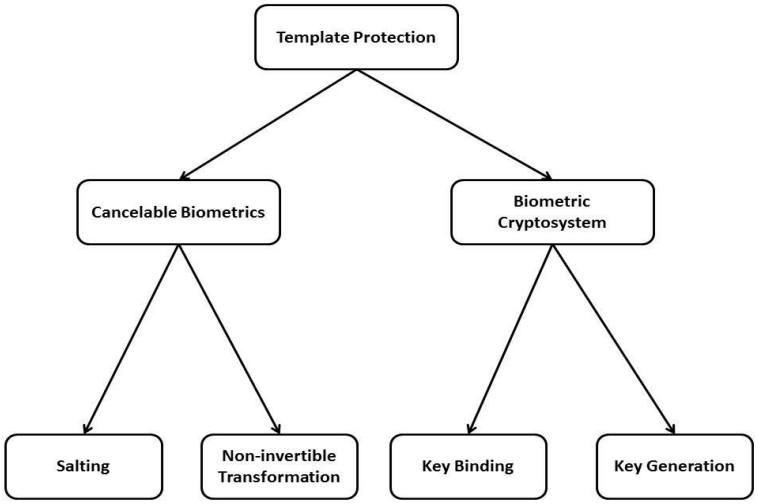


Fig. 1. Block diagram of the different categories of template protection schemes

The biometric traits can be categorized into physical, behavioral and both physical and behavioral modalities (Kaur et al. 2014). The physical modality deals with the body shape and includes fingerprint, face, hand geometry, iris, retina, vein, ear shape, face, DNA, etc. The behavioral modalities relate to the human behavior that can vary over time, such as keystroke pattern, signature, and gait (Jaiswal et al. 2011). There are some biometric traits that act as both physical and behavioral characteristics; e.g., voice and brain waves or EEG. Our voice depends on the shape of the mouth, but it varies over the time. The Electroencephalography or EEG depends or the head or skull shape and size, but it changes time to time depending on the circumstances and varies according to the age. Thus, depending on the biometric traits, biometric system can either be contact or contactless.

In this section we will discuss about the existing and emerging biometric traits having the ability to distinguish individuals.

2.1 Face Recognition:

In facial recognition, the spatial geometry like shape, size, the structure of the face is considered as features to recognize a person (Zhao et al. 2003). Facial recognition is one of the easy and popular ways of recognizing the individuals. 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.

2.2 Ear Geometry

The shape of the outer ear, bone structure and ear lobe are considered for person recognition using the ear. However, ear structure is not distinctive enough for recognition, prone to external injury and shape, size changes over time (Jaiswal et al. 2011), (Abaza et al. 2013).

2.3 Smile Recognition

The smile is captured by high-speed cameras. The slight movements of the lips, the wrinkles in the skin, muscle movement around the lips are observed in the acquired smile map (Goudelis et al. 2008), (Akkoca et al. 2015).

2.4 Fingerprint

The fingerprint is the most popular way for biometric authentication. The pattern of the ridges and furrows of the fingers are unique for each individual. Therefore, based on the pattern of the ridges, furrows and minutiae points a person is identified or verified (Hasan et al. 2013). The advantage of fingerprint biometric is that it is socially acceptable, easy to collect the fingerprint and even the fingerprint of each finger on the same hand are different from each other. The limitation of the fingerprint is that, the factors like a person's age, occupation or any kind of accident might make it difficult for the sensors to capture the fingerprint (Goudelis et al. 2008).

2.5 Hand Geometry

The hand geometry recognition method measures the physical structure of the hand, including size, length, width, the shape of the finger, gaping between the fingers, etc. (Gonzalez et al. 2003). The advantage is the ease of acquisition and supposed to be stable over the time. But, it requires training for the users, needs a large space or sensor to acquire the hand geometry and not distinctive enough to distinguish over large database (Jaiswal et al. 2011).

2.6 Finger and Hand Knuckles

It is feasible to distinguish a person based on the structure of the finger or hand knuckles. Depending on the hand or finger knuckles' texture, the wrinkles around the knuckles, recognition is done (Aoyama et al. 2014)

2.7 Palm Print

In palm print, the entire hand palm is taken as a biometric trait. It is similar to a fingerprint in terms feature extraction and matching process. In fingerprint, the minutiae points of one finger (or more) are taken as features. Considering the minutiae points of all five fingers, the palm print has more number of minutiae points to make comparisons during the matching process (Kong et al. 2009) compared to fingerprint.

2.8 Nail ID

Human nailbed is one of the latest biometric modality. The nailbed is a distinctive tongue-and-groove longitudinal arrangement of papillae and skin folds organized in parallel rows. Naibed consists of Keratin microfibrils, those are situated at the boundary between the nailbed and the nailplate, or fingernail. Using a broadband interferometer technique, the polarized phase changes are detected by exposing the light through the nailplate (Goudelis, 2008), (Kumar et al. 2014).

2.9 Iris

Iris is the pigmented portion of the eye. The region between the pupillary boundary and the limbic boundary is highly rich in texture and that remains same throughout the life (Kaur et al. 2014), (Bowyer et al. 2008). Iris provides high accuracy and it is less prone to external injury. It is contactless and possesses a high degree of randomness. Moreover, the iris texture of both eyes is different from each other. The main problem with the iris biometric is that the eye is obscured by eyelids, eyelashes, reflection, contact lenses, glasses, etc. The image acquisition process requires more training (Bowyer et al. 2008).

2.10 Retina

Retina refers to the blood vessel pattern found in the back of the eye. To perceive the blood vessel pattern, a bright light source is focused into the eye (Goudelis et al. 2008), (Borgen et al. 2008). Because of the highly intrusive property, authentication process using retina scanning is not socially acceptable. Moreover, the pattern changes during medical conditions like pregnancy, blood pressure, other ailment etc. (Kaur et al. 2014).

2.11 Signature

Every person has a unique writing style and hence a person has an own identical signature. The biometric system that identifies a person using the dynamic signature, measures the speed and the direction of writing, pressure applied while writing, the interval when stylus comes in the contact of the writing surface, time taken to finish the signature (Plamondon et al. 2008), (Zanuy et al. 2007). However, dynamic signature is not considered as a reliable trait to identify a person.

2.12 Keystroke

Examining the dynamic keystroke is another biometric trait to recognize a person (Monrose et al. 2000). It is a behavioral characteristic. This technology measures the time taken to type particular word; time, pressure and speed while hitting the keys. This technology is still developing (Goudelis et al. 2008).

2.13 Voice

Voice recognition is a popular method for authentication. It identifies the vocal characteristic of the individual while uttering the pass-phrase or password. But, this technology is highly affected by the background noise (Yoshioka et al. 2012).

2.14 Gait

The gait is the way a person walks. So, the recent technology makes it possible to recognize a person by observing the walking style or gait (Liu et al. 2009).

2.15 DNA

DNA is an emerging biometric trait that can be used for recognizing individuals. The specific area of the long DNA sequence is observed to find the identical feature. DNA itself is unique for each individual, except the identical twins. Therefore, it achieves high accuracy. DNA can be acquired easily from hair, saliva, skin follicles etc. However, the process is time-consuming and expensive (Jain et al. 2004), (Zayaraz et al. 2009).

2.16 Brainwave or EEG

Electroencephalography or EEG is an emerging and promising biometric trait to recognize a person. The EEG based recognition system captures the brain waves by electrodes and identifies the unique brain signals stimulated by the given task. It provides high security and accuracy. However, it is a time consuming and expensive process. Moreover, brain signals for specific task might change during different circumstances and even it is possible for a person to change his/her own brainwave pattern (Khalifa et al. 2012), (Gui et al. 2014).

2.17 Electrocardiography or ECG

Recently, researchers have discovered that heartbeat of every person differs from each other. Using ECG, fiducial points are extracted from the heart. From the fiducial points identical features are extracted for person recognition. Similar to EEG, it is a time consuming and complex process (Odinaka et al. 2012).

2.18 Body Odor

Body odor is considered as one of the biometric trait that can recognize a person. Each person has a unique body odor and such chemical agents of human body odor can be extracted from the pores to recognize a person (Shu et al. 2014).

2.19 Facial Thermography

It is the heat pattern emitted by the face vascular system. Heat generated by the facial tissues is unique and has a measurable repeatable pattern. It is more stable than the facial structure (Prokoski et al. 1992), (Hanmandlu et al. 2012).

2.20 Body Salinity

It is believed that the salinity level of the salt in the body is unique for each individual. The salt level in the body is analyzed by passing a small amount of electrical current through the body (Zhao et al. 2003).

2.21 Hand Vein Pattern

The blood vessels underneath the skin are unique from person to person. The structure of the hand vein patterns can be captured using infrared sensors. The vein patterns tend to remain constant over a long period of time. However, visibility depends on the factors like age, mole, physical activity, thickness of the skin etc. (Yuksel et al. 2010).

G. Kaur et al. (2011) provided an extensive comparison among different biometric modalities based on the properties like universality, uniqueness, permanence, performance, circumvention, social acceptance, security evaluation, etc. Based on their assessment, we have provided a comparison study of different biometric modalities in relation to the uniqueness, permanence, performance, circumvention, False Acceptance Rate (FAR) and False Reject Rate (FRR). Table I shows the comparison of various modalities based on the properties like uniqueness, permanence, performance, circumvention, processing speed and accuracy. Here, the uniqueness defines the capability of the biometric trait to discriminate a person. The permanence refers to the consistency of remaining the same for a long duration of the life. Performance refers to the overall performance of the authentication system in terms of security and speed. Circumvention refers to the difficulty to forge the biometric trait. Processing speed refers to the time taken by the authentication system to verify or identify an individual. The accuracy refers to how accurately the system can recognize an individual using that biometric trait. They also evaluated different biometric systems in terms of Crossover Error Rate (CER), also defined as Equal Error Rate (EER). The CER is a metric for comparing different biometric devices and technologies. It is an error rate when FAR equals to FRR, and so, the lower value of EER/CER indicates high reliability of the biometric device. Figure 2 shows the Equal Error Rate (EER) or CER of the biometric system using different biometric traits. The EER for iris is 0.01%. From the evaluations based on the properties and the performance, the iris is considered as an effective and efficient biometric trait among all the biometric traits for the recognition purpose.

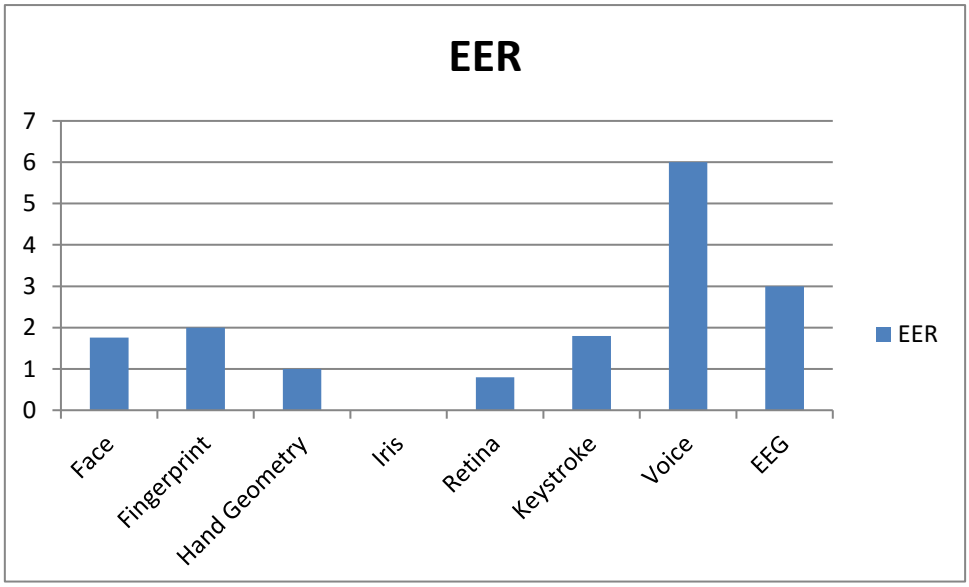


Fig. 2. The Equal Error Rate (EER) or Crossover Error Rate (CER) for different biometric systems (Kaur et al.)

3. FUNCTIONALITY OF THE BIOMETRIC SYSTEM

All the biometric based authentication systems have two main stages: Enrolment phase and Authentication phase. During the enrolment phase, a user is registered with the acquired biometric data. During the authentication phase, the user is recognized by comparing the live biometric trait with the stored biometric data. There are four main steps in the biometric system (Kaur et al. 2011), (Delac et al. 2004).

(1) Biometric data Acquisition: The biometric data are collected using different sensors. For, e.g., the face image is captured using camera, video camera; fingerprints and hand geometry are collected using sensors; iris and retina scanning in done by Infra-Red Camera; gait is captured by walking surface; EEG is captured by electrodes placing over the scalp; keystrokes are acquired by keyboard, writing pad etc.

Table I. Comparison of different biometric modalities based on properties

Biometric Modalities	Uniqueness	Permanence	Performance	Circumvention	Processing Speed	Accuracy
Face	Medium	Medium	Low	High	Medium	Low
Fingerprint	High	Medium	Medium	Medium	High	Medium
Palm print	High	High	High	Medium	High	Medium
Hand Geometry	Medium	Low	Medium	Medium	High	Medium
Iris	High	High	High	Low	Medium	High
Retina	High	High	High	Low	Medium	High
Signature	High	Low	Medium	High	High	Medium
Keystroke	Low	Low	Low	Medium	Medium	Low
Gait	Medium	Medium	Low	Medium	Medium	Low
Voice	High	Low	Medium	High	High	Low
Hand vein	Medium	Medium	Medium	Low	Medium	Medium
Ear	Medium	High	Medium	Medium	Medium	Low
DNA	High	High	High	Low	Low	High
EEG	High	High	Medium	Low	Low	High
ECG	High	High	Medium	Low	Low	High
Facial Thermography	High	Low	Medium	Low	Medium	Medium
Odor	High	High	Low	Low	Medium	Low

(2) Pre-processing: The collected biometric data is pre-processed to discard the noise and improve the signal or image quality for further process.

(3) Feature extraction and Template generation: The most distinguishing features are extracted from the biometric data so that it can identify or verify a person. There are different feature extraction techniques for different biometric modalities. The extracted features are transformed into a template in such a way that it is easily readable and comparable during the matching process. The templates can be either in numeric form or in image form.

(4) Matching: In this step, the input query biometric template is matched with the stored biometric template. Generally, matching is done by distance metrics such as Euclidean distance, Hamming distance, pixel counts, etc. However, recently, a learning based classifier is gaining popularity to classify the authorized and unauthorized person. A matching score is computed by finding the degree of similarity between the live and the stored biometric template. Based on the matching score, a decision is made whether the person is legitimate or not.

Figure 3 displays the block diagram representation of the conventional biometric verification system.

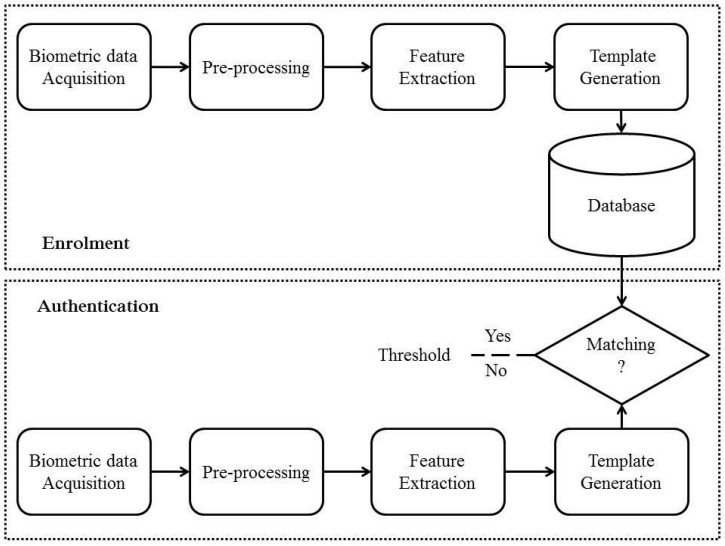


Fig. 3. Block diagram of the Biometric Verification System

4. SECURITY AND PRIVACY ISSUES OF THE BIOMETRIC SYSTEM

While the biometric system is considered to be a secure way of authentication, the impostors also created new ways to bypass the security of the biometric system. The main problem with the biometric based authentication system is that biometric traits are not secret. Intruders can easily get access to the fingerprints, face image, etc. There are eight possible attacks against biometric systems (Kamaldeep 2011). Figure 4 shows the different attacks on the different points on the biometric system for verification. Table II shows the possible attacks on the biometric system and their possible solutions.

(1) Attack on the sensors: The intruders can present fake biometrics in front of the sensors (Jain et al. 2008). For e.g. someone can produce fake finger with fake fingerprints to the sensors; one can produce images of the legitimate user in front of the camera to bypass the face recognition system; one can wear some kind of lenses to bypass iris scanner and so on.

Table II. Different attacks on biometric system and their possible solutions

Attacks	**Solutions**
Attack on the sensor	Liveness Detection, Multi-modal Biometric Systems, Soft Biometrics
Replay Attack	Steganographic and Watermarking Techniques, Challenge-Response Systems
Overriding the feature extractor	-------
Attack by synthesized feature vector	-------
Overriding the matcher	-------
Attack on the database	Cancelable Biometrics, Biometric cryptosystem
Attack on the channel between the matcher and database	Steganographic and Watermarking Techniques, Challenge-Response Systems
Overriding final decision	Soft Biometrics

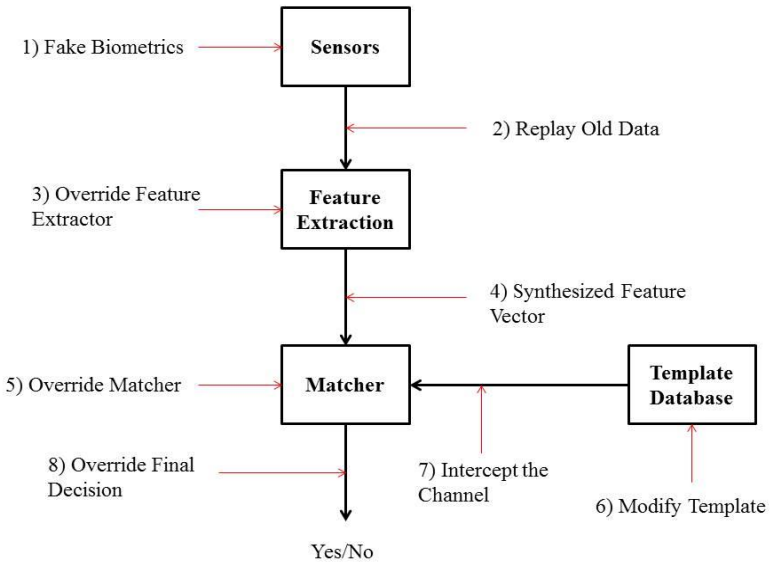


Fig. 4. Possible Attacks on Biometric Verification System

The possible solutions for this type of attack is liveness detection, multi-biometrics and soft biometrics (Kamaldeep 2011). Currently, the researchers are working on liveliness detection. Liveness detection mechanism helps to find out if the presented biometric trait is provided by the live human or it is just an artefact. Using an extra hardware or software, it is possible to detect various live signs. For face recognition, the face temperature, sweating pores, eye movement, face movement; for fingerprint temperature, blood pressure, pulse rate and sweat can be measured; for iris and retina the slight movement of the eyelashes, dilation and constrictions, spontaneous iris movement can be measured. However, employing extra live detection hardware or software makes the biometric system more complex.

Multi-biometrics is another way to prevent this kind of attack and to make the biometric system more secure. In multi-biometrics, two or more biometric traits are considered for authentication. For e.g. combined features of face and fingerprint or fingerprint and iris or iris and face can be used to verify or identify a person. When multiple biometric traits are used, then it becomes challenging for the intruder to get access to all of the biometric traits. So, it can avoid spoofing attack. In multi-biometrics, the multiple biometric are fused either by combining their features or by combining their matching scores. Therefore, the probability to forge the biometric patterns and hack the system is quite low.

Another solution is the soft-biometrics. Soft biometrics in the biometric traits those are not specific enough to distinguish individuals. For e.g., age, skin colour, eye colour, gender, height, weight, etc. While enrolment, if any of the soft biometrics is considered as well, then it can improve the system's security level to some extent. Moreover, it can avoid spoofing and also can contribute to measure the correct threshold for the matching score in both unimodal and multi-biometrics.

(2) Replay attack: Replay attack is an attack on the communication channel between the sensors and the feature extractor module. In this attack, an impostor can steal the biometric data and later can present old recorded data to bypass the feature extraction module (Jain et al. 2008).

This type of attack can be prevented by steganography, watermarking techniques, challenge-response system (Kamaldeep 2011). Using steganography the acquired biometric traits can be securely communicated without giving any hint to the intruders. Steganography is mainly used for covert communication and therefore biometric data can be transmitted to different modules of the biometric system within an unsuspected host image.

Watermarking is a similar technique where an identifying pattern is embedded in a signal to avoid counterfeit. Watermarks are not easily removable. If a watermark is used, it will be difficult for the attackers to provide fake biometric traits. Moreover, biometric data can be watermarked for secure transmission as well.

In challenge-response system, a task or a question as a challenge is given to the person and the person responses to the challenge voluntarily or involuntarily. In this way a biometric system can perceive the presence of the live human being. For e.g. the system asks for some security codes or to

do some actions while presenting the biometric traits to the sensor, and the user responds to the questions or actions.

(3) Overriding feature extractor: In this attack, the feature extractor is substituted by a Trojan horse and controlled remotely to intercept the biometric system (Kamaldeep 2011), (Jain et al. 2008), (Bolle et al. 2002).

(4) 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 (Kamaldeep 2011), (Jain et al. 2008), (Bolle et al. 2002).

(5) Overriding matcher: The matcher is overridden by a Trojan horse. In this way the intruder can control the matching score and can generate a high matching score to confirm authentication to the imposter (Kamaldeep 2011), (Jain et al. 2008), (Bolle et al. 2002).

(6) 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 templates (Kamaldeep 2011), (Jain et al. 2008), (Bolle et al. 2002). To counter the attack against this attack, various methods for template protection are proposed. Cancelable biometrics and biometric cryptosystem are such template protection scheme (Kamaldeep 2011). In cancelable biometrics, instead of the original biometric data a distorted version is stored in the database. Therefore, the intruder cannot get access to the original biometric pattern from the database. In biometric cryptosystem, the biometric data is encrypted before storing in the database. So, it is quite difficult for the attacker to decrypt the data and steal the original template from the database.

(7) The attack on the channel between the database and the matcher: In this type of attack, the invader intrudes the channel to replay old data or to modify the existing data (Bolle et al. 2002). This attack can also be prevented by a challenge-response system, watermarking and steganographic techniques.

(8) 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).

5. CANCELABLE BIOMETRICS

The cancelable biometrics provides a way for authentication even when the biometric template is compromised or stolen. Cancelable Biometric is a template protection mechanism, where the original biometric pattern is distorted intentionally to enroll in the authentication system. When the cancelable biometric scheme is applied, instead of the original biometric pattern a deformed version of the template is stored. In case of conventional biometric system, most of the people show unwillingness to provide their biometric traits as they are concerned about their privacy. Cancelable biometrics resolves such privacy-related issues, as it prevents the system to store 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 (Rathageb et al. 2011). The concept of cancelable biometrics is first provided by N. K. Ratha et al. (2007). The cancelable biometrics is categorized into: i) Biometric salting and ii) Non-invertible transforms. There are various methods proposed by different researchers, however, the base of those methods still falls under these two basic categories.

(1) Biometric Salting: In biometric salting, a user-specific data (password or any random number) is combined with the biometric data to get the distorted adaptation of the biometric template. As the biometric salting process is completely dependent on the external auxiliary data, the method is revocable by simply changing the password. In (Lacharme et al. 2011), a Personal Identification Number or PIN is used to generate a cancelable template for iris recognition. But, salting approach raises serious security issue. Because, the user-specific data can be stolen or compromised and in such situation, the whole system becomes vulnerable. The block diagram of the biometric salting process for verification system is shown in Figure 5. Apart from the user-specific helper data, some methods use random noise pattern, synthetic pattern etc. to create the transformed template. In (Zuo et al. 2008), a random noise pattern is added to generate cancelable iris template.

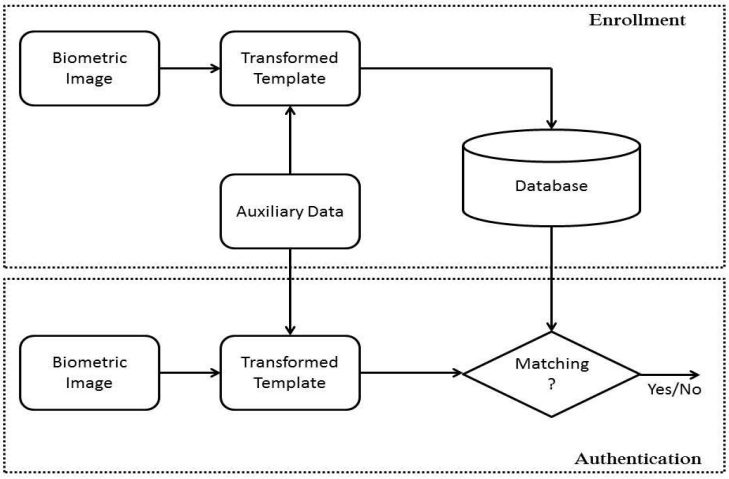


Fig. 5. Block diagram of Biometric Salting for Verification

(2) Non-Invertible Transformation: In case of non-invertible transformation scheme, the biometric data are transformed by applying a one-way non-invertible function. The parameters of the transformation are modified to provide updatable templates. "The transformation is done either in signal domain or in feature domain" (Ratha et al. 2007), (Bolle et al. 2002), (Ratha et al. 2001). The advantage of the non-invertible transform is that the imposter cannot reconstruct the original biometric template even if the transforms are compromised (Rathageb et al. 2011). But the use of non-invertible transformation boosts the performance decrease due to information loss and difficulty in alignment of the templates. Figure 6 exhibits the block diagram of the non-invertible transformation function for biometric verification system.

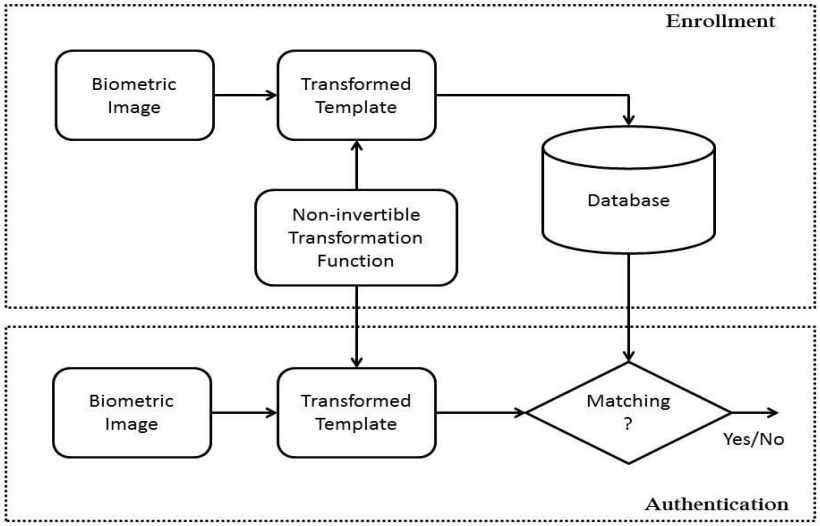


Fig. 6. Block diagram of Non-invertible Transformation Function for Verification

(Ratha et al. 2007) and (Bolle et al. 2002) proposed three transformation functions for fingerprints: "Cartesian, Polar and Surface folding". Before applying the transformation, the image of the fingerprint is registered. In the registration process, the position and angle of the minutiae points are estimated with reference to the location and the orientation of the singular points. In Cartesian transformation, the rectangular co-ordinate system is distributed into cells according to the minutiae points aligned with the orientation of the singular points. Then, the transformation is done by mapping each cell into randomly selected cell. More than two cells can be plotted into the same cell. The transformation can be expressed by the equation:

$$C' = CM \tag{1}$$

where M is the transformation matrix, C is the position of the cell before transformation and C' is the position of the cell after the transformation (Ratha et al. 2007). Figure 7 shows the transformation process by Cartesian transformation.

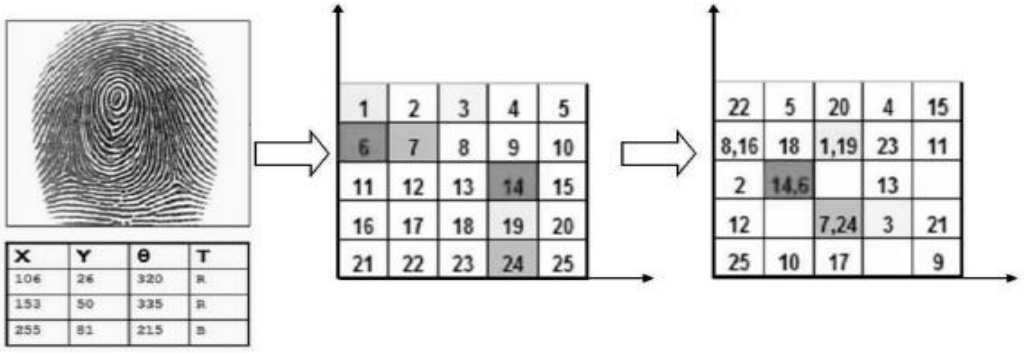


Figure 7: Cartesian transformation of the fingerprint that maps each cell into randomly selected other cell (Ratha et al.)

In Polar transformation, all the features are converted into polar form sector by sector. The minute positions and angles are measured with respect to the core position and orientation. For the transformation, the positions of the sectors are changed by mapping one sector to another random sector (Ratha et al. 2007). If C is the sector position before transformation, C' is the sector position after the transformation and M is the transformation matrix, then polar transformation can be expressed as:

$$C' = C + M \tag{2}$$

Figure 8 shows the process of the Polar transformation.

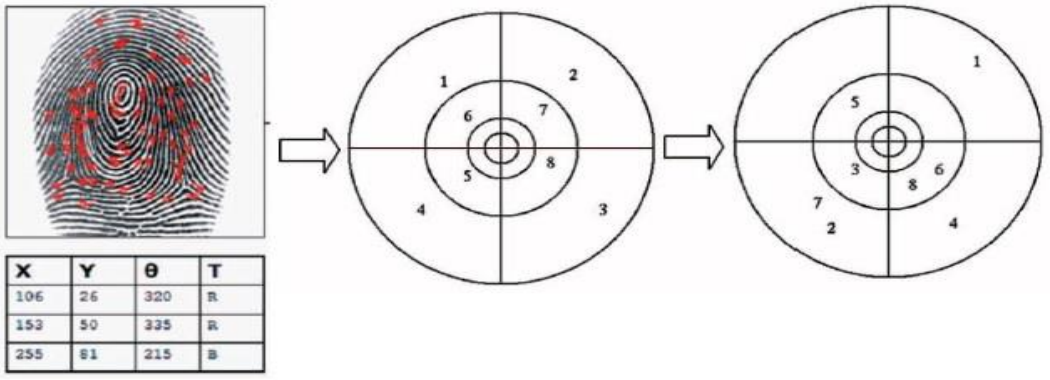


Figure 8: Polar transformation where every sector is mapped to other randomly selected sector (Ratha et al.)

In the surface folding process, the location and the direction of the minutiae points are changed by applying some parameterized transformation function. The function can be parameterized by randomly distributed electric field charge or by randomly mixed Gaussian kernels (Ratha et al. 2007). The direction of translation is modelled by a vector function $\vec{S}(a, b)$. The direction of the translation is determined by the phase Φ and the degree of the translation is determined by the magnitude $|\vec{S}|$ or by another function $\vec{G}(a, b)$. The equation of the magnitude and the phase is given by,

$$|S| = \left| \sum_{i=1}^{J} \frac{q_i(w - w_i)}{|(w - w_i)|^3} \right| \tag{3}$$

$$\Phi(a, b) = \frac{1}{2} arg \left(\sum_{i=1}^{J} \frac{q_i(w - w_i)}{|(w - w_i)|^3} \right) \tag{4}$$

where $w = a + ib$ is the position vector and $J = [q_1, q_2, \dots, q_j, w_1, w_2, \dots, w_j]$ is random keys that determine the value of the magnitude and the position of the electric charge. The transformation is given by,

$$A' = a + J\left|\vec{G}(a,b)\right| + J\cos(\Phi_F(a,b)) \quad (5)$$

$$B' = b + J\left|\vec{G}(a,b)\right| + Jsin\left(\Phi_F(a,b)\right) \quad (6)$$

$$\theta' = mod(\theta + \Phi_G(a,b) + \Phi_{rand}, 2\pi) \quad (7)$$

Figure 9 shows the process of the surface folding transformation function.

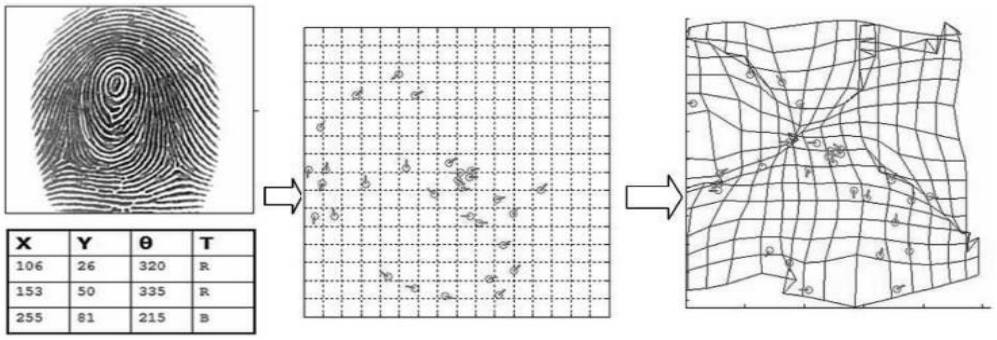


Figure 9: Surface folding approach where minutiae position and orientation is changed by randomly parameterized function (Ratha et al.)

Mesh warping is another non-invertible transformation method explained in (Uhl et al. 2009). There, a regular mesh grid is placed over the iris and the texture distortion is done by randomly displacing the vertices using a key.

2.1 Methods for Generating Cancelable Templates:

There are other methods to generate the cancelable biometric template proposed over the time. Here, we will briefly discuss the other methods.

(a) *Random Projection:* In this approach, the extracted features of the biometric pattern are projected into a random subspace (Pillai et al. 2010), (Pillai et al. 2011), (Teoh et al. 2007). If p is the extracted features in the feature space F^N such that $p \in F^N$, then the features are mapped to an arbitrary subspace R such that $R \in F^{n \times N}$ where $n < N$. If p' is a random projection vector, then the transformation can be given by the equation:

$$p' = Rp \quad (8)$$

Since, the feature vector of the higher dimensional space N is embedded into a lower dimensional space n, it is essential to maintain the distance between any two feature points in the output random feature vector.

In (Pillai et al. 2010), (Pillai et al. 2011) cancelable iris template is generated using random projection. During the segmentation process, some of the outliers remain due to eyelashes, specular reflection, etc. Therefore, applying a linear transformation on the entire feature vector might corrupt the biometric data. To solve this problem, sectored random projection is proposed in (Pillai et al. 2010). In the sectored random projection, the random projection is applied separately in each of the sectors and then the resulting vectors are combined to construct the transformed cancelable iris template.

(b) *Cancelable Biometric Filters*: In this method, the biometric template is encrypted using a user specific random convolution kernel. A randomly generated number is used as a seed to create the arbitrary convolution kernel, which is utilized as a PIN. The training images and the random

convolution kernel are convolved together to produce a Minimum Average Correlation Energy (MACE) filter. The generated encrypted biometric filter is saved to use during authentication (Savvides et al. 2004). When the stored biometric filter is lost or stolen, different encrypted biometric filters are synthesized using the different convolution kernel. The MACE filter is calculated using the following equation:

$$f = P^{-1}X(X^{+}P^{-1}X)^{-1}c \tag{9}$$

Here X is a $a \times b$ matrix where b is the total number of the training images, a is the number of pixels in each image. P is a $a \times a$ diagonal matrix comprising the "average power spectrum of all the training images". A column vector c with size $b \times 1$ contains the estimated correlation values. f is the resulting column vector which is reordered to generate the MACE filter. In (Takahashi et al. 2011) and (Hirata et al. 2009), correlation invariant biometric filter is used to generate cancelable biometric templates.

(c) *Biohashing:* In biohashing scheme, the extracted biometric features are combined with a tokenized random number to create the transformed template. Biohashing is the extended version of the Random Projection method (Teoh et al. 2007). The biometric features are extracted using wavelet and Fourier Transformation to generate the feature vector. Then, a user-specific number or token is randomly generated that is used to create orthogonal vectors. The cancelable template is spawned by finding the inner dot product of the feature vector and the orthogonal pseudo-random vector (Teoh et al. 2007), (Teoh et al. 2004). Mathematically, suppose f is a feature vector in the feature space $\mathrm{R^N}$ such that $\mathrm{f} \in \mathrm{R^N}$. Using the tokenized random number, k orthogonal vectors $\mathrm{a_i}$ is generated such that $\mathrm{a_i} \in \mathrm{R^N}$, $\mathrm{k} < \mathrm{N}$ and $\mathrm{i} = (1, 2, \ldots, \mathrm{k})$. After finding the dot product within the feature vector and the orthogonal vector, k bit Biohash template is generated by binary discretization. The equation to generate the biohash template is given by:

$$b = Sig\left(\sum_i f a_i - t\right) \tag{10}$$

where " $\mathrm{Sig}(.)$ is a Signum function" and t is the experimentally calculated threshold.

(d) *Permutation:* Random permutation of the features is another popular method for producing cancelable biometric templates. Here, the extracted features are randomly permutated seeded by some helper data. In (Ratha et al. 2001), the minutiae position of the fingerprint is permutated to different locations. If there are n minutiae points, d defines the direction of the minutiae points and the degree of freedom is L, then the possible ways to locate n minutiae in L location is:

$$\binom{L}{n} \tag{11}$$

And the number of ways to assign direction to the minutiae is $\mathrm{d^n}$. Therefore, possible number of minutiae combination is given by the equation:

$$\binom{L}{n} \times d^n \tag{12}$$

In (Zuo et al. 2008), the Gabor features extracted from the iris texture are shifted and the rows are combined to generate the transformed template. This approach is known as GRAY-COMBO. In another method BIN-COMBO, the iris code is randomly selected and combined (Zuo et al. 2008). In (Pillai et al. 2011), the features are divided into different sectors and then permutated randomly to store in a dictionary. In (Hammerle-Uhl et al. 2009), instead of permutation, remapping is done. The blocks of the target iris texture are drawn from the blocks the source texture.

(e) *Bioconvolving:* Bioconvolving method is applicable to any biometric pattern whose spatial, temporal, or spectral behaviour can be represented as a set of discrete sequence (Maiorana et al. 2010). For e.g., signature, handwriting, voice and gait. If the original biometric template is denoted by a set of sequences $\mathrm{s_i[m], i = 1, 2, \ldots, F}$, using Bioconvolving method, a set of transformed templates $\mathrm{t_i[m], i = 1, 2, \ldots, F}$ with length N can be generated. A number $(\mathrm{W} - 1)$ of different integer values $\mathrm{k_j}$ is randomly picked from 1 to 99 and arranged in a vector $\mathrm{k} = [\mathrm{k_0}, \ldots, \mathrm{k_W}]^{\mathrm{T}}$, $\mathrm{k_0} = 0$, $\mathrm{k_W} = 100$, in

increasing order such that $k_j > k_{j-1}$, $j = 1, 2, \ldots, W$. k is represented as a key to the transformation. Then, original biometric sequence $s_i(m)$ is split into W non-overlapping segments $s_{(i)j,M_j}(n)$ of length $M_j = a_j - a_{j-1}$

$$s_{(i)j,M_j}[m] = s_i[m + a_{j-1}], \qquad m = 1, 2, \ldots, M_j, \qquad j = 1, 2, \ldots, W \tag{13}$$

where,

$$a_j = \left\lfloor \frac{k_j}{100} M \right\rfloor, \qquad j = 1, 2, \ldots, W \tag{14}$$

The transformed sequence $t_i[m]$, $i = 1, 2, \ldots, K$ is obtained by the linear convolution of the portions of the original sequence $s_{(i)j,M_j}(m)$, $j = 1, 2, \ldots, W$. The equation for Bioconvolution is given as,

$$t_i[m] = s_{(i)1,M_1}[m] * \ldots * s_{(i)W,M_W}[m] \tag{15}$$

The generated transformed sequence is of length K where $K = M - W + 1$.

(f) Knowledge Signature: Knowledge signature is mostly used for group signatures, when one group tries to convince other group about their knowledge of certain values. It allows on group member to provide the knowledge signature on behalf of the group. In (Xu et al. 2008), voiceprint is used as a knowledge signature to generate cancelable voiceprints templates. The voiceprint of the user is acknowledged as the user's knowledge, and the signature of the knowledge is transferred to the template instead of the original features. Different signatures can be produced by altering the security parameters, but features remain the same.

(g) *Bloom Filters:* A Bloom filter, which is a data structure, estimates the cardinality of a set with high probability. A Bloom filter signifies a set that provides the support to membership queries. A bloom filter is space-efficient and provides fast processing of the queries (Rathgeb et al. 2014). In (Rathgeb et al. 2013), (Rathgeb et al. 2014) cancelable iris templates are generated using adaptive bloom filters. Suppose, bf is a bloom filter of length n. If bf is a simple bit array, then at the beginning all bits are assigned as 0. For representing a set $A = \{x_1, x_2, \ldots, x_m\}$, a bloom filter uses n dispersed hash functions $h_1, h_2, \ldots h_n$ in the range $[0, k-1]$. For each member $x \in A$, $h_i(x)$ of bloom filter bf is set to 1 such that $1 \leq i \leq n$. To test the membership of an element y in A, it is checked whether all bits $h_i(y)$ in bf are set to 1 or not. If all values are 1, then y is a member of A. To generate the transformed iris template, the iris code is equally distributed into B blocks. Each block, containing j bits, are transformed according to the location within the bloom filter. That means, using B number of the bloom filters of length 2^w, the total no of transformed templates generated will be $K.2^w$.

(h) Hybrid Techniques: In hybrid approach, the cryptosystem and the cancelable biometrics is merged to generate transformed templates. In (Boult et al. 2006), Biotokens are proposed for face biometrics. Biotokens or Biotopes provides a public key to support an invertible mapping of the biometric template. Moreover, it also supports a robust distance metric that maintains the distance between the intra-class subjects and inter-class subjects. The transformation is done in the features space based on the biometric signature. In (Boult et al. 2007), a similar approach has been used for fingerprint.

The different schemes of cancelable biometrics either work with the already existing matcher or need a special matcher to calculate the similarity scores. Again, some of the schemes require the training samples to be registered before applying the transformation function. On the other hand, some schemes are registration free. Those methods can be further distributed into the two groups. In one approach, the transformation is done in the raw biometric template i.e. signal domain. In the other approach, the transformation is done on the extracted features of the biometric data (Patel et al. 2015). Figure 10 shows the different categories of the cancelable biometric and examples of the schemes falling under those categories.

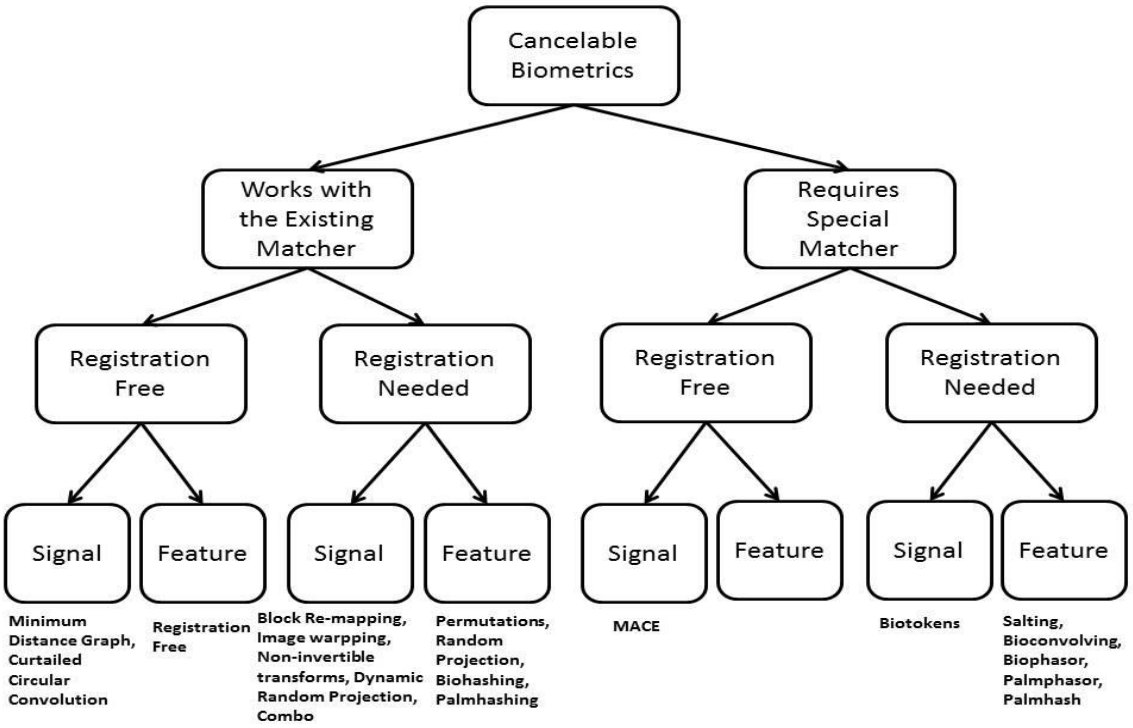


Fig. 10. Different Categories of Cancelable Biometric schemes and some of the Examples (Patel et al. 2015).

6. STATE-OF-THE-ART: CANCELABLE BIOMETRICS

Many research works have been done in the field of template protection of different biometric modalities. Among all biometric modalities fingerprints, iris and face models are popular for the biometric authentication system.

N. K. Ratha et al. in 2007, provided the concept of cancelable biometrics for fingerprint template. They provided three transformation functions, viz. Cartesian, Polar and Surface Folding transformation for minutiae based fingerprint template. However, the Cartesian and Polar transformation degrades the performance when the minutiae intersect the boundaries. Then, they provided surface folding function as a solution to the problem of smallest translation by modelling the direction of the translation. So, compared to other two transformation functions, the surface folding method provides better security as well as accuracy. But, it has been proved that the surface folding process can be attacked by record multiplicity.

P. P. Paul et al. in 2012, proposed cancelable biometric template generation for multimodal biometrics system (Face and Ear) using random projection. They divided the proposed cancelable biometric scheme into three parts. First, the transformation is done using Two Fold Random projection. Then, the transformed features are projected by Principal Components (PCs) and two fold features are merged by k-means clustering. Lastly, the interclass variability is enhanced using Linear Discriminant Analysis (LDA). k-NN classifier is used for classification. They concluded that their cancelable multimodal biometrics system performs better than the unimodal biometric system.

P. Lacharme et al. in 2011, provided a pin-based cancelable biometrics for fingerprint template. They comprehended a biometric authentication with a secret, i.e. a PIN code or different kinds of passwords only known by the user. This technique attains a 0-FAR and a 0-EER. But since it is user dependent PIN based method, the vulnerability of the system is high.

E. Y. Du et al. in 2011, provided a key integration method for cancelable biometrics. They fabricated the Gabor Descriptor for generating cancelable iris template by implementing the proposed key incorporation Scheme. They used partial key information in the feature extraction step so that it can be used in later stages and thereby it will increase the recognition capacity. They implemented this scheme practically in the Iris recognition system. The achieved EER is approximately 0.22%.

A.B.J. Teoh et al. in 2007 undertook a formal statistical analysis of the BioHash scheme for cancelable biometrics in terms of the ensemble of the quantized Random Projections. They applied their method for the face biometrics. In their methods, firstly, the raw biometric pattern is transformed into a feature space having a low-dimension. Then, the user-specific feature vector is re-projected

onto a series of random subspaces which is indicated by the tokenized random vectors. At last, these projections are quantized to generate the binary bit string. They also demonstrated the usage of multi-state BioHash to find the solution for the stolen-token problem.

J. Zuo et al. in 2008 provided biometric salting and non-invertible template protection scheme for iris. For non-invertible cancelable biometrics, they proposed two methods: “GRAY-COMBO and BIN-COMBO”. In the GRAY-COMBO method, the rows of the normalized iris image are shifted and combined. In BIN-COMBO method, row combination is replaced by XOR or XNOR function. They again provided two salting methods: GRAY-SALT and BIN-SALT. In salting approach, they added random noise to create the transformed iris image. They gained FAR of 0% and FRR of 0.005% with increased performance rate for the non-invertible approach. For salting approaches they achieved FRR of 0.005% and FAR of <10-3. The problem with the non-invertible methods is that due to shifting and combing the amount of valid iris region decreases. In case of BIN-SALT and GRAY-SALT, it is tough to determine the comparative strength of the noise patterns to be combined.

J. K. Pillai et al. in 2010, provided sectored random projection for cancelable iris biometrics. Their method has two steps: feature extraction and random projection. A feature vector is formed by the Gabor features extracted during the feature extraction. Then, it is randomly projected onto a subspace of lower dimension using an arbitrary matrix. They have achieved high recognition rate of 97.7%.

J. H. Uhl et al. in 2009, used “block re-mapping and image warping” for achieving cancelable iris biometrics. They followed Ma et al. algorithm for constructing iris texture or bit code. Then they used a key to construct the transformed template. In the block re-mapping method, every block of the source texture is mapped to one of the target texture’s block. In the next transformation, they employed a mesh warping to distort the texture. In this method the iris pattern is re-mapped in accordance with the distorted grid mesh placed over it. They achieved EER of 1.2% and 1.3% using block re-mapping and image warping respectively. Both of these approaches degraded the performance. Moreover, if an attacker gets access to the parameters of the transformations, then it is possible to reconstruct an iris pattern that is the closest approximation of the original template to pass the valid threshold.

E. Maiorana et al. in 2010, provided Bioconvolving method to generate cancelable template for online signature. They considered that the signature can be represented a set of sequence. The original biometric pattern is characterised as discrete sequence. From the original sequence, a set of sequence is extracted. Shifting and convolution are done among the extracted sequences to generate a variety of cancelable templates. They used a Hidden Markov Model (HMM) to calculate the matching score. They achieved EER of 6.33%. However, their method slightly degrades the system performance.

C. Rathgeb et al. in 2014, used an adaptive Bloom filter to gain cancelability for iris biometrics. They applied an adaptive Bloom filter to the binary iris feature vector in order to obtain rotation invariant transformed iris code. The Bloom filter enables biometric template protection, biometric data compression and speeding up of biometric identification. They gained EER of 1.49% using 1-D Log Gabor feature extraction and EER of 1.14% using Ma et al. feature extraction.

J. H. Uhl et al. in 2013, used two variants of key-dependent wavelet and a combination thereof in the feature extraction stage. They used parameterized wavelets and wavelet packets for gaining cancelability. Using wavelet packets, they obtained EER of 0.4%. Using quadratic spline wavelet is 0.42%. The problem with their scheme is that the extracted iris code is highly sensitive towards slight change in the key parameter especially in case of wavelet packets.

Z. Jin et al. in 2014, provided a template protection method to protect the minutiae of the fingerprint using Randomized Graph-based Hamming Embedding (RGHE). Their method adopted Minutiae Vicinity Decomposition (MVD) together with the random projection to develop a set of randomly invariable geometrical features. The discrimination of randomized MVD is then enhanced by User specific Minutiae Vicinities Collection scheme and embedded into a Hamming space through Graph-based Hamming Embedding. They gained EER of 1.77%.

Y. Sui et al. in 2014, introduced a hybrid scheme. Here, a Reference Subject is combined with the user’s biometric template to generate a revocable BioCapsule. The Reference Subject can be either physical object or logical object such as a biometric image kept in the server. The Reference Object is generated using a key extracted from the user’s biometric template. They achieved EER 0.94% for ICE database, 0.61% for CASIA v1.0 dataset.

R. Dwivedi et al. in 2015, provided a method for cancelable iris biometric using randomized look up table mapping of decimal vector generated by the Log Gabor filter. The generated row vector of iris features are partitioned into fixed length words, then mapped to a decimal vector. It is possible to map multiple numbers of words to a same positive number. The transformed template is generated by selecting any no of bits (less than the number of bits in the fixed length word) from every single row of the look-up table.

W. Wong et al. in 2013, provided minutiae based cancelable biometric scheme for fingerprints. Here, several single line codes designed by the minutiae of the fingerprint are combined to generate multi-line codes. Generated multi-line codes are the representation of the transformed template. The method addressed the alignment invariance of the templates also. They obtained EER of 4.69% for FVC2002 DB1 database in the stolen token scenario. However, they used a user specific key to seed the permutation of the lines of code which itself can be compromised. Moreover, it requires a large storage capacity as the templates are stored in real values.

N. Nishiuchi et al. in 2011, provided a cancelable biometric scheme that involves a combination of external artifacts to the biometric data. Here, an external artifact, i.e. a sticker, is attached to the fingernail of thumb or forefinger. During the enrollment process, a user register with the sticker on the fingernail and the template is generated by considering the outline of the finger and the position of the sticker. Therefore, every time the user has to wear the sticker for identification. The scheme is cancelable in the sense that the all the information registered previously, can be aborted by pulling out the artifact. Although, the permissible range of location and angle of the artifact are verified, the system is cumbersome. Moreover, limited number of users can use this system and the time span of usage is limited to five days only.

M. Butt et al. in 2014, used Bloom filter for the cancelable face template. The stable features of the face are taken as helper data to generate the transformed template. After feature extraction, the position of the stable feature (bits) is passed through the bloom filter using a user PIN. The generated bloom filter is the desired transformed template for the face biometric. However, their scheme degraded the system performance.

S. Nazari et al. in 2014, provided a new version of Biohashing using Chaos map. They used a Chaos map to permutated the feature vector and then applied Biohashing scheme on the new feature vector to generate the transformed template. They claimed that the intruder cannot reconstruct the original template even if the transformed parameters are compromised.

O. Ouda et al. in 2010, provided a tokenless scheme for securing the iris template. They extracted the most stable bits of iris from the feature vector, and then mapped those bits randomly to a different set of bits to generate the protected BioCode. They achieved the EER of 2.30% without degrading the system performance.

M. Savvides et al. in 2004, proposed the biometric filters to generate cancelable templates for face biometrics. A random convolution kernel produced by a Personal Identification Number (PIN) is convolved with the training images. Then, a Minimum Average Correlation Energy (MACE) filter is synthesized from those convolved training images. They achieved 100% recognition rate.

S. Wang et al. in 2014, provided an alignment free cancelable biometric scheme for fingerprints. They used curtailed circular convolution to generate the transformed template. First, fingerprint images are registered according to the singular points. Then, curtailed convolution is applied by multiplying Discrete Fourier Transformation (DFT) of two series. They performed their experiment on the “DB1, DB2 and DB3 of FVC2002” database and achieved EER of 2%, 3% and 6.12% respectively.

Some of the significant work done on cancelable biometrics and their comparison in terms of performance and limitations are summarized in the Table III.

7. SECURITY ATTACKS ON CANCELABLE BIOMETRICS

The template protections schemes are developed for enhancing the security of the biometric templates. However, these template protection schemes are also vulnerable to security threats. The adversaries are working on finding new ways to counterfeit these secured schemes. The cancelable biometrics is not free from such security threats. Here, we will discuss about the possible security attack on the cancelable biometrics.

7.1 FAR Attack

In all biometric systems, the decision is made by giving a positive or negative response by comparing the similarity scores of the extracted features. The evaluation of the biometric system is done with respect to the “False Acceptance Rate (FAR), False Reject Rate (FRR) and Equal Error Rate (EER)”. Depending on the intra-class variation or interclass correlation false acceptance and false reject might occur. Now, even if the FAR is 0.01%, there is a chance to find 2 identical templates for 104 trials of comparison. That means, if the intruders have access to a large database of biometric templates, then they can exploit the false acceptance error. Moreover, we know that biometric modalities can be physiological or behavioural. Most of the times twins have identical biometrics features like face, fingerprint, etc. Those genotypic biometric traits can be used as FAR attack against the biometric system and cancelable biometrics schemes as well (Zhou et al. 2009).

Table III. Summary of the state-of-the-art of Cancelable Biometric systems

Authors	Year	Modality	Method Adopted	Performance	Limitations
Ratha et al.	2007	Fingerprint	Non-invertible geometric transformation	15/10-4	Degrades performance, Record multiplicity attack
Lacharme et al.	2011	Fingerprint	PIN based	0 EER	User dependent
Teoh et al.	2006	Face	Random Projection	2.10-3 EER	User dependent
Teoh et al.	2004	Fingerprint	Biohashing	0 EER	User dependent
			Random Permutation	0.005/0 Increases performance, Alignment free	Decrease in the valid iris region
			Random Noise	0.005/<10-3 Increase performance	Difficult to decide strength of noise
Pillai et. al	2010	Iris	Random Projection	2.3 EER	Less secure
Savvides et al.	2004	Face	Biometric Filters	100 RR	Degrades performance
H. Uhl et al.	2009	Iris	Image Wrapping	1.3 EER	Degrades performance, reconstruction is possible
			Block Re-mapping	1.2 EER	
E. Maiorana et al.	2010	On-line Signature	Bioconvolving	6.33 EER	Degrades performance
Rathgeb et al.	2014	Iris	Adaptive Bloom Filter	<0.5 EER Alignment free	Reconstruction is possible
Uhl et al.	2013	Iris	Key Incorporation	0.22 EER	Highly Unstable to slight changes
Jin et al.	2014	Fingerprint	Non-invertible geometric transformation	1.77 EER	Degrades performance
Dwivedi et al.	2015	Iris	Log Gabor Filter	5.75 EER	Less Secure
Ouda et al.	2010	Iris	Permutation	1.33 EER	Record Multiplicity Attack
Teoh et al.	2006	Fingerprint	Biophasor	5.31 EER	User dependent
Boult et al.	2006	Face	Bio-tokens	~0.08 EER	User dependent
Connie et al.	2005	Palmprint	Palmhashing	0 EER	User dependent
Das et al.	2012	Fingerprint	Minimum Distance Graph	2.27 EER Alignment free	–
Wang et al.	2014	Fingerprint	Curtailed Circular Convolution	2 EER	User dependent

7.2 Linkage Attacks

To avoid the cross matching of the same biometric templates used in different applications, cancelable biometrics scheme is designed in such a way that each generated transformed templates are different from each other. However, in case of biometric salting process, helper data, i.e. the user specific information are used to generate the transformed templates. The feature sets to generate the transformed templates can be limited. The selections of the most reliable bits are dependent on the statistical attributes of the individuals (Zhou et al. 2009). So, it is more likely to be found a correlation between different transformed templates used in different applications. The adversary can exploit such correlation of the features to generate an approximation of the original template. In (Bringer et al. 2014), it is explained how the inner correlation of the different transformed iris templates generated by permutation of the bits, can be exploited to design a countermeasure.

7.3 Hill Climbing Attacks

In the cancelable biometric, the matching score is provided to give a decision. That matching score reveals about the amount of similarity between the stored template and the query template (Adler 2004). Using that knowledge, an intruder can regenerate the original biometric data (Hill 2001). The

Hill climbing attack optimizes the searching process to make it efficient. In hill climbing attack, the intruder starts with an initial biometric template. Then, the template is modified and then compared with the target biometric template. The template is modified recursively until they find a good matching score with the target biometric template. Since, the comparison scores can be overwritten (Ratha et al. 2001), the intruder can perform hill climbing attack for both biometric slating and non-invertible transformation. Hill climbing attack is performed against block remapping process in (Quan et al. 2008) and surface folding process in (Shin et al. 2009).

7.4 Substitution Attacks

In this type of attack, the impostor intercepts the feature module and replaces the transformed feature set with his/her own feature set (Rathgeb et al. 2011). Using a substitute template the adversary can make it accepted by the biometric system. In case of salting process, if the intruder has the access to the user specific key, it becomes easier to execute substitution attack. In the similar way, if the transformed parameter is known to the intruder, it is feasible to attack non-invertible transformation schemes as well.

7.5 Attack via Record Multiplicity

If the adversary has the access to multiple number of different transformed templates, it is possible to find the correlation between those transformed templates. Therefore, it is viable to generate the original biometric template from the existing correlation among multiple templates. Attack via record multiplicity assumes that the all the information about the transformed parameters and the transformation methods are stored in the database along with the transformed templates (Li and Hu 2014). For e.g. the cancelable biometric schemes in (Ratha et al. 2007), (Ouda et al. 2010) are vulnerable to the record multiplicity attack. Again in (Li and Hu 2014), it is experimentally shown that the methods provided for cancelable fingerprint in (Wang et al. 2012), (Lee et al. 2007), (Ahmad et al. 2011), (Yang et al. 2009) are vulnerable to attack via record multiplicity and the original biometric template can be reconstructed. In (Jenisch and Uhl 2011), it has shown the vulnerability of the block re-mapping process against attack via record multiplicity.

7.6 Masquerade Attacks

In this attack, a master biometric template is compromised to analyse and produce an artefact having the similar features as the master template (Hill 2001). If the intruder can get the access to different transformed templates, after a hill climbing attack, masquerade attack can be performed to hack the biometric system. In salting approach, if the process is invertible, then using masquerade attack the original template can be reconstructed. In (Hill 2001) it is explained how masquerade attack exposes the structure of the fingerprint by using the minutiae template only.

7.7 Overwriting Final Decision

Similar to the conventional biometric system, a biometric system with the cancelable biometric schemes is also vulnerable to this attack. Since, the matching score provided in the final decision can be overwritten (Ratha et al. 2001), the cancelable biometric scheme also fails to avoid this attack.

7.8 Stolen Token

In case of biometric salting, user-specific helper data are being used to create the transformed template. Since, the token is possessed by the user; it is easier for the intruder to compromise the token by stealing it (Kong et al. 2006). Therefore, evaluation of the biometric salting process is always done in a stolen token scenario.

Table IV shows the different possible attacks on the biometric salting and non-invertible transformation scheme of the cancelable biometrics.

8. ADVANTAGES AND OPEN PROBLEMS OF CANCELABLE BIOMETRICS

There are some significant advantages of cancelable biometrics over the traditional biometric systems and few of them are listed as follows:

(1) The main advantage is that the biometric templates can be replaced just like a password and token once lost or stolen.

Table IV. Security Attacks on Cancelable Biometrics

Cancelable Biometrics	Possible Security Attacks
Biometric salting	Substitution attack, Attack via record multiplicity, Linkage attack, FAR attack, Masquerade attack, Hill climbing attack, Overwriting final decision, Stolen token
Non-invertible transformation	Substitution attack, Attack via record multiplicity, Linkage attack, Hill climbing attack, Overwriting final decision

(2) Even if the biometric template has been lost or compromised, it is challenging for the intruders to reconstruct the original pattern from the transformed one.
(3) Using one original template several unique transformed templates can be generated to use for different applications. Therefore, it is not required for the users to provide their biometric trait for enrolment on different applications.
(4) It might increase the social acceptance of biometric applications since users need not to worry about their biometric trait being stored.
(5) It can prevent attacks on the database against the biometric applications.

The cancelable biometrics schemes are supposed to be designed in such a manner that it is not possible to retain the original biometric pattern from the distorted one. It should take care of the system performance as well. Because when a transformed template is used to store and match, the possibility of reducing the system's recognition rate gets higher. The two methods, salting and non-invertible transformation, have their own issues. If biometric salting provides better performance, then it is also less secure. While non-invertible transformation provides better security by transforming the biometric templates using one-way function such that there is almost zero possibility of reconstructing the original biometrics. But, this also raises the false acceptance rate of the system (Nandakumar and Jain 2015). Some of the listed problems/disadvantages that exist in the cancelable biometrics are (Nandakumar and Jain 2015):

(a) Finding an appropriate transformation function for cancelable biometrics is a complicated task. Standard non-invertible transformation functions do not operate properly with biometric data because of the intra class variability of the biometric pattern. Hence, in most of the cases, transformation is reliant on the user, i.e., the user either has to memorize a password/pin or to bring the transformation parameter stored in the form of a token.
(b) There is no standard parameter to check the security strength regarding the non-invertibility of the method. Therefore, it is hard to perform security analysis, particularly when the algorithm for the transformation and associated keys/parameters are negotiated as well. In (Nagar et al. 2010), provided six measures to estimate the security strength of the template protection schemes.
(c) The claim that non-invertible transformation doesn't allow reconstruction of original biometrics, even the key or transformation parameter is known, is somehow an assumption. In Record Multiplicity attack, the invader can reconstruct the original biometric template by interlinking multiple copies of the transformed templates.
(d) One fundamental challenge signifies the problem of alignment, which considerably affects the recognition performance. The biometric templates are concealed when template protection methods are used and, so, the alignment of these secured templates is extremely inconsistent. To keep the proper alignment of the training image and the query image during the matching process, it is required to register the training images. Very few schemes are alignment-free without any pre-registration of the biometric data.
(e) Most of the existing cancelable biometric schemes are tested on a mid or small-scale database. To evaluate the impact and the practicality of those schemes, it is necessary to test those methods on large-scale database of the biometric samples.

9. A NOVEL METHOD FOR CANCELABLE IRIS BIOMETRICS

We have proposed a novel method for cancelable biometrics in this section. We have presented a non-invertible transformation function using the concept of Steganography. The combination of

Discrete Cosine Transformation (DCT) and Huffman encoding is a non-invertible transformation used in Steganography. Steganography is a covert communication, where the secret image/message is communicated through an unsuspicious cover image. For secret communication, the secret image is hidden by embedding in the Least Significant Bits (LSBs) of each pixel in the cover image. Only the intended receiver can extract the secret image from the cover image using the secret key or algorithm (Abbas Cheddad et al. 2010). When the combination of DCT and Huffman encoding is used, the Huffman encoded bit stream of the secret image is embedded in the LSBs of DCT coefficients of the cover image (Nag et al. 2010). During the process, most of the cover image's pixel values are destroyed. Again, after extraction of the secret image also, it is not possible to get the exact same cover image (Das et al. 2013). Therefore, we have used this concept to form the transformed iris template.

The Discrete Cosine Transformation (DCT) converts an image from the spatial domain to the frequency domain by subdividing the image into 8×8 blocks. In each block 64 DCT coefficients are generated. The most of the energy in the form of lower frequencies are stored in the upper left corner of the DCT matrix. The 2-dimensional DCT transforms an image $\mathrm{f(i,j)}$ into the frequency domain $\mathrm{F(u,v)}$ by an equation given as,

$$F(u,v) = \alpha_u \alpha_v \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f(i,j) \cos\left[\frac{\pi u(2i+1)}{2M}\right] \cos\left[\frac{\pi v(2j+1)}{2N}\right] \quad (16)$$

Where,

$$1 \le u \le M-1 \ , 1 \le v \le N-1$$

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}} , & u = 0 \\ \sqrt{\frac{2}{M}} , & 1 \le u \le M-1 \end{cases} \qquad \alpha_v = \begin{cases} \frac{1}{\sqrt{N}} , & v = 0 \\ \sqrt{\frac{2}{N}} , & 1 \le v \le N-1 \end{cases}$$

Again, the Huffman encoding is a lossless image compression technique that represents the data or image pixels by a minimum possible bit stream.

In the proposed cancelable biometrics scheme, the Huffman encoding of a secret image (Here we used the eye image itself) is embedded in the DCT coefficients of the iris template. First, consider a set of secret images. Then, randomly select an image and find the Huffman encoded bit stream. After that, apply DCT on the iris image and embed the Huffman encoded bit stream in the LSBs of the DCT coefficients. After performing the Inverse Discrete Cosine Transformation (IDCT), we get the transformed iris template. Fig. 11 shows the block diagram of the proposed method. The algorithm for generating the cancelable iris template is as follows:

Algorithm:
Input: Unwrapped iris image of size $M \times N$ and selected secret image of size $m \times n$
Output: Transformed template.

Step 1: Read the unwrapped iris image of size $M \times N$.
Step 2: Convert the cover image, i.e. unwrapped iris image into the DOUBLE format.
Step 3: Divide the cover image into 8×8 block and apply 2D DCT on each block of the unwrapped iris image.
Step 4: Find the minimum value of the DCT coefficients and subtract the minimum value from all the DCT coefficients to convert the negative values into positive values.
Step 5: Convert the modified DCT coefficients into UINT32 format to remove the fractional part.
Step 6: Resize the selected secret image (original eye image) to $m \times n$ such that $m \le \mathrm{M}$ and $n \le \mathrm{N}$.
Step 7: Generate Huffman Table from the intensity values of the selected secret image.
Step 8: Create Huffman encoded bit stream of the secret image using the Huffman table.
Step 9: Compute the size of the encoded bit stream in bits.
Step 10: Convert the encoded bit stream of the secret image into a 1-D block of size 8 bits.
Step 11: Embed each bit computed in Step 7 in the first 8x8 block of the unwrapped iris image by

changing the LSBs of the modified DCT coefficients computed in Step 5.

Step 12: Embed the Huffman table and the Huffman encoded bit stream of 8 bit block generated in Step 8 by altering the LSBs of the modified DCT coefficients in each block (excluding the first 8x8 block) of the unwrapped iris image.

Step 13: Add the minimum value to the modified DCT coefficients generated in Step 12.

Step 14: Apply Inverse DCT (IDCT).

Step 15: Convert image into UINT8 format to generate the transformed template.

The different transformed templates can be generated by embedding different secret images for each transformation. The generated transformed templates will satisfy the criteria of unlinkability as each of them will be unique.

After generation of the transformed template the features are extracted by applying 2-D Discrete Wavelet (DWT). Using Haar wavelet, the transformed template is decomposed up to 4 levels to get the Approximation, Horizontal, Vertical and Diagonal Details. The Diagonal details are considered as these coefficients providing the high-frequency components. A feature vector of size 1×96 is generated by including all the diagonal details of the 4th level and average values of the diagonal coefficients of the other 3 levels. Then, the positive values are assigned as 1 and negative values are assigned as 0 to generate a binary feature vector of 96 bits. The matching score between the query and stored template is calculated by Hamming distance. Based on a calculated threshold, the genuine users are authenticated. We tested the scheme on the 250 images of CASIA v.4 Interval dataset. We considered 50 users and then the method is evaluated by taking one user's template and considering others as imposters. The proposed method is giving promising results. Fig. 12 shows a normalized eye image. Fig. 13(a) show the secret eye image, Fig. 13(b) shows the generated transformed iris template. The Recognition Rate (RR) is 98.8%, Equal Error Rate is (EER) is 1.2%. Fig. 14 shows the ROC curve between Genuine Acceptance Rate (GAR) and False Acceptance Rate (FAR).

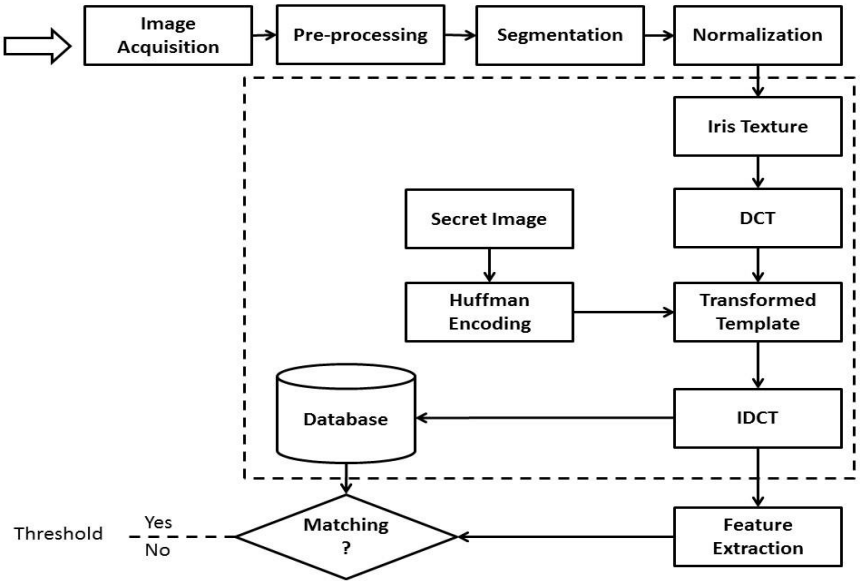


Fig. 11. Flow Diagram of the Proposed Cancelable Biometrics Scheme

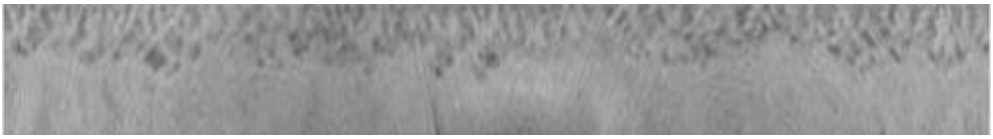
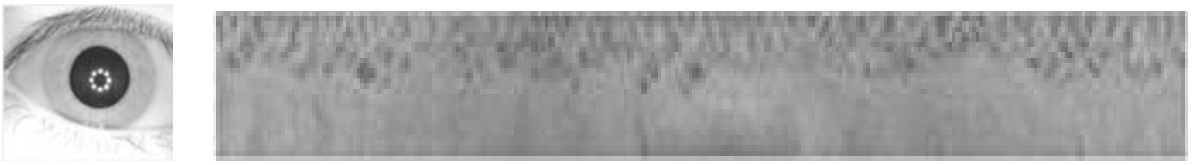


Fig. 12. Normalized Eye Image



(a) (b)

Fig. 13. (a) Secret Eye Image, (b) Transformed Iris Template

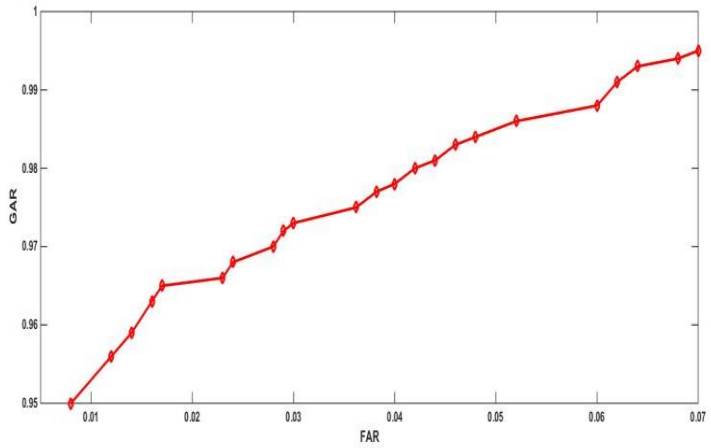


Fig. 14. ROC curve

The Table V shows the comparison of different cancelable biometrics and the proposed method. From the table, we can see that the proposed method is performing better than some of the existing methods. Therefore, it can be one of the potential methods for generating transformed templates. However, further experiments regarding the uniqueness and unlinkability are yet to be done.

Table V. Equal Error Rate (EER) of different cancelable biometrics

Cancelable Biometric Schemes	Equal Error Rate (%)
Pillai et al. (44)	2.33
Uhl et al.(49)	1.33
Dwivedi (62)	5.75
Proposed Method	1.2

10. CONCLUSION

In this extensive survey, we have discussed about popular and emerging biometric traits along with their security issues. The futuristic technique like cancelable biometrics has shown the potential to boost the security and confidentiality of a traditional biometric system. However, there are not so extensive uses of cancelable biometric systems in real life scenarios as compared to the traditional one. The researchers are working on new approaches for making cancelable biometrics less complex, yet secured, without degrading the recognition performance of the overall biometric system. In this paper, we have reviewed most of the traditional biometric systems, their performances, along with their security and privacy issues, which leads us to the potential cancelable biometric-based systems. We have also reviewed some of the state-of-the-art literature of cancelable biometrics and compared their performances and highlighted the main pros and cons of cancelable biometrics. This article can be used as basic information about traditional and cancelable biometrics, which we hope will help researchers and students to get encouraged to further research and build a practical cancelable

biometric-based application to overcome the standard security and privacy issues of traditional biometric systems.

REFERENCES

1. Gursimarpreet Kaur, Chander Kant Verma. 2014. Comparative Analysis of Biometric Modalities, International Journal of Advanced Research in Computer Science and Software Engineering, 4(4), (2014), 603-613.
2. Sushma Jaiswal, Sarita Singh Bhadauria, Rakesh Singh Jadon. 2011. Biometric: Case Study, Journal of Global Research in Computer Science, 2(10), (2011), 19-49.
3. Georgios Goudelis, Anastasios Tefas, Ioannis Pitas. 2008. Emerging Biometric Modalities: A Survey, Journal on Multimodal User Interfaces, 2, (2008), 217- 235. DOI: http://dx.doi.org/ 10.1007/s12193-009-0020-x
4. W. Zhao, R. Chellappa, P. J. Phillips, A. Rosenfeld. 2003. Face recognition: A Literature Survey, ACM Computing Surveys, 35(4), (2003), 399-458. DOI: http://dx.doi.org/ 10.1145/954339.954342
5. Ayman Abaza, Arun Ross, Christina Hebert, Marry Ann F. Harrison, Mark S. Nixon. 2013. A Survey on Ear Biometrics, ACM Computing Surveys, 45(2), (2013), Article No 2. DOI: http://dx.doi.org/ 10.1145/2431211.2431221
6. Bilge Suheyla. Akkoca, Muhittin Gokmen. 2015. Automatic Smile Recognition from Faces. In: 23rd Conference on Signal Processing and Communications Applications, Malatya, May, 2015, pp. 1985 – 1988.
7. DOI:http://dx.doi.org/10.1109/SIU.2015.7130253
8. Haitham Hasan, S. Abdul Kareem. 2013. Fingerprint Image Enhancement and Recognition Algorithms: A Survey. Neural Computing and Application, 23(6), (2013), 1605-1610. DOI: http://dx.doi.org /10.1007/s00521-012-1113-0
9. Santiago Gonzalez, Carlos M. Travieso, Jesus B. Alonso, Miguel A. Ferrer, 2003. Automatic Biometric Identification System by Hand Geometry. In: IEEE 37th Annual International Carnahan Conference on Security Technology, October, 2003, pp. 281 – 284. DOI: http://dx.doi.org/10.1109/CCST.2003.1297573
10. Shoichiro Aoyama, Koichi Ito, Takafumi Aoki. 2014. A Finger-Knuckle-Print Recognition Algorithm using Phase-based Local Block Matching, ELSEVIER journal on Information Sciences, 268, (2014), 53-64. DOI:http://dx.doi.org/ 10.1016/j.ins.2013.08.025
11. Adams Kong, David Zhang, Mohamed Kamel. 2009. A Survey of Palmprint Recognition, ELSEVIER journal on Pattern Recognition, 42(7), (2009), 1408–1418. DOI: http://dx.doi.org/ 10.1016/j.patcog.2009.01.018
12. Amioy Kumar, Shruti Garg, M. Hanmandlu. 2014. Biometric Authentication using Finger Nail Plates, ELSEVIER journal on Expert Systems with Applications, 41(2), (2014), 373–386. DOI: http://dx.doi.org/ 10.1016/j.eswa.2013.07.057
13. Kevin W. Bowyer, Karen Hollingsworth, Patrick J. Flynn. 2008. Image Understanding for Iris Biometrics: A Survey, ELSEVIER journal on Computer Vision and Image Understanding, 110(2), (2008), 281–307. DOI: http://dx.doi.org/ 10.1016/j.cviu.2007.08.005
14. Halvor Borgen, Patrick Bours, Stephen D. Wolthusen. 2008, Visible-Spectrum Biometric Retina Recognition. In: International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, August, 2008, 1056 – 1062. DOI: http://dx.doi.org/10.1109/IIH-MSP.2008.345
15. Rejean Plamondon, Sargur N. Srihari. 2000. Online and Off-line Handwriting Recognition: A Comprehensive survey, IEEE Transactions on Pattern Analysis and Machine Intelligence, 22(1), (2000), 63 – 84. DOI: http://dx.doi.org/10.1109/34.824821
16. Marcos Faundez Zanuy. 2007. On-line signature recognition based on VQ-DTW, ELSEVIER Journal on Pattern Recognition, 40(3), (2007), 981–992. DOI: http://dx.doi.org/10.1016/j.patcog.2006.06.007
17. Fabian Monrose, Aviel D. Rubin. 2000. Keystroke Dynamics as a Biometric for Authentication, ELSEVIER Journal on Future Generation Computer Systems, 16(4), (2000), 351–359. DOI: http://dx.doi.org/10.1016/S0167-739X(99)00059-X
18. Takuya Yoshioka, Armen Sehr, Marc Delcroix, Keisuke Kinoshita. 2012. Survey on Approaches to Speech Recognition in Reverberant Environments. In: Asia-Pacific Signal & Information Processing Association Annual Summit and Conference (APSIPA ASC), Hollywood, December, 2012, pp. 1 – 4.
19. Ling Feng Liu, Wei Jia, Yi-Hai Zhu. 2009. Survey on Gait Recognition, Springer Lecture Notes in Computer Science, 5755, (2009), 652-659. DOI:http://dx.doi.org/10.1007/978-3-642-04020-7_70
20. Anil Kumar Jain, Arun Ross, Salil Prabhakar. 2004. An Introduction to Biometric Recognition, IEEE Transactions on Circuits and Systems for Video Technology, 14(1), (2004), 4-20. DOI: http://dx.doi.org /10.1109/TCSVT.2003.818349
21. G. Zayaraz, V. Vijayalakshmi, D. Jagadiswary. 2009. Securing Biometric Authentication using DNA Sequence and Naccache Stern Knapsack Cryptosystem. In: International Conference on Control, Automation, Communication and Energy Conservation, Perundurai, Tamilnadu, June, 2009, 1 – 4.
22. W. Khalifa, A. Salem, M. Roushdy, K. Revett. 2012. A Survey of EEG based User Authentication Schemes. In: 8th International Conference on Informatics and Systems, Cairo, May, 2012, pp. 55-60.
23. Qiong Gui, Zhanpeng Jin, Wenyao Xu. 2014. Exploring EEG-based Biometrics for User Identification and Authentication. In: IEEE Signal Processing in Medicine and Biology Symposium, Philadelphia, PA, December, 2014, pp. 1 – 6. DOI: http://dx.doi.org/10.1109/SPMB.2014.7002950
24. Ikenna Odinaka, Po-Hsiang Lai, Alan D. Kaplan, Joseph A. O'Sullivan, Erik J. Sirevaag, John W. Rohrbaugh. 2012. ECG Biometric Recognition: A Comparative Analysis. IEEE Transactions on Information Forensics and Security, 7(6), (2012), 1812 – 1824. DOI: http://dx.doi.org/10.1109/TIFS.2012.2215324
25. Mingley Shu, Yunxiang Liu, Hua Fang. 2014. Identification Authentication Scheme using Human Body Odour. In: Proceeding of IEEE International Conference on Control Science and Systems Engineering, Yantai, December, 2014, pp. 171 – 174. DOI: http://dx.doi.org/10.1109/CCSSE.2014.7224531
26. Francine J. Prokoski, Robert B. Riedel, Jeffrey. S. Coffin. 1992. Identification of Individuals by Means of Facial Thermography. In: Proceeding of International Carnahan Conference on Security Technology, Atlanta, October, 1992, pp. 120 – 125. DOI: http://dx.doi.org/10.1109/CCST.1992.253768
27. Madasu Hanmandlu, Shantaram Vasikarla. 2012. Online Biometric Authentication using Facial Thermograms. IEEE Applied Imagery Pattern Recognition Workshop, Washington, DC, October, 2012, pp. 1 – 6. DOI:http://dx.doi.org/10.1109/AIPR.2012.6528223
28. Aycan Yuksel, Lale Akarun, Bulent Sankur. 2012. Biometric Identification through Hand Vein Patterns. In: International Workshop on Emerging Techniques and Challenges for Hand-Based Biometrics, Istanbul, August, 2010, pp. 1-6. DOI: http://dx.doi.org/10.1109/ETCHB.2010.5559295
29. Kresimir Delac, Mislav Grgic. 2004 A Survey Of Biometric Recognition Methods. In: Proceeding of 46th International Symposium Electronics in Marine, Zadar, Croatia, June, 2004, pp. 184-193.

30. Kamaldeep. 2011. A Review Of Various Attacks On Biometrics System And Their Known Solutions, International Journal of Computer Technology and Application, 2(6), (2011), 1980-1992.
31. Anil K. Jain, Karthik Nandakumar, Abhishek Nagar. 2008. Biometric Template Security, EURASIP Journal on Advances in Signal Processing, 2008, (2008), Article no. DOI :http://dx.doi.org/113. 10.1155/2008/579416
32. Christian Rathageb, Andreas Hammerle-Uhl. 2011. A Survey on Biometric Cryptosystem and Cancelable Biometrics. EURASIP Journal on Information Security, (2011). DOI: http://dx.doi.org/10.1186/1687-417X-2011-3
33. Abhishek Nagar, Karthik Nandakumar, Anil K. 2010. Jain, Biometric Template Transformation: A Security Analysis. In: Proc. of SPIE 7541, Media Forensics and Security II, 7541, (2010). DOI: http://dx.doi.org/10.1117/12.839976
34. Vishal M. Patel, Nalini Kumar. Ratha, Rama Chellappa. 2015. Cancelable Biometrics: A Review, IEEE Signal Processing Magazine, 32(5), (2015), 54 – 65. DOI: http://dx.doi.org/10.1109/MSP.2015.2434151
35. Nalini K. Ratha, Sharat Chikkerur, Jonathan H. Connell, Ruud M. Bolle. 2007. Generating Cancelable Fingerprint Templates. IEEE Transactions on Pattern Analysis and Machine Intelligence, 29(4), (2007), 561-572. DOI: http://dx.doi.org/10.1109/TPAMI.2007.1004
36. Ruud M. Bolle, Jonathan H. Connel, and Nalini K. Ratha. 2002. Biometrics Perils and Patches, Pattern Recognition, 35(12), (2002), 2727–2738. DOI: http://dx.doi.org/ 10.1016/S0031-3203(01)00247-3
37. Nalini K. Ratha, Jonathan H. Connel, and Ruud. Bolle. 2001. Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM System Journal, 40(3), (2001), 614–634. DOI:http://dx.doi.org/ 10.1147/sj.403.0614
38. Padma Polash Paul, Marina Gavrilova. 2012. Multimodal Cancelable Biometrics. In: Proceedings of ICCI*CC, Kyoto, August 22-24, 2012, pp. 43-49. DOI: http://dx.doi.org/ 10.1109/ICCI-CC.2012.6311208
39. Patrick Lacharme, Aude Plateaux. 2011. PIN-based Cancelable Biometrics. In: Proceedings of International Journal of Automated Identification Technology, 3(2), (2011), 75-79.
40. Eliza Yingzi Du, Kai Yang, Zhi Zhou. 2011. Key Incorporation Scheme for Cancelable Biometrics. Journal of Information Security. 2(4), (2011), 185-194. DOI: http://dx.doi.org/10.4236/jis.2011.
41. Andrew B. J. Teoh, Yip Wai Kuan, Sangyoun Lee. 2007. Cancellable Biometrics and Annotation on BioHash. ELSEVIER Journal of Pattern Recognition Society, 41(6), (2007), 2034-2044. DOI: http://dx.doi.org/10.1016/j.patcog.2007.12.002
42. Andrew B.J. Teoh, David Ngo Chek Ling, Alwyn Goh. 2004. Biohashing: Two Factor Authentication Featuring Fingerprint Data and Tokenised Random Number, Pattern Recognition 37 (11), (2004) 2245–2255. DOI: http://dx.doi.org/10.1016/j.patcog.2004.04.011
43. Jinyu Zuo, Nalini K. Ratha, Jonathan H. Connel. 2008. Cancelable Iris Biometrics. In: Proccedings of 19th Int. Conf. on Pattern Recognition, Tampa, FL, December 8-11, 2008, pp. 1-4. DOI: http://dx.doi.org/10.1109/ICPR.2008.4761886
44. Jaishaker K. Pillai, Vishal M. Patel, Rama Chellappa, Nalini K. Ratha. 2011. Sectored Random Projections for Cancelable Iris Biometrics. In: ICASSP, 2010, pp. 1838 – 1841. DOI: http://dx.doi.org/10.1109/ICASSP.2010.5495383
45. Jaishaker K. Pillai, Vishal M. Patel, Rama Chellappa, Nalini K. Ratha. 2011. Secure and Robust Iris Recognition using Random Projections and Sparse Representations. IEEE Transaction on Pattern Analysis and Machine Intelligence, 30(9), (2011), 1877–1893. DOI: http://dx.doi.org/10.1109/TPAMI.2011.34
46. Andrew B.J. Teoh, Chong T. Yuan. 2007. Cancelable Biometrics Realization with Multispace Random Projections. IEEE Transaction on Systems, Man, and Cybernetics, Part B: (Cybernetics), 37(5), (2007), 1096-1106. DOI: http://dx.doi.org/10.1109/TSMCB.2007.903538
47. Marios Savvides, B. V. K. Vijaya Kumar, P. K. Khosla. 2004. Cancelable Biometric Filters for Face Recognition. In: Proceedings of International Conference on Pattern Recognition, 3, (2004), 922–925. DOI: http://dx.doi.org/10.1109/ICPR.2004.1334679
48. Kenta Takahashi, Shinji Hirata. 2011. Cancelable Biometrics with Provable Security and its Application to Fingerprint Verification. IEICE Transaction on Fundamental Electronic Communication and Computer Science, 94(1), (2011), 233–244.
49. Shinji Hirata, Kenta Takahashi. 2009. Cancelable Biometrics with Perfect Secrecy for Correlation-based Matching. Lecture Notes in Computer Science, Springer, 5558, (2009), 868–878. DOI: http://dx.doi.org/10.1007/978-3-642-01793-3_88
50. Jutta Hammerle-Uhlr, Elias Pschernig, Andreas Uhl. 2009. Cancelable Iris Biometrics Using Block Re-Mapping And Image Warping. Springer Lecture Notes on Computer Science Information Security, 5735. (2009), 135-142. DOI:http://dx.doi.org/10.1007/978-3-642-04474-8_11
51. Emanuele Maiorana, Patrizio Campisi, Julian Fierrez, Javier Ortega-Garcia, Alessandro Neri. 2010. Cancelable Templates for Sequence-based Biometrics with Application to On-line Signature Recognition. IEEE Trans. Syst., Man Cybern. A, 40(3), (2010), 525–538. DOI: http://dx.doi.org/10.1109/TSMCA.2010.2041653
52. Wenhua Xu, Qianhua He, Yanxiong Li, Tao Li. 2008. Cancelable Voiceprint Templates based on Knowledge Signatures. In: Proceedings of International Symposium of Electronic Commerce and Security, August, 2008, pp. 412–415. DOI: http://dx.doi.org/10.1109/ISECS.2008.100
53. Christian Rathgeb, Frank Breitinger, 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
54. Christian Rathgeb, Frank Breitinger, Christoph Busch. 2013. Alignment-free Cancelable Iris Biometric Templates based on Adaptive Bloom Filters. In: Proceedings of International Conference on Biometrics, Madrid, June 2013, pp. 1–8. DOI:http://dx.doi.org/10.1109/ICB.2013.6612976
55. Christian Rathgeb, Christoph Busch. 2014. Cancelable Multi-Biometrics: Mixing Iris-codes based on Adaptive Bloom Filters. Comput. Security, 42, (2014), 1–12. DOI: http://dx.doi.org/10.1016/j.cose.2013.12.005
56. Jutta Hammerle-Uhl, Elias Pschernig, Andreas. Uhl. 2013. Cancelable Iris-Templates using Key-dependent Wavelet Transforms. In: Proceedings of International Conference on Biometrics Compendium, IEEE Biometrics, Madrid, June 4-7, 2013. pp. 1-8. DOI: http://dx.doi.org/10.1109/ICB.2013.6612960
57. Cai Li, Jiankun Hu. 2014. Attacks via Record Multiplicity on Cancelable Biometrics Templates, Concurrency and Computation: Practice and Experience. 26(8), (2014), 1593–1605. DOI:http://dx.doi.org/10.1002/cpe.3042
58. Anil K. Jain, Arun Ross, Umut Uludag, Biometric Template Security: Challenges and Solutions. In: Proceedings of 13th European Signal Processing Conference, Antalya, September, 2005, pp.1-4.
59. Xuebing Zhou, Stephen D. Wolthusen, Christoph Busch, Arjan Kuijper. 2009. A Security Analysis of Biometric Template Protection Schemes. Lecture Notes in Computer Science, 5627, (2009), 429-438. DOI: http://dx.doi.org/10.1007/978-3-642-02611-9_43
60. Rima Belguechi, Estelle Cherrier, Christophe Rosenberger. 2012. How to Evaluate Transformation Based Cancelable Biometric Systems? In: NIST-IBPC, United States, March, 2012.
61. Zhe Jin, Meng-Hui Lim, Andrew Beng, J. Teoh, Bok-Min. Goi. 2014. A non-invertible Randomized Graph-based Hamming Embedding for Generating Cancelable Fingerprint Template. ELSEVIER, Pattern Recognition Letter, 42, (2014), 137-147.

DOI: http://dx.doi.org/10.1016/j.patrec.2014.02.011
62. Yan Sui, Xukai Zou, Eliza Y. Du, Feng Li. 2014. Design and Analysis of a Highly User-Friendly, Secure, Privacy-Preserving, and Non Revocable Authentication Method. IEEE Transaction on Biometrics Compendium, 63(4), (2014), 902-916. DOI: http://dx.doi.org/10.1109/TC.2013.25
63. Rudresh Dwivedi, Somnath Dey. 2015. Cancelable Iris Template Generation using Look-up Table Mapping. In: Proceedings of 2nd International Conference on Signal Processing and Integrated Networks (SPIN), Noida, Feb 19-20, 2015. pp. 785-790. DOI: http://dx.doi.org/10.1109/SPIN.2015.7095296
64. Wei-jing Wong, Mou-ling Dennis Wong, Yau-hee Kho. 2013. Multi-line code: A Low Complexity Revocable Fingerprint Template for Cancelable Biometrics. Journal of Central South University, 20(5), (2013),1292-1297. DOI: http://dx.doi.org/10.1007/s11771-013-1614-8
65. Nobuyuki Nishiuchi, Hiroka Soya. 2011. Cancelable Biometric Identification by Combining Biological Data with Artifacts. In: Proceedings of ICBAKE, Kagawa, September, 2011, pp. 61-64. DOI: http://dx.doi.org/10.1109/ICBAKE.2011.11
66. Moazzam Butt, Naser Damer. 2014. Helper Data Scheme for 2D Cancelable Face Recognition using Bloom Filters. In: Proceedings of International Conference on Systems, Signals and Image Processing (IWSSIP), Dubrovnik, May, 2014, pp. 271-274.
67. Sara Nazari, Mohammad Shahram Moin, Hamidreza Rashidy Kanan. 2014. Cancelable Face using Chaos Permutation. In: Proceedings of 7th International Symposium on Telecommunications (IST), Tehran, September, 2014, pp. 925-928. DOI: http://dx.doi.org/10.1109/ISTEL.2014.7000835
68. Osama Ouda, Norimichi Tsumura, Toshiya Nakaguchi. 2010. Tokenless Cancelable Biometrics Scheme for Protecting Iris Codes. In: Proceedings of 20th International Concefence on Pattern Recognition (ICPR), Istanbul, August, 2010, pp. 882-885. DOI: http://dx.doi.org/10.1109/ICPR.2010.222
69. Stefan Jenisch, Andreas Uhl. 2011. Security Analysis Of A Cancelable Iris Recognition System Based On Block Remapping. In: Proceedings of 18th IEEE International Conference on Image Processing (ICIP), Brussels, September, 2011, pp. 3213 – 3216. DOI:http://dx.doi.org/10.1109/ICIP.2011.6116352
70. Andrew B. J. Teoh, David C. L. Ngo. 2004. Biophasor Token Supplemented Cancelable Biometrics. In: Proceedins of Int. Conf. on Control, Automation, Robotics and Vision, Singapore, December 2006, pp. 1-5. DOI: http://dx.doi.org/10.1109/ICARCV.2006.345404
71. Marios Savvides, B. Kumar, P. K. Khosla. 2004. Cancelable Biometric Filters for Face Recognition. In: Proceedings of 17th ICPR'04, August, 2004.Vol. 3, pp. 922-925. DOI: http://dx.doi.org/10.1109/ICPR.2004.1334679
72. Alwyn Goh, Anderw B. J. Teoh, David C. L. Ngo. 2006. Random Multispace Quantization as an analytic Mechanism for Biohashing of Biometric and Random Identity Inputs, IEEE Transaction in Pattern and Machine Intelligence, 28(12), (2006), 1892-1901. DOI:http://dx.doi.org /10.1109/TPAMI.2006.250
73. T. Boult. 2006. Robust Distance Measures for Face Recognition Supporting Revocable Biometric Token. In: Proceedings of 7th Int. Conf. on Automatic Face and Gesture Recognition, Southampton, April 2-6, 2006, pp. 560-566. DOI: http://dx.doi.org /10.1109/FGR.2006.94
74. T. Boult, W. Scheirer, and R. Woodworth. 2007. Revocable Fingerprint Biotokens: Accuracy and Security Analysis. In: Proceedings of IEEE Conference on Computer Vision and Pattern Recognition, June 2007, pp. 1–8. DOI: http://dx.doi.org /10.1109/CVPR.2007.383110
75. Tee Connie, Andrew Teoh, Michael Goh, David Ngo. 2005. Palmhashing: A Novel Approach for Cancelable Biometrics. ELSEVIER Journal on Information Processing Letter, 93(1), (2005), 1–5. DOI: http://dx.doi.org/10.1016/j.ipl.2004.09.014
76. Priyanka Das, Kannan Karthik, Boul Chandra Garai. 2012. A Robust Alignment-free Fingerprint Hashing Algorithm based on Minimum Distance Graphs. ELSEVIER Journal on Pattern Recognition, 45(9), (2012), 3373–3388. DOI: http://dx.doi.org/10.1016/j.patcog.2012.02.022
77. Song Wang, Jiankun Hu. 2014. Design of Alignment-free Cancelable Fingerprint Templates via Curtailed Circular Convolution. ELSEVIER Journal on Pattern Recognition, 47(3), (2014), 1321–1329.
78. DOI:http://dx.doi.org/10.1016/j.patcog.2013.10.003
79. Karthik Nandakumar, Anil K. Jain. 2009. Biometric Template Protection: Bridging the Performance Gap between Theory and Practice. IEEE, Signal Processing Magazine, 32(5), (2015), 88-100. DOI: http://dx.doi.org/10.1109/MSP.2015.2427849
80. Xuebing Zhou, Stephan D. Wolthusen, Christoph Busch, Arjan Kuijper. 2009. A Security Analysis of Biometric Template Protection Schemes. Lecture Notes in Computer Science, 5627, (2009), 429-438. DOI: http://dx.doi.org/10.1007/978-3-642-02611-9_43
81. Andy Adler. 2004. Reconstruction of Source Images from Quantized Biometric Match Score Data. In: Proceedings of Biometrics Conference, Washington, DC, September 2004
82. Nalini K. Ratha, Jonathan H. Connell, Ruud M. Bolle. 2001. An Analysis of Minutiae Matching Strength, in: 3rd International Conference on Audio- and Video-Based Biometric Person Authentication, 2001, pp. 223-228. DOI: http://dx.doi.org/10.1007/3-540-45344-X_32
83. Andy Adler. 2003. Sample Images can be Independently Restored from Face Recognition Templates. In: Proceedings of Canadian Conf on Electrical and Computer Engineering, 2003, pp. 1163-1166. DOI: http://dx.doi.org/10.1109/CCECE.2003.1226104
84. Russell Ang, Rei Safavi-Naini, Luke McAven. 2005. Cancelable key-based fingerprint templates. In: Proceedings of 10th Australian Conf. Inf. Security Privacy, Jul. 2005, pp. 242–252. DOI: http://dx.doi.org/10.1007/11506157_21
85. Song Wang, Jiankun Hu. 2012. Alignment-free Cancelable Fingerprint Template Design: A Densely Infinite-to-One Mapping (DITOM) approach, Pattern Recognition, 45(12), (2012), 4129–4137. DOI: http://dx.doi.org/10.1016/j.patcog.2012.05.004
86. Chulhan Lee, Jeung-Yoon Choi, Kar-Ann Toh, Sangyuong Lee, J. Kim. 2007. Alignment-free Cancelable Fingerprint Templates Based on Local Minutiae Information. IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics, 37(4), (2007),980–992. DOI: http://dx.doi.org/10.1109/TSMCB.2007.896999
87. Tohari Ahmad, Jiankun Hu, Song Wang. 2011. Pair-polar Coordinate based Cancelable Fingerprint Templates. Pattern Recognition, 40(10–11), (2011), 2555–2564. DOI: http://dx.doi.org/10.1016/j.patcog.2011.03.015
88. Huijuan Yang, Xudong Jiang, Alex C. Kot. 2009. Generating Secure Cancelable Fingerprint Templates using Local and Global Features. In: Proceedings of 2nd IEEE International Conference on Computer Science and Information Technology, Beijing, 2009, pp. 645–649. DOI: http://dx.doi.org/10.1109/ICCSIT.2009.5234870
89. C. J. Hill. Risk of Masquerade Arising from the Storage of Biometrics. 2001. B.S. Thesis, Australian National University, November 2001.

90. Adams Kong, King Hong Cheunga, David Zhanga, Mohamed Kamelb, Jane You. An analysis of BioHashing and its variants. ELSEVIER Journal on Pattern Recognition, 39, (2006), 1359-1368. DOI: http://dx.doi.org/10.1016/j.patcog.2005.10.025
91. Feng Quan, Su Fei, Cai Anni, Zhao Feifei. 2008. Cracking Cancelable Fingerprint Template of Ratha. In: Proceedings of International Symposium on Computer Science and Computational Technology, 2008, pp. 572-575. DOI: http://dx.doi.org/10.1109/ISCSCT.2008.226
92. Sang Wook Shin, Mun-Kyu Lee, Daesung Moon, Kiyoung Moon. 2009. Dictionary Attack on Functional Transform-based Cancelable Fingerprint Templates, ETRI J, 31(5), (2009), 628-630. DOI: http://dx.doi.org/10.4218/etrij.09.0209.0137
93. Julien Bringer, Herve Chabanne, Constance Morel. 2014. Shuffling is not sufficient: Security analysis of Cancelable Iris codes based on a Secret Permutation. In: Proceedings of IEEE International Joint Conference on Biometrics, Clearwater, FL, 2014, pp. 1-8. DOI: http://dx.doi.org/10.1109/BTAS.2014.6996280
94. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, Digital image steganography: Survey and analysis of current methods, Elsevier, Signal Processing, 90, (2010), 727-752.
A. Nag, S. Biswas, D. Sarkar, P. P. Sarkar, A Novel Technique for Image Steganography based on Block-DCT and Huffman Encoding, in: Proc. of International Journal of Computer Science and Information Technology, 2(3), June 2010.
95. Rig Das, T. Tuithung, A Review On “A Novel Technique For Image Steganography Based On Block-DCT And Huffman Encoding”, in: Proc. SPIE 8768, International Conference on Graphic and Image Processing (ICGIP), March 2013.

Author Biographies

Bismita Choudhury is a PhD student in the Faculty of Engineering, Computing and Science, Swinburne University of Technology (Sarawak Campus), Malaysia and her research interests are in biometrics and cancelable biometrics, steganography, image processing, machine learning etc.

Patrick Then is working in Swinburne University of Technology (Sarawak Campus), Malaysia and is an active researcher with strong collaboration with industries. He has been actively publishing papers for journal, conference proceedings and book chapters. His research interests are in Knowledge Discovery, Data Mining, Information Security, Privacy Preserving, Health Economics, Biostatistics and Microbiology.

Biju Issac is working in Teesside University as an academic staff. He earned PhD in Networking and Mobile communications, along with MCA (Master of Computer Applications) and BE (electronics and communications engineering). Dr Issac is research active and has authored more than 90 refereed conference papers, journal papers and book chapters. He is in the technical programme committee of many peer-reviewed international conferences and journals.

Valliappan Raman is currently serving as a lecturer at the Swinburne University of Technology (Sarawak Campus), Malaysia. He has done Bachelor of Engineering (Mechanical), Master of Science (Computer Science), and PhD (Computer Vision and Pattern Recognition). His research interest involves Medical Imaging, Object Recognition, Biometrics, Health Informatics and Data mining.

Manas Kumar Haldar has been with Swinburne University of Technology (Sarawak Campus), Malaysia since 2006. He has obtained his PhD as Charles Hestermann Merz scholar of Trinity College, Cambridge, UK. He worked on high frequency power generation by electron wave interactions. He also worked on surface acoustic waves at the University of Oxford, UK. He has over 30 years of teaching and research experience.