Abstract — Biometric is simply a dimension related to human characteristics. It deals with automated strategies for recognizing or verifying someone based on his biological or behavioral features. The safety and convenience provided by biometric data are higher than any other personal identification methods. But there is also a high-risk factor in case of compromising biometric traits, since revoking it and reissue with a new one is not possible for biometric data. This paper focuses on the security aspects of iris biometric recognition system and a survey based on various template protection schemes. Many schemes are proposed to provide security to iris templates in a database such as biometric cryptosystems, template transformation methods, steganography, and visual cryptography.

Key words: Biometric, Iris Biometric recognition system, Template, Visual cryptography.

I. INTRODUCTION

Recognizing an individual making use of passwords isn't adequate for a stable personal authentication since they will be effortlessly shared, or stolen. These days, automatic authentication has turned out to be very popular. Different applications want individual identification such as passport control, cell phones security, PC access control, electronic banking, ATM, airport security and so on. Rather than utilizing “what somebody has” or “what, somebody recalls” it's more appropriate to utilize “who somebody is”. The innovation exploring this concept is referred to as biometrics. A biometric framework assembles raw information from various body parts, such as fingerprint, iris, palm print, voice, retina etc. Then, it utilizes a feature extraction algorithm to change this raw information into biometric templates and they are saved in a database. Iris recognition is a most promising biometric method that is used to identify people. It is fixed and does not change throughout the lifespan of a person. The randomly distributed features of an iris are the most distinct fact about iris recognition system. Iris is good for one-to-many identifications and the speed of comparison is also high. A single entry of iris template can last for a long time, so frequent updating is not needed. As appeared in the figure: 1[7], Iris is a circular anatomical structure placed in the middle of cornea and lens of the eye. Its function is controlling the light entering through the pupil. The average iris diameter is between 11.6 mm and 12.0 mm, and the pupil measure is between 10% and 80% of the iris diameter [7].

The most well-known and commercial iris system was proposed by J. G. Daugman [1, 2]. For these algorithms, he has the patents and those forms the premise of most of today’s commercial iris recognition systems. Now iris system is efficiently used in various applications handling large database. An iris recognition system structure for converting an iris image to the corresponding template is portrayed in figure 2[13].
A high-quality digital camera is used for capturing iris images. Near-infrared illuminators are used for getting the rich iris features. Specular reflections due to a bright background are avoided using the NIR spectrum. The segmentation is a process to segment the annular iris regions of an eye image. The iris region is assumed as two circles bounded by iris-pupil and iris-sclera. The eyelids and eyelashes are typically interference in iris segmentation, these are avoided using some threshold strategies. Rubber sheet model of Daugman’s is used for normalization. Every pixel in the iris portion is remapped to a pair of polar coordinates during normalization. It helps in getting a common format. The pupil center is assumed as the reference. The feature encoding derives the most varying capabilities of iris and results in a binary encoded format. The hamming distance calculation is used for the matching process, where a hamming distance value of zero indicates a correct fit and one indicates non-match.

II. ATTACKS ON IRIS BIOMETRIC SYSTEM

A biometric system is exposed to various attack vectors between starting and conveying the result. Point of attack of a biometric framework can be classified into eight: fake biometric on the sensor, extraction process overriding, feature illustration tampering, replay attack, matcher corruption, channel attack among saved template and matcher, tampering in the saved template and the final decision tampering. These are depicted in figure 3[3].

Biometric frameworks are more consistent and easy to use. The principle issue about biometrics is the irrevocable connection between biometric traits and personal record about a user. One of the key aspects of outlining a reliable biometric framework is the security of the system. We can modify our passwords but we can’t modify our biometric features. This shows that after a biometric data has been compromised, there could be no going back. The tight link between user personal records and biometrics have both advantages and disadvantages. Simply biometric templates in database reveal
non-changeable information of individuals, once somebody gets a hand on them, they lose their purpose of utilization. The iris template is normally saved as a raw data in the databases. It was trusted that this form of iris layout doesn’t deliver any quality details to reconstruct the iris image. But some researchers could propose a reversibility idea for the iris code utilizing a probabilistic method based on genetic algorithm [6]. These scientists demonstrated the possibility frameworks against modifying templates in database. At the point when the security of template database was not available, templates could be removed; altered or new templates could be added to the framework. It might bring authorization to unauthorized users or denial of service to authenticated users. Researchers have attempted different strategies to secure the database. The techniques are cryptography, watermarking and steganography, visual cryptography.

III. STUDY ON IRIS TEMPLATE SECURITY

A template represents a briefing of salient capabilities that sum up the biometric facts of an individual. As biometrics is used in excessive safety zones and it is subjected to many forms of attacks, providing security to templates is more crucial.

An excellent biometric template safety method should have the four properties given below [3].

1) Diversity: For guaranteeing user’s privacy, the cross-matching over the database shouldn’t be permitted.
2) Revocability: It should be trustworthy to repudiate a compromised template and recreate another one based on the same biometric information.
3) Security: Acquiring the original biometric template from the protected template should be a difficult task. This prevents the attack based on creating physical spoofs of biometric traits from a stolen template.
4) Performance: The security plan of templates should not reduce the performance of recognition (FAR and FRR) in the biometric system.

Handling intra-user variability is the principal challenge within the development of biometric template security schemes, which is agreeable to all of the above-mentioned features. Different acquisitions of the same biometric characteristic deliver variations in feature set [5]. Because of this cause, the templates stored in an encoded format (using RSA, AES schemes) is not appropriate for biometric traits. Encryption is not an easy task and a small change in the feature set may cause an expansive difference in encrypted format. Decryption of the template and performing matching it with the query is possible, but that approach leads to template exposing throughout each authentication attempt. So general encryption schemes are not suitable for providing security to a biometric template. Different categories of biometric template protection methods are depicted in figure 4[5]. These template protection techniques are broadly divided as feature transformation and crypto-based systems.

Fig 4. Categories of iris template security.

A. Feature Transformation

In this method, a function is utilized to convert a biometric trait into a transformed template format. The resultant transformed templates are stored in a database. The similar function is used to query features in recovery part to obtain transformed query. The functions are taken in order that it
should not decrease the uniqueness of biometric traits but it should be tolerant to intra-class variations. Using different transforms for different applications is suggested to prevent the cross-matching attacks in transformed templates. Cancelable biometric is such a template protection scheme that replaces a biometric template when the stored template is stolen or lost [4]. CB is designed in a manner that it must be computationally tough to get back the original unique biometric data. Based on the features of transformation function or the approach of transform, the feature transformation functions are of two types.

1) Invertible Feature Transformation

Biometric salting is a transform of biometric-based on invertible functions. Any invertible transform of biometric template is taken as salting (even if the original biometric template can’t be able to reconstruct), for this reason, the secrecy of transform parameters is very important. In case of a user-specified transform are applied, the transform parameters (which is supposed as secret) should be supplied at every authentication. If the transform parameters are compromised, an attacker can recover the original template and that leads to performance loss to the system. So the secrecy of transform parameters is important. The key outcomes introduction reduce false accept rates of an overall system. Because the key is user specific, for a same user biometric data multiple templates can be available. One of the advantages of the system is, by utilizing an alternative user-specific key the revoking and replacing of compromised template become easy.

2) Non-Invertible Feature Transformation

In this technique, the transformation function is in one-way format. For updating the templates, the implemented transform parameters are modified. The main feature of non-invertible transforms is that even if the transformed template and key are available the template inversion is difficult. This method provides an effective security system than the Invertible feature transformation method. By utilizing user-specific and application-specific functions, revocability and diversity can be easily accomplished, respectively. Lack of accuracy is one of the disadvantages of the non-invertible transform. The transformed biometric templates are difficult to align so that, the performance decreases [25].

Research is continuing for cancelable biometrics templates using different transformation functions. A pseudo-random password generation and combining it into the template creation is an example of invertible transformation method. The bio hashing schemes have been proposed for iris in [10]. Transformation using iris shuffling algorithm utilizes the n-bit binary key to rearrange the iris code format after partitioning it into n portions. These outcomes demonstrate that the algorithms not just accomplish revocability, yet in addition build separation between the hamming distance distribution of real and imposter user. The inverse operation and pre-imaging attacks in iris-based CB are discussed in [14]. Applying non-invertible transformation function to CB template is explained in [15]. Cancelable iris templates can be created using two methods by applying non-invertible transformation function. Shifting and combining rows of the binary iris template is the first function used. The other method utilizes a key for adding a random noise pattern to the binary template. Some schemes using non-invertible transforms called block remapping and image wrapping in the image domain before iris feature extraction [25]. A cancelable iris biometrics which does not require any tokenized random number and using bloom filters to eliminate local location relationship in the iris is also proposed. But [16, 17] says that the security schemes based on bloom filters cannot satisfy the cross-matching. To prevent cross-matching in schemes based on bloom filters a permutation strategy is adopted. A cancelable iris biometric based on the Indexing-First-One (IFO) hashing is described by Lai et al. [18]. It is inspired by the Min-hashing a CB based on the (IFO) hashing scheme.

B. Biometric cryptosystems

The combination of biometrics with cryptographic algorithms results in a much effective scheme known as a biometric cryptosystem (BCS). This system takes gain of the cryptographic degree of protection together with the unique nature of biometric traits. It is very hard to sharing, copying biometrics as compared to passwords. Biometric cryptosystem uses some public data about the biometric features saved in a database that is called helper data. Helper data do not disclose any valuable information about the original templates. Based on how the helper data is gotten, the biometric cryptosystem is divided into key binding and key generation schemes. Biometric comparisons are done by verifying key validities. Either a key or a failure message is the output of authentication process [13]. Based on how helper information is gotten, BCS is categorized into two types.
1) **Key binding Method**

In the key binding BCS, the helper data is acquired by binding a chosen key (not depend on any biometric features) to the biometric template. The binding process results in a stored code or helper data which is a fusion of the biometric template and secret key as shown in figure 5[30]. A pseudo-random generator produces a user-specific key, which is then extended to a code word using error correction code. So it is difficult to get the biometric template or the key only using helper data. In the verification, the key-releasing algorithm utilizes the stored code and biometric query. This system helps to avoid the intra-user or intra-class variations in biometric information. The matching accuracy has to be reduced because of the usage of error correction schemes. BCS is drafted in such a way that they not to provide diversity and revocability.

![Fig 5. Key binding method.](image)

Fuzzy commitment scheme suggested by Juels and Wattenberg is one of the popular key binding BCS. Combination of error correcting codes and cryptography is used to attain a secure system. At the enrollment time, the user chooses a secret message C from a group of code words of some error-correcting code. Existing methods use fuzzy commitment, fuzzy vault fuzzy extractor/fuzzy sketches to support fuzzy iris recognition while protecting data privacy. Fuzzy commitment schemes for iris biometric cryptosystem are explained by Hao et al. [19]. Hadamard and Reed Solomon error-correcting codes are used in the fuzzy commitment, and a biometric key is utilized to “encrypt” biometric data. But [20] demonstrated that data privacy could be leaked in the fuzzy commitment scheme. This scheme suffering from a decodability attack based cross-matching is also demonstrated. Fuzzy vault scheme to iris template protection is explained in [21]. Vault is created using polynomial encoding and error corrections. Cross-matching attack in the fuzzy vault scheme might disclose original iris data.

2) **Key generation Method**

In this scheme stored data is derived only from the biometric query. The secure sketch is considered as helper data which doesn’t provide adequate details about the template. This scheme is depicted in figure 6[30]. Keys are directly produced from the helper data and the available biometric template. Direct key generation from biometrics is a better proposition but his intrauser variability makes it difficult. This scheme suffers from key stability and key entropy. During verification, the biometric sample is used in the same way as in the enrollment to create a sample code that is a noisy version of the enrolment code. This kind of direct key generation from biometrics can be more useful in many applications. Producing a key with high stability and entropy is difficulty in this system.
The first to address biometric key generation is using keystroke dynamics. Key-generation schemes based on helper data are also known as “fuzzy extractors” or “secure sketches” that is explained in [22]. A uniformly random string from the biometric trait is extracted using the fuzzy extractor. Fuzzy extractor based iris template protection scheme is explained in [23]. Bringer et al. explained the way to extract optimal secure sketches to protect data privacy for a given iris database. Security problems such as privacy leakage and cross-matching for existing fuzzy extractor construction are pointed out in [24].

C. Watermarking

This is one of the security mechanisms that is used to concealing critical information into a multimedia content. The embedding of one pattern into another pattern is known as a watermarking approach. Only if the intruder knows the watermark data, he can replace the biometric template. Marking with encryption system gives greater security, and it is helpful in various applications such as copyright assurance, tempering discovery, and broadcast observations and data authentication [11]. The major parts of a watermarking framework are embedder and a detector as appear in figure 7[30].

To utilize keys in a comparable manner for encryption, watermarking framework can be designed. The key is utilized for casting, detecting and removing a watermark. Without the knowledge of the key, it is exceptionally hard to identify the occurrence or existence of a watermark in a validate work. This is again difficult on those circumstances where the watermarking algorithm is known in advance. It is further extremely hard to provide the restriction on the access to the key. Protect iris templates by watermarking them is explained in [4], it helps to detect the tampering in the original template.
D. Steganography

Steganography is a type of "secured composing". The primary target of steganography is to safely communicate, so it is particularly useful in distributed systems where raw information’s transmitted through a non-secure channel. The covers utilized as a part of steganography strategy can be pictures, audio, video and other PC documents that contain insignificant data. Stego images are created by implanting secret image into a cover image. The original image is embedded in a digital image utilizing a key and encoder framework, this scheme is depicted in figure 8[11]. Steganography is utilized for providing biometric template protection is depicted in [26, 27]. The stego or covered image is then transmitted over a channel to the destination where a similar key is utilized to decode this stego image.

![Steganography Diagram]

Fig 8. Steganography.

The application of steganography in iris biometric is proposed in [25], an upgrade of temporal-spatial domain algorithm which involves the scheme of Least Significant Bits (LSB) is applied as the new model which changes iris images to a binary stream and hides into an appropriate lower bit plane.

E. Visual cryptography

It is a novel secret sharing method in which visual information (images, text, etc.) to be encrypted such that their decryption can be done by a human visual system, without any hard cryptographic calculations [8]. Here secret images encrypted into shares in a way that stacking an adequate number of shares only disclose the secret image. Shares are typically represented as transparencies. It provides an additional layer of authentication to iris system. Iris template is separated into multiple shares and those shares are distributed as shown in figure 9[29]. Regardless of whether one of the shares is compromised the original image can’t be recovered.

![Visual Cryptography Diagram]

Fig 9. Visual cryptography.
IV. COMPARISON

The below table depicts the different iris template security methods discussed in this paper with the advantages and disadvantages [30].

<table>
<thead>
<tr>
<th>APPROACH</th>
<th>METHOD</th>
<th>ADVANTAGES</th>
<th>DISADVANTAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometric</td>
<td>Key Binding and Generation</td>
<td>• Tolerant to intra user variation&lt;br&gt;• Useful in cryptosystem</td>
<td>• Generation of a key with high stability and entropy is hard&lt;br&gt;• Not ensuring diversity&lt;br&gt;• Non-revocable&lt;br&gt;• Careful attention is needed to create helper data (it takes some biometric features information)</td>
</tr>
<tr>
<td>Cryptosystems</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature Transformation</td>
<td>Invertible and Non invertible transform</td>
<td>• A user can have different transformed template&lt;br&gt;• Cross-matching not possible</td>
<td>• Finding transformation function is difficult (Hashing cannot be used for biometric templates)&lt;br&gt;• User-dependent function (password/pin needed)</td>
</tr>
<tr>
<td>Watermarking</td>
<td>Invisible (Parity method )</td>
<td>• Hard to forge the stored biometric template&lt;br&gt;• Proving ownership</td>
<td>• Time complexity is huge for inserting watermark pattern.</td>
</tr>
<tr>
<td>Steganography</td>
<td>Secret embedded to a digital image using key</td>
<td>• Better way of transmitting biometric raw data through insecure channels</td>
<td>• Attacks are possible</td>
</tr>
<tr>
<td>Visual Cryptography</td>
<td>Encryption using secret sharing</td>
<td>• Decryption is not complex</td>
<td>• Need space for storing shares</td>
</tr>
</tbody>
</table>

V. SUMMARY AND CONCLUSION

In today’s world, progress in technology has made life easier by providing us with higher levels of data through the invention of various products. But every technology innovation contains the potential of hidden problems to its users. With an ever-growing emphasis on security systems, automatic personal identification frameworks based on biometrics have been obtaining more focus in practical and research aspects. With the increase of applications including personal digital assistants like Aadhaar, smartphone security, banking, border crossing and so on, more and more confidential data is stored. However, the misuse and theft of those security systems are increasing. Iris biometric is one of the tremendously developed personal identification ways. Because an iris is unique for an individual the security is a major concern for iris-based systems. Different kinds of attacks are propelled against an iris recognition system. This paper discussed the different methodologies proposed by researchers to secure the iris biometric template in a database.

There is no ideal template protection approach. The application scenario and necessities play a significant role in the choice of a protection method. The other main factors that impact the determination of a template protection scheme are the chosen biometric, illustration of its features and the intra-user variations extent. A single template protection scheme might not be ample to fulfill the needs of applications. So, hybrid schemes which are build use of the benefits of various template protection approaches should be created. Now, these kinds of hybrid schemes are proposed by many researchers. For example, a framework that secures an invertible- transformed template utilizing a biometric cryptosystem may have the advantages of both transformed template and biometric cryptosystem approaches. At last, with the developing interest in multi biometric and multifactor
verification schemes, frameworks that concurrently secure multi biometric templates and multiple authentication factors (biometrics, passwords, etc.) have to be produced.

REFERENCES


