International Journal on Emerging Technologies **11**(1): 421-432(2020)

ISSN No. (Print): 0975-8364
ISSN No. (Online): 2249-3255

A Survey of Biometric Key-Binding Biocrypto-System using different Techniques

Neeraj Tantubay and Jyoti Bharti
Department of Computer Science and Engineering,
Maulana Azad National Institute of Technology Bhopal (Madhya Pradesh), India.

(Corresponding author: Neeraj Tantubay)
(Received 23 October 2019, Revised 23 December 2019, Accepted 28 December 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: In Data Secrecy, cryptography acting most significant role for data security, most importantly Data Confidentiality. But the security of any cryptographic algorithm is depended on its cryptography-key or secret- key, as much as secure the key, cryptography algorithm will be secure and robust. Biocrypto-System provide a mechanism known as Biometric key-binding to protect cryptography secret key. This system uses the fusion of user's biometric information and Crypto-Secret-key and forms composite data know as helper data for storage and retrieving secret-key again when the legitimate user attempt to access. This paper reviews different existing techniques of key-binding with different biometric traits as well as Biometric System and its working i.e. feature extraction from fingerprint and Iris image. In addition, this review paper analyses these techniques, compare its limitations based on different biometric characters and various Secret-Key size. The main issue involved in Symmetric cryptography algorithms is its secret-Key size. Large key-size may reduce the performance and security of key-binding techniques.

Keywords: Biocrypto-System, Biometric Key-Binding, fuzzy commitment, fuzzy vault, chaff points, Helper Data.

I. INTRODUCTION

Biocrypto-System (BS) or commonly known as Biometric-Encryption system is a fusion of Biometric-System and Cryptography system, which apply security features of Biometric system to cryptography system to secure its secret-key [2].

Data secrecy has become an essential need in real-world of latest technologies. Biometric-system is a very strong technique to provide security and privacy by its strong unique characteristics of different biometric-samples, that's why, this system is implemented by many organize to enrich its security. It is ratified that a strong recognition system with strong security is not available that substitute the biometrics-system [1].

The bio-systems are automated recognition systems for individuals centered on biometric Characteristics such as behavioral (like Gait, voice and signature etc.) and physiological (like fingerprint, face, and iris etc.). This Biometric system is work mainly in two phases, first is Enrollment phase and other is Verification or Authentication phase. In enrollment phase, behavioral or physiological biometric features are abridged using competent devices and extracted strong idiosyncratic features to construct a template of biometric features then these templates can be stored in local database as well as global i.e. on Internet for further use [1, 2].

The Bio-system authentication is performed the validation of inimitability of personalities based on their unique characteristics of physiological or behavioral same as used in enrollment. During authentication process, the juxtaposition of biometric features of individual against the features taken in enrollment phase of the appealed personality are made and provide authorized access the system or data only when there is satisfactory match [3].

Whereas, cryptographic systems are used to provide privacy and security, to any kind of data by using encryption and decryption techniques. In this technique the user's data is enciphered using a key so that it becomes very complicated to understand it by illegitimate. The actual data is retrieved by deciphering the encoded data using only same key. Security of these techniques are solely depend on its secret-key (in case symmetric cryptography), if key is secure or inaccessible by unauthorized one, they perform well. A number of cryptographic techniques based on secret key and public key like DES, AES and RSA, are used for data security and verification purpose [4, 5].

The Biocrypto-Systems (BSs) are mainly design for providing security to the cryptography key. BSs are implemented to securely hide a digital secret key using biometric features or to generate a secure user biometric dependent cryptographic-key from biometric features. BSs also provides key release systems based on biometric for replacing key release system which are based on password like PKI and offers significant security advantages [6]. Though, the forgery, copy, sharing, and distribution of biometrics traits are very challenging or impossible in comparison of alphanumeric passwords [1]. As biometric characteristics are inconsistent therefore conventional bio-systems implement "fuzzy comparisons" based on thresholds matching, whereas the BSs are developed to release or generate constant keys which are unique as original key at authentication [8].

II. CRYPTOGRAPHY SYSTEM

In the field of Information security, cryptography plays a most vital role to secure data and provides confidentiality to the data. Two types of cryptography techniques are available in literature: one is Symmetric-

Key, in which only single Secret-key is applied for Encryption and Decryption of the message. Second Cryptographic systems are based on two types of keys The security and robustness of these algorithms is solely depend on its secret key, if it is compromised then both algorithms are directly breakable while these are more complex. Cryptography technique faces some issues like [5, 7]:

- Secret-Key of encryption algorithm should be as large as possible to protect such algorithm from Brute Force attack.
- If user uses a large key then it is intricate to memorize such large key. In this context user have to note down their secret somewhere, such activity improve chance of key compromise.
- To overcome above situation there is a third party mechanism known as PKI in which users save their secret key and third party provides security to it. In such cash security of secret key again depend on third party trust which may be compromised.

Biocrypto-system is an efficient model which can resolve such problems associated with cryptographic secret-key. BSs are able to protect the cryptographic secret-key either by merging it with the user dependents biometrics data, these biometric data may be from a single biometric source or multi-biometric source, or by directly generating the cryptographic secret-key using user's biometrics, these biometric again may be from a single biometric source or multi-biometric source [30].

III. BIOMETRIC-SYSTEM

Biometric is used to distinguish the identity of a person by comparing their biometrics based on certain characteristics. The word Biometric (bios ="life", metron ="measure") comprises two diverse fields of learning and use [1].

The two functions Verification and Authentication are provided by the biometric-system i.e. biometric authentication techniques such as face recognition, iris scanning, fingerprint-scanning, signature, hand geometry and voice authentication are currently playing an important role particularly in Information security area. Biometric techniques are able to eradicate difficulty of forgotten secret codes and to reinforce security to passcodes and all. Presently, several biometric-cryptographic Techniques have been designed using face, iris, palm prints, fingerprints, signature and voice [9, 10].

Biometrics are denotes as "To Identify an individual using their distinguished features". The biometric information should have the following properties [1, 9]:

- **Distinctiveness:** In this, large distinctness of biometric characteristics should exist (Uniqueness), over the variety of humans so that have great inter-class variability.
- **Robustness:** The biometric characteristic should not be alter (Permanence) over time, so that they have low intra-class variability.
- **Accessibility:** The biometric characteristics should be easy to obtain (Collectability).
- **Availability:** The all humans should have the biometric characteristic (Universality).

secret-key for encryption and public-key for decryption or vice-versa, these are known as Asymmetric-Cryptography systems [4].

Among all biometric techniques, two types of biometric techniques i.e. fingerprint and Iris are used very frequently by organizations for authentication. Working of these two techniques are discussed in details as:

Introduction to Iris Techniques: The iris is part of human eyes that can be represented as annular area of eye surrounded by the pupil and sclera (eye's white part). The iris texture consists very distinguishing information that can be used for personal verification and authentication. The most popular personal recognition systems are based on iris because the accuracy and speed of large-scale identification systems is very high. Each iris consists unique information. The irises information of twins are different [14].

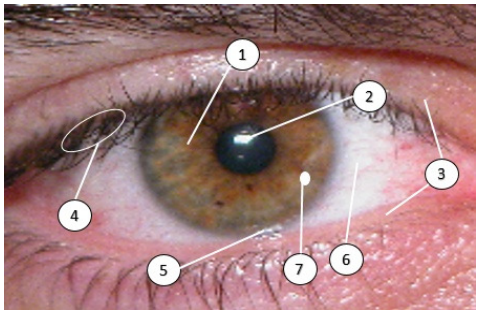


Fig. 1. An Eye Image taken from UBIRIS DATASET which have following parts: (1) Iris (2) pupil (3) eyelids (4) eyelashes (5) shadow caused by an eyelid (6) Sclera (7) specular reflections.

An iris based recognition system uses the iris pattern. Each Iris has a unique patterns that can be extracted through image acquisition system. The iris pattern has the following specific unique features: freckles, crypts, pits, corona, rings, striations, furrows and filaments.

Iris duplication is impossible because of its unique characteristics. The human brain is directly related with the iris that's why this is the parts of the body which firstly decompose after human death. Therefore it is very difficult to generate a synthetic iris to falsely skip security of the biometric verification systems [9, 11].

A. The Iris based Biometric-system

The biometric recognition systems which are based on iris, have the process of extracting features from an iris image. Iris recognition systems are very strong system to provide user verification or authentication. The most essential feature of an iris is its uniqueness i.e. two irises of human cannot be same even they belong to same person (of both eyes) or even among twins [13]. The iris of human eyes is the blackish circular part between white sclera and black pupil has an unusual pattern that provides some important features like coronas, freckles, stripes etc. These features are visible and known as the iris texture [12]. The steps involved to extract these feature from the iris image are given below.

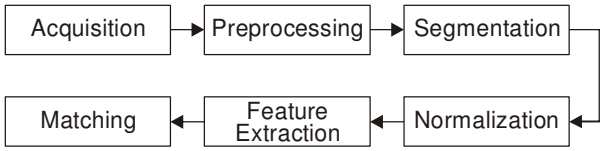


Fig. 2. Working of Iris Biometric-system.

1. Acquisition: There are many kinds of methods have been devised for iris acquisition in iris recognition systems. These methods are depend on the types of devices, spectrums and distances between iris and capturing device.

The iris capturing equipment consists of hardware as well as an infrared sensor to take iris picture. The development of sensor technologies have been provided the great pliability in the development of different acquisition methods. The current advancement in the development of iris acquisition systems uses cameras, lower resolution systems, visible and spectrum which acquires the iris image at multiple distances [1].

2. Pre-processing: Iris image preprocessing is required for enhancing image quality which is degraded during image capturing by the hardware device. Preprocessing is also required to quality assessment. At the time of image acquisition there is chance to any type of noise or any error may be captured with the images. In that case, these erroneous images need quality improvement using pre-processing techniques before applying authentication techniques, Fig. 3. To improve feature's quality of motion blurred and defocused iris images, Iris-preprocessing is used. When pupil enlargement information is obtained during acquisition, pre-processing is again apply to eliminate it. Efficiently enhanced image and remove noise are the important factors to obtain high recognition rates of iris [9].

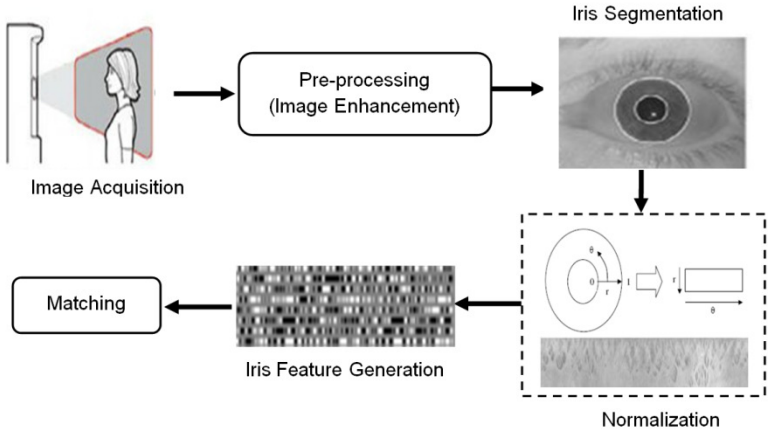


Fig. 3. Iris Image Processing Steps.

Li and Savvides (2013) proposed a FJ-GMMs (Gaussian Mixture Models) for distributions of the regions on iris to estimate strong obstacle. In this proposed work, GFB (Gabor Filter Bank) descriptors is used to obtain the most sophisticated features of the images [16]. Simulated Annealing optimization method is used to optimize GFB attributes to design strong recognition system of iris. Obtained results concluded that given algorithm improve the rate of iris recognition for the dataset UBIRIS and ICE. The optimization of the GFB parameters, expressions to formulate feature set of visual features, calculating the computational efficiency of the Gaussian function and iris masks are the important research of this article.

3. Segmentation: Before pre-processing the iris image, the segmentation is applied, because it finds the effective region of the iris image to process subsequently for feature extraction. The segmentation process is very essential component of any iris based systems. The iris segmentation is a composition of the following methods [15, 18]:

(a) Finding iris boundary: To calculation the boundary of iris image, the canny algorithm is one which is used to create the edge maps from an iris image. To calculate the correct boundaries of iris and pupil, Hough Transformation is used.

– Canny method of edge detection: The canny edge detection method is firstly proposed John F. Canny in 1986. To extract possible rang of edges in images canny method is employed with its multi-stage algorithms. It starts by applying the linear filter function for calculating the gradient using image intensity. This process is stopped by calculating the thresholding and thinning of the edges. The canny edge detection method can also be applied for noisy images, as this method merge the poor edges with the massy edges if these poor edges are belong to those of massy edges. Therefore canny edge detection is very feasible method as compared with other method of edge detection in the case of noisy images [11].

– Hough Transformation: The earlier developed Hough transformation was used to extract the unique lines from any image. The enhanced version of Hough transformation has been extended to find location of shapes as well in the images. After the edge map found, the parameters of the circles passing through each edge point in Hough space is obtained. These obtained parameters are used as the coordinates (x, y) of the

Centre and the radius r of the iris. These parameters are also used to determine any circle using the following formula [15]:

$$x^2 + y^2 = r^2 \quad (1)$$

The coordinates of centre and radius of the circle are greatly described in the Hough space by using edge points.

(b) Noise Removal: Separation of Eyelashes and Eyelids from iris: In iris images, the upper and lower regions iris are overlapped by the upper eyelashes and upper-lower eyelids. During capturing iris image, the specular reflections can be existed in the iris region, those can weak the quality of iris texture. The removal of such deficiencies and noises from the image is very important to finding actual and reliable iris features, before processing the recognition algorithm [17].

– In iris images, the eyelashes are dark in color in comparison with eyelid. Hence, to eliminate eyelashes, the thresholding is used.

– In iris images, the Eyelids can be removed by using linear Hough transform and fitting a line to the upper boundary and lower boundary of the eyelid. A new horizontal line is drawn, that will intersect to first line at the iris edge that will be nearby to the pupil.

4. Iris Normalization: After the iris image pre-processing and Segmentation, the transformation is applied, which will generate a rectangular image of fixed sized. The famous Daugman's Rubber Sheet Model is used for this transformation process [12, 18].

Daugman's Rubber Sheet Model: In Normalization of iris image, a circular iris image is unwrapped first and then transformed into its polar equivalent.

In an iris image, every pixel is equivalent to a position which is found out on polar axes. This method consist two resolutions: the first is Angular, which shows number of radial lines in the iris and the second is Radial, which shows number of data points in radial direction. The iris region is converted into 2D array with horizontal dimensions and vertical dimension of angular resolution and radial resolution respectively using the following expression.

$$I[x(r,\ \theta), y(r,\ \theta)] \rightarrow I(r,\ \theta) \quad (2)$$

where $I(x, y)$ represents region of the iris, $(x,\ y)$ is the Cartesian coordinates and (r, θ) is the normalized polar coordinates. The limit of θ and r is [0, 2π] and [0 1] respectively. The values of $x(r, \theta)$ and $y(r, \theta)$ are linear combinations set of pupil boundary points. The transformation is performed by using the following equations:

$$x(r, \theta) = (1 - r)x_p(\theta) + x_i(\theta) \quad (3)$$

$$y(r, \theta) = (1 - r)y_p(\theta) + y_i(\theta) \quad (4)$$

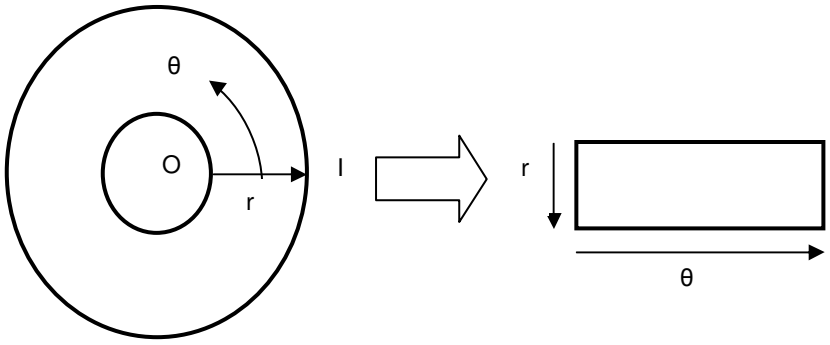
$$x_p(\theta) = x_{p0}(\theta) + r_p\cos(\theta) \quad (5)$$

$$y_p(\theta) = y_{p0}(\theta) + r_p\sin(\theta) \quad (6)$$

$$x_i(\theta) = x_{i0}(\theta) + r_i\cos(\theta) \quad (7)$$

$$y_i(\theta) = y_{i0}(\theta) + r_i\sin(\theta) \quad (8)$$

Where the values of (x_p, y_p) and (x_i, y_i) represent the coordinates on the boundaries of pupil and iris along the θ direction. The values of (x_{p0}, y_{p0}) and (x_{i0}, y_{i0}) represent the center's coordinates of pupil and iris [15].



(a) Daugman's Rubber Sheet Model.

(b) Normalized iris.

Fig. 4.

5. Texture Extraction of the iris: Texture of an image is a feature pattern of information with a random intervals. The textures generally refers as features appeared on the surface of any image. Texture feature pattern can be retrieve using some methods, those methods are known as statistical, structural, transform and model based methods.

Gabor decomposition method is a transform based, used very frequently to extract the feature of an image. In this method, the 2D normalized image is transformed into 1D signals, then these 1D signals are curl with 1D Gabor wavelets. The Log-Gabor filter gives the frequency response by following equation:

$$G(f) = \exp\left[\frac{-(\log(f/f_0))^2}{2(\log(\sigma/f_0))^2}\right] \quad (9)$$

Where f_0 and σ represents the centre frequency and bandwidth of the filter respectively. The output of the Log-Gabor filter is the biometric texture feature of the iris image [17].

Introduction to Fingerprint Techniques: The identification of an individual personal using Fingerprints is a tradition method which have been developed hundreds of years ago. The fingerprint technology was first used by the Law enforcement agency to recognize criminals. They made a Dataset of fingerprints by collecting fingerprints of each criminal in late nineteenth century. At that time fingerprint recognition is done manually, therefore this process was very time taken. Now a days, fingerprint technology has been revolved to fulfill the requirements of general applications, which may be apart from former criminal use in many aspects [19].

In Fingerprint recognition system, an algorithm is used to compare two finger images, both the images may vary in quality and orientation, to find whether these images from the identical person's finger. In this comparison the fingerprint features known as minutiae compare. If a necessary number of feature are match then it is found that two fingerprint images are same.

B. The Fingerprint based Biometric-system

This section describes all the steps to find the features points called the minutiae points of a fingerprint. A fingerprint image is consists a unique texture of ridges and valleys. The ridges terminals and ridges bifurcations are the minutiae points. These minutiae points provides significant information to fingerprint based recognition system [20, 29]. The minutiae points are extracted by the following steps:

1. Acquisition of Fingerprint image: Fingerprint image is acquired with acquisition device. In Fig. 5, an image of a device shown which is used to capture finger image. These devices consist a light source, lenses, a digital camera, and a prism where the fingertip is put. The user have to put fingertips on the dark area of the sensor, where the prism is located. A digital image is created using this device, which is saved in system storage for further processes [21].

Fig. 5. Finger image capturing device (SecuGen Hamster Pro Duo SC/PIV [48]).

2. Preprocessing: The preprocessing is required when the input image has any kind of noise, it enhances the quality of fingerprint image so that algorithms for minutiae extraction can perform efficiently. The following are fingerprint image enhancement techniques [22]:

– Histogram Equalization
– Wiener Filtering
– Gaussian Low-Pass Filter
– Gabor Filter.

(i) Histogram Equalization (HE): The basic technique to improve the contrast quality of the images is the Histogram equalization. The concept of HE technique is to map gray levels using distribution probability of the input gray levels [20]. The intensity values of pixels are transformed by the following equation:

$$s_k = T(r_k) = \sum_{j=1}^{k} P_r(r_j) = \sum_{j=1}^{k} \frac{n_j}{n} \quad (10)$$

where s_k, represents intensity value of the image after processing, which is correspond to the intensity value r_k of the input image and $P_r(r_j) = 1,2,3 \ldots \ldots L$ that represents intensity level of input fingerprint image [21].

(ii) Wiener filtering: Wiener filtering is applied to increase the lucidity of fingerprint such that the structure of the finger ridges remain constant. This filter uses the statistics estimated methods. The local neighborhood η is of size 3 × 3 for each pixel. This filter is represented by the following expression:

$$w(n_1, n_2) = \mu + \frac{\sigma^2 - v^2}{\sigma^2}(I(n_1, n_2) - \mu) \quad (11)$$

where v^2 represents noise variance, μ shows the local mean and σ^2 shows the variance and the I shows the gray level intensity values such that $n_1, n_2 \in \eta$ [23].

(iii) Gaussian Low-Pass Filter: This filter is applied to blur the image. In this process, the `weighted-average' is created for all neighborhood each pixel. The average weighted is more near to the value of central pixels. The edge preserving and gentler smoothing is obtained using this process. The 2-D distribution is used by the Gaussian filter as a point-spread function that is given as [24].

$$G(x, y) = \left[\frac{1}{2\pi\sigma}\right]^2 \exp\left\{\frac{(x^2+y^2)}{2\sigma^2}\right\} \quad (12)$$

Where, σ represents the distribution's standard deviation.

(iv) Gabor Filter (GF): The most common contextual filter used to improve the quality of fingerprint image, is the GF. This filter consists orientation-selective and frequency-selective properties of the objects. Therefore they have optimal joint resolution in both frequency and spatial domains. The 2-D Gabor filter is shown by the following equation [25].

$$G(x, y, \theta, f_0) = \exp\left\{-\frac{1}{2}\left[\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right]\right\}\cos(2\pi f_0 x_\theta) \quad (13)$$

$$\begin{bmatrix} x_\theta \\ y_\theta \end{bmatrix} = \begin{bmatrix} \sin\theta & \cos\theta \\ -\cos\theta & \sin\theta \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \quad (14)$$

Where f_0 represents ridge frequency, θ represents orientation of the filter, x_θ and y_θ are the value of x and y coordinates after (90º - θ) clockwise rotation of the Cartesian-axes, the σ_x and σ_y represents the value of standard deviation with respect to *x*-axis and *y*-axis of the Gaussian envelope.

3. Estimation of Orientation Field of fingerprint image: The fingerprint orientation field estimation defines the local orientation field of valley and ridges. The gradients of gray intensity provides the most reliable ridge orientation. In this method, the gradient vectors

$[g_x, g_y]^T$ are derived by computing partial derivatives of each pixel intensity. In Conventional gradient method, the input images are divided into blocks of same size i.e. $N \times N$ pixels. Then calculate the average of each block. The formula to calculate the Orientation field direction of a block is as follows [19, 20].

$$\theta_B = \frac{1}{2} a\tan\left[\frac{\sum_{i=1}^{N}\sum_{j=1}^{N} 2g_x(i,j)g_y(i,j)}{\sum_{i=1}^{N}\sum_{j=1}^{N} g_x^2(i,j)g_y^2(i,j)}\right] + \frac{\pi}{2} \quad (15)$$

where function $a\tan(...)$ provides value of an angle of limit (-π, π) which is corresponded to squared gradients, and θ_B represents the required orientation angle of range [0, π].

4. Fingerprint image Minutiae extraction: The unique features-points of a Fingerprint are known as the minutiae point, these points are necessary to process the fingerprint image in the biometric recognition system. The minutiae point extraction process involves the Binarization and Morphological Operators.

The grey scale images are converted into a binary image using this Binarization technique. This technique is used to enrich the contrast quality of the ridges and valleys of the fingerprint, so that features points can be retrieved easily. In binarization process, the grey scale values of pixels in the enhanced image are processed, i.e. if grey scale values are higher than the global threshold value, then the values of such pixels are set to a binary value 1; or else, these are set to binary value 0. This produced binary images contain information of the background valleys and foreground ridges. This binary image is helpful for minutiae extraction methods, in this case only two interests are there: one is the white pixels that shows the valleys and second is the black pixels that shows the ridges.

The Morphological Operations follows the binarization methods, in terms these operators are used on the binary fingerprint images. The morphological techniques eliminate noise from the erroneous images. This operator removes the unwanted line breaks, bridges and spurs from the fingerprint image as well as the redundant pixels values until the ridges become one-pixel wide. This is known as thinning of the ridges [19, 26].

IV. THE BIOCRYPTO-SYSTEM

The Biocrypto-Systems (BSs) are implemented to retrieve or generate secret-key for encryption using the stored biometric depended information of the user. This stored information is known as helper data. Due to variability properties of the biometric it is not possible extract keys directly using the biometric characteristics. In this case, Helper data, which is generated using biometric templates, helps to retrieve the key. BSs are used to protect biometric-template, as well as to bind and retrieve information. The Biocrypto-System is also work in two enrollment and authentication or verification phase as in Biometric-system [6, 31].

BS in enrollment takes biometric traits as input and securely bind or generate cryptography key. At the end of enrollment phase it produces a public information known as helper data for storage either local or remote system. At the time of Authentication or verification phase, BS takes the live biometric from the user and helper data to successfully retrieve or generate key. Widely used BSs are shown in Fig. 6.

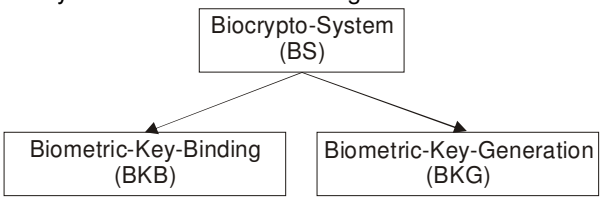


Fig. 6. Classification of BS.

A. Biometric Key- Binding (BKB)

In BKB system, a cryptographic secret key provided by the user and user's biometric featured data are combined using some binding algorithms in enrollment phase and retrieve same key whenbiometric input is provided by the same user otherwise mismatch massage is shown in verification phase, Fig. 7.

B. Biometric Key-Generation (BKG)

BKG scheme is applied to directly extract cryptographic key from biometric traits. In this a biometric image is taken as input during enrollment phase, process it and extract strong biometric features then quantized to obtain binary key.

This extracted features transformed and stored as helper data which is used in authentication phase. In authentication phase, live biometric input taken from the candidate and process it like enrollment phase and extract features. Stored helper data and extracted features are used to generate same key if the input is taken from the legitimate candidate, Fig. 8.

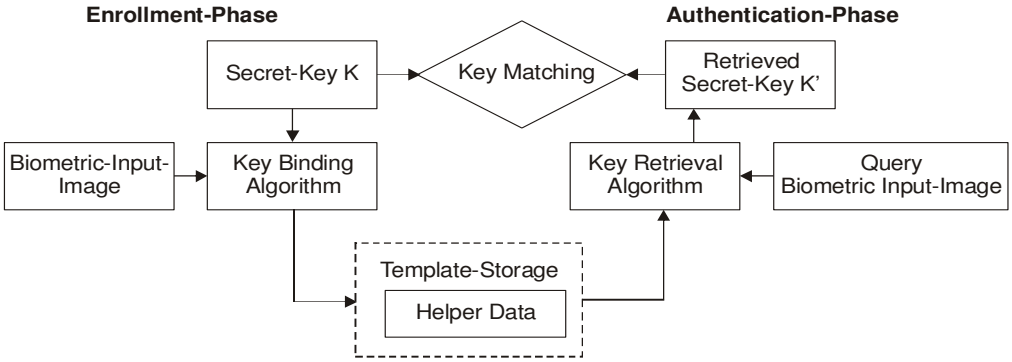


Fig. 7. Biometric Key-Binding.

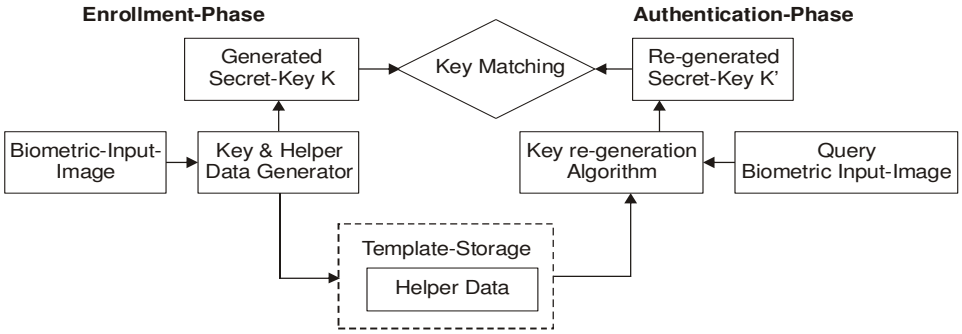


Fig. 8. Biometric Key-Generation.

C. Helper-Data (h_data)

In the BCSs the storage of biometric dependent information is required. This information is required to recover or re-generate keys again, and known as *h_data*. The *h_data*, must not consists substantial data of original biometric, helps to reconstruct the keys. Biometric template is represented as either a set of characteristics or a binary-string [28, 31].

Two ways to generate Helper Data for BKB and BKG schemes:

(i) In BKB schemes: The *h_data* is generated using fusion-techniques on biometric-template and cryptographic secret-key in binding process and stored in database. By using key-retrieval algorithm, the keys can be again generated with the use of *h_data* at authentication-phase. In this, cryptographic-secret-key keeps free from biometric features because such biometric features are revocable while the secret-keys usually require to be updated in this case re-enrollment is performed to generate new *h_data*.

(ii) In BKG schemes: In this, only biometric template is used to create the Helper data, and then keys can be generated directly by using the *h_data* and a input biometric. Such *h_data* based key-generation methods are known as "secure sketches" and "fuzzy extractors".

D. Performance Evaluation Parameters

When the biometric authentication is used, the degree of security is concerned. Many types of biometric recognition method are available, therefore there are some parameters used to evaluate these available methods and determines strength of these method. Using these parameters the performance of any biometric recognition method can be measured. These parameters can be described as [30].

FAR or FMR: This shows that the biometric recognition method incorrectly make successful match of input-features to the non-matching features in the dataset. The rate of invalid matches is given as:

$$\text{FAR} = \frac{\text{No. of successful matches by impersonator}}{\text{Total no. of matches by impersonator}}$$

FRR or FNMR: This shows that the biometric recognition method incorrectly makes failure of match of the input feature to the matching template feature in the dataset. It gives the rate of legal inputs being rejected.

$$\text{FRR} = \frac{\text{No. of failed matches by legitimate user}}{\text{Total no. of matches by impersonator}}$$

In biocrypto-system, biometric key-binding scheme is very commonly and widely used for cryptographic-key security whereas biometric key-generation scheme is rarely used. In this survey paper, the further discussion is made mainly about biometric key-binding system.

V. BIOMETRIC KEY-BINDING

Biometric key-binding system bind a cryptography key to biometric data extracted from user biometric images. The two techniques Fuzzy Vault and Fuzzy Commitment are common used in key-Binding approach.

The following Approaches are used for biometric key-binding:

1. Mytec1 and 2: The Mytec1 is first developed method for key-binding, but this method was not strengthen in the security and accuracy. This method was developed using fingerprints image [6]. The Mytec1 was enhanced and developed as Mytec2. Mytec1 and 2 are known as Biometric Encryption™. The function of correlation is the main functional part of the Mytec2 (and Mytec1).

In the enrollment-phase of this approach, by using the degree of similarity between an input image $f_1(x)$ and another image $f_0(x)$, a filter function $H(u)$ is determined. This function is 2-D image array. The correlation function $c(x)$ is of $f_0(x)$ and another input-biometric $f_1(x)$ is determined in the authentication-phase, can be given as:

$$c(x) = FT^{-1}\{F_1(u)F_0^*(u)\} \quad (16)$$

Where $c(x)$ is the product of inverse Fourier transform $F_1(u)$ and $F_0^*(u)$, where $F_1(u)$ represents FT of input- biometric image and $H(u)$ represents $F_0^*(u)$.

The output $c(x)$ in stage E-1 as shown in Fig. 9, is an array that contains values of similarity degree. A set of T training images $\{f_0^1(x),\ f_0^2(x),..,f_0^T(x)\}$ are used to find the filter function. The $c_0^t(x)$ is output pattern of $f_0^t(x)$ with its FT of $F_0^t(u)H(u)$. The $e^{i\Phi}(H(u))$ is a phase

component of $H(u)$. To create a secure filter, $H_{stored}(u)$, the $e^{i\Phi}(H(u))$ is multiplied by a random phase.

The $c_0(x)$ in stage E-2, is then linked using a linking algorithm with cryptographic key k_0 of N-bits. It checks the n^{th} bit of k_0 if it is 0 then L no. of locations of the $c_0(x)$ which are 0 then selected and the entry is made into look-up table's n^{th} column with the indices of the locations and stored as the part of the template, which is known as BioScrypt.

The redundancy is added when linking is performed by using repetitive code. The hash of k_0 is determined as id_0 and stored as part of template.

In verification phase, a set of input biometric images are processed with $H_{stored}(u)$ and create $c_1(x)$ pattern. After that, $c_1(x)$ and the values of look-up table are applied to retrieval method to compute key k_1 of N-bits. A hash value id_1 is computed and compare with id_0 to validate k_1.

2. Fuzzy Commitment (FC): The fuzzy commitment method was developed by Juels and Wattenberg [33]. This method uses the binary biometric secrecy system to protect secret keys. This method employs standard Reed-Solomon error-correcting codes.

The template protection techniques are generally used the fuzzy commitment method which is based on key-binding to or key-extracting from, a biometric sample.

Working of FC scheme:

– An arbitrary code-word c is taken from a set of ECC, C, that have codes which can be used to correct t-bits of error.

– The Exclusive-OR operation performed between values of x and the code-word c. The $x \oplus c$ will the result.

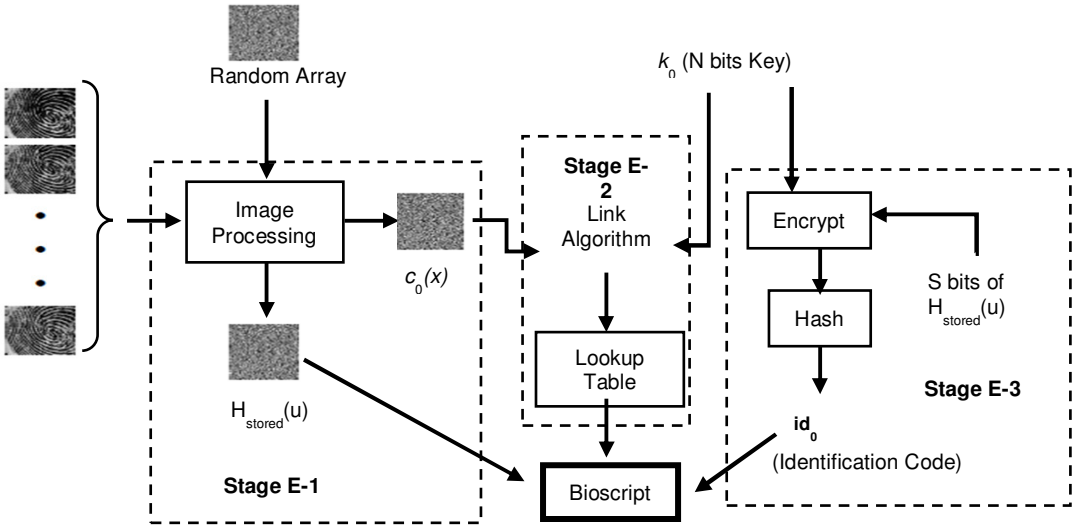


Fig. 9. Enrollment Process for Biometric Key-Binding [6].

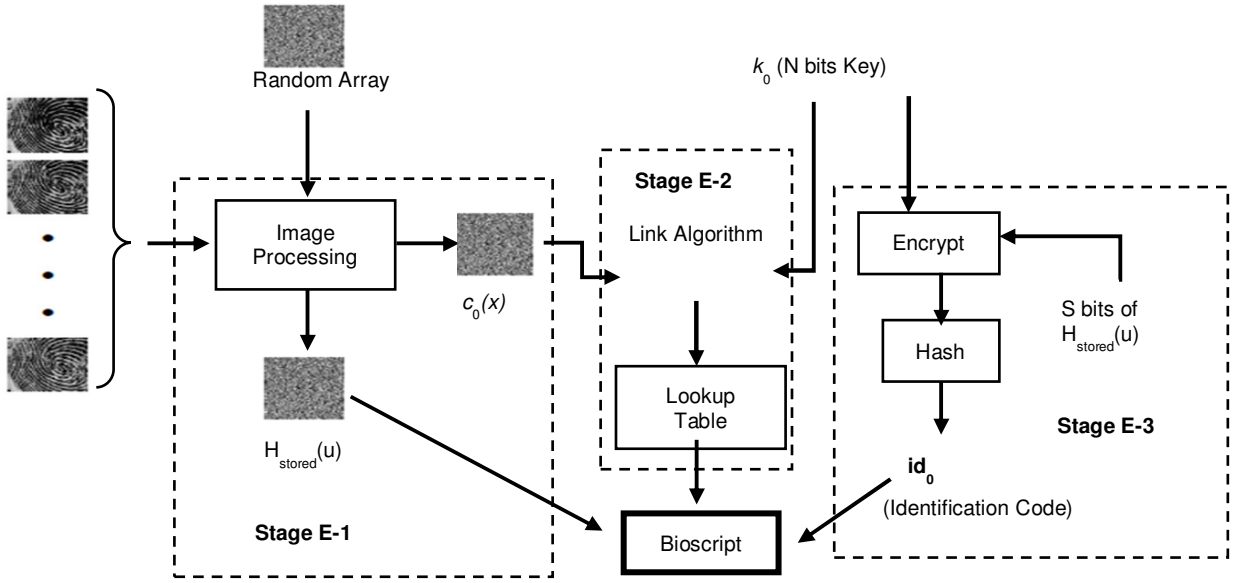


Fig. 10. Verification Process for Biometric Key-Binding [6].

– The code-word *c* is hashed to produce *H*(*c*). The values of *c* and *x* will be deleted from the records, only the value of $c \oplus x$ and H(*c*) saved in database as the helper data or Commitment.
– In verification, user enters *x'* to this method, which will compute $x' \oplus x \oplus c$. If the value of *x'* is not different from *x* by more than t-bits, then $x' \oplus x \oplus c$ can be rectified to find *c* again. For the verification, the Hash of corrected $x' \oplus x \oplus c$ is calculated and compared with the stored H(*c*).

3. Fuzzy Vault (FV): FV is very standard BCs, which was developed in 2002 by the Juels and Sudan [34]. This scheme is designed to protect a cryptographic-key by securely bind it with fingerprint Biometric data [35].

The FV method secure the secret data using the biometric information thereby only the legitimate person will be able to retrieve original data bound in encoding-phase by using their actual biometric data i.e. fingerprint data. In FV, the vault is generated in encoding phase by using polynomial based encoding method with ECC [27]. The secret-key is used as the coefficients values of the polynomial in order to secure this. Some random generated points known as the chaff points, not in the set of polynomial-points, are merged with vault in order to secure original-points (Fig. 12).

To retrieve the secret-key in decoding phase, a live biometric template is produced using the live biometric. Firstly the genuine points extracted from the vault using actual biometric and ECC then regenerates the polynomial equation. After recreating polynomial coefficients are extracted which represents the secret-key (Fig. 13).

The Chaff Point (CF): The chaff points provide the security to the genuine point in the generated Vault Template of FV method so that the genuine point cannot be extracted easy by the attackers from the vault. The chaff points must be created thereby no one can distinguishable it from genuine points. Therefore, the chaff points generation method should be more accurate so that no chaff point overlaps the genuine points or not on the *P(x).*

The first chaff generation method was proposed by the Juels and Sudan in FV method [34]. The coordinate's values of each minutiae point were taken to compute the coordinates of chaff points in the following two way:
(i) The x-coordinate of the newly generated chaff points should not be equal to genuine point's x-coordinate and the existing chaff point's x-coordinate (ii) The y-coordinate of the newly generated chaff points should not be on the polynomial P(x).

Clancy *et al.*, [32] proposed a well-known chaff generation technique based on distance. In this scheme, the distance among the newly created chaff points, genuine points and other existing chaff points must be greater than a defined threshold value. In Clancy's technique, the Euclidian distance is calculated among the newly created chaff points, genuine points and other existing chaff points to find its fitness to be chaff point.

Working of Key-Binding in FV: In Key binding phase [36, 37]. A cryptographic secret key $K=\{k_i\}^{n}_{i=1}$ of length n-bits is bound with biometric information using any ECC method and produced q-bits ECC. This q-bits ECC is affixed with the secret key at the end to produce K' of (n+q)-bits. A polynomial is constructed using this (n+q)-bits K'. The secret K' is divided into (m+1) values to form a polynomial *P* with degree of m, the secret is bound as the coefficients of this polynomial *P* such as $(c_0, c_1, c_2 \ldots c_m)$ that is $P(x)= c^m x_m + \ldots\ldots + c^0$. The minutiae points of the user's fingerprint are used to secure the secret. As long as the $(m+1)$ minutiae points are found the secret K' can be recreated using the generated fuzzy vault.

In next of this process, genuine points set *G* is generated. The set of minutiae points is $Z=\{a_i\}^{r}_{i=1}$ where r is the number of genuine point. These r genuine minutiae point are well separated by a minimum threshold distance between two minutiae points. Now the set *Z* is treated as the x-coordinates. The elements of *Z* are used to evaluate polynomial *P* and construct a polynomial to find the genuine points set *G* where $G=\{a_i, P(a_i)\}^{r}_{i=1}$.

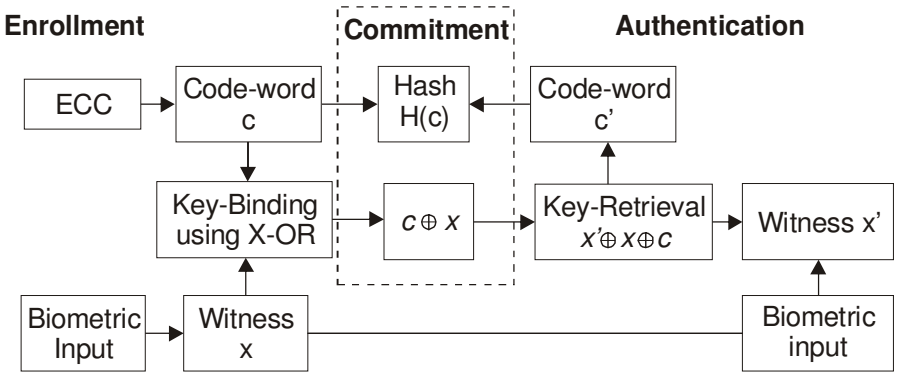


Fig. 11. Fuzzy Commitment Scheme.

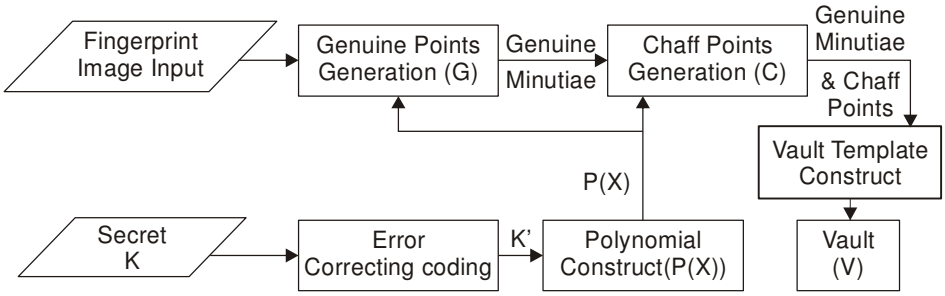


Fig. 12. FV Encoding Phase.

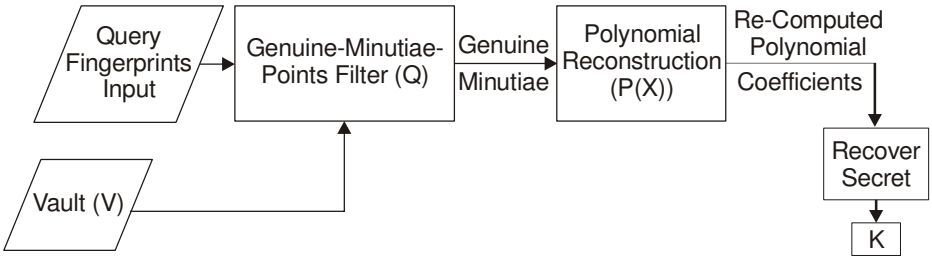


Fig. 13. FV Decoding Phase.

Table 1: Comparison of Biometric-crypto system for Key-Binding.

Author	BCS Method	Biometric Trait	Key-Size (bits)	FAR/FMR (%)	FRR/FNMR (%)
Jain *et al.*, (2008) [38]	Fuzzy Vault	Fingerprint	112	0.13	9
			128	0.01	9
			160	0	14
Li *et al.*, (2010) [39]	Fuzzy Vault	Fingerprint	14 (Degree of polynomial	0	12
Marino *et al.*, (2012) [40]	fuzzy Extractor	Iris	192	4.42	9.67
Eskander *et al.*,(2014) [41]	Fuzzy Vault	offline signature	192	1.41	20.68
Amirthalingam and Radhamani (2016) [42]	Fuzzy Vault with PSO	Multi model- Face and Ear	10	10	10
Adamovic *et al.*, (2017) [43]	Fuzzy Commitment	Iris	400	0	3.75
			300	0	2.21
			200	0	1.26
Yang *et al.*, (2018) [44]	Cancelable biometric system (Fuzzy Commitment)	Face	15	0	13
			29	0	16
			36	0	35
			64	0	59
Chitraand Sujitha (2018) [45]	Fuzzy Vault	Fingerprint	8 (Digit)	0.72	11
			9 (Digit)	0.51	16
			10 (Digit)	0.04	17
			11 (Digit)	0.01	22
			12 (Digit)	0.01	25
Elrefaei and Al-Mohammadi (2019) [46]	Fuzzy Commitment	Gait	50-bits	0 (fast walk)	0 (fast walk)
			64-bits	0 (slow walk)	4 (slow walk)
			45-bits	0 (45-degree)	0 (45-degree)
Ponce-Hernandez *et al.*, (2020) [47]	Fuzzy Vault	Signature	128-bits	MCYT database	
				6.91	7.85
				Proprietary database	
				6.21	4.86
				BioSecure database	
				6.16	13.6

Now, a set of random points *s* are generated, then a subset *C* of set *s*, known as chaff points, is chosen from *s* points thus not overlapping polynomial $P(x)$, this set of chaff points *C* protects the cryptographic secret key. This subset cab be represented as $C=\{c_j, h_i\}^s_{j=1}$ where $y_i \neq P(c_i)$, $j \in [1,\ldots\ldots, s]$.

The vault template is generated finally such that, $V'=\{xi, yi\}^{r+s}_{i=1}$, by merging chaff points C with genuine points G. The *V'* is now scrambled, and produced *V* as the final FV.

Working of Key Retrieving in FV: In the key retrieving or decoding phase, the vault *V* has to be unlock by the

user using his live query fingerprint. The query fingerprint image processed and query minutiae points are extracted and represented as field elements, $B=\{b_j\}^{t}_{j=1}$, where $b_j \in$ F. For every b_j minutiae point the vault set V is searched and find an element such that, ($b_j=xi$) and projection point on $P(x)$, $Y=\{b_l, P(b_l)\}^{t'}_{l=1}$ corresponding to it. The n-order polynomial P can be recreated by applying the Lagrange interpolation method if and only if set Y consists (n+1) elements. After successfully reconstruction of polynomial, the coefficients can be found which represent the secret K.

VI. KEY-BINDING COMPARISON

Table 1 give the comparison of different key-binding techniques by different authors using fuzzy vault, fuzzy extractor and fuzzy commitment on different biometric images. The comparison parameters are the key size to be bound and FAR and FRR.

VII. CONCLUSION

As many authors' worked for biometric key-binding biocrypto-system for improving the security of cryptographic algorithms. In this study, several authors worked for key-binding system using different methods like fuzzy commitment, fuzzy vault etc. for many biometric traits. These system work for altered secret-key size. These algorithms show altered results in terms of FAR and FRR parameters for changed Dataset and biometric Data. Many authors' works towards achieved FAR 0% that improved FRR. The performance of any biocrypto-system will be better if these show the low rate of FAR, FRR is high and Key value is low. If the key size will increase then it may increase FAR and FRR. The outcomes of this review are as follows: to enhance the strength and security of any symmetric cryptography system, increase its secret-key size, but increasing the secret-key size may reduce the performance of biocrypto-system. Therefore, there is a need of developing such Biocrypto-systems of Key-Binding which much be able to bind the large key as well as retrieve the same key efficiently.

VIII. FUTURE SCOPE

In this proposed survey, different biometric key-binding method are explored with its working. The authors also discuss the working of biocrypto-system with various biometric modalities in detail.

All the key-binding methods are analyzed using biometric performance parameters, secret-key size and various biometric traits. As it can be seen that in some cases, when the key size is increasing the performance of biocrypto-system is reducing accordingly. Therefore, the new authors can develop a new efficient biocrypto-system which will be able to bind large secret key as well as retrieve without altering it. This work may assist to enhance the efficiency of Biocrypto-systems.

ACKNOWLEDGEMENTS

In this article, the study different biometric key-binding biocrypto-system has been accomplished with the knowledge full support of my supervisor who contributed to the preparation and completion of this paper. I would like to express my profound thanks to my superiors for their enthusiastic guidance, continuous support and kind encouragement throughout the whole period of my study.

Conflict of Interest. The authors declare no conflict of interest associated with this work.

REFERENCES

[1]. Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. *IEEE transactions on circuits and systems for video technology*, *14*(1), 4-20.

[2]. Uludag, U., Pankanti, S., Prabhakar, S. & Jain, A. K. (2004). Biometric Cryptosystems: Issues and Challenges. *Proceedings of the IEEE*, *92*(6), 948-960.

[3]. Dong, J.,& Tan, T. (2008). Security Enhancement of Biometrics, Cryptography and Data Hiding by Their Combinations. *5th International Conference on Visual Information Engineering (VIE 2008), Xian China, IET,* 239-244.

[4]. Hao, F., Anderson, R., & Daugman, J. (2006). Combining Crypto with Biometrics Effectively. *IEEE transactions on computers*, *55*(9), 1081-1088.

[5]. Kim, Y.,& Kim, J. F. (2007). U-City User Authentication Methods and Encryption Techniques Based on Biometric Technology. The *Convergence of Bioscience and Information Technologies*, 695-697.

[6]. Soutar, C., Roberge, D., Stoianov, A., Gilroy, R.,& Kumar, B.V.K. V. (1999). Biometric Encryption. chapter 22 in ICSA Guide to Cryptography, *McGraw-Hill*, 1-28

[7]. Jin, Z., Teoh, A. B. J., Goi, B.M., & Tay, Y. H. (2016). Biometric cryptosystems: A new biometric key-binding and its implementation for fingerprint minutiae-based representation. *Elsevier Journal Pattern Recognition,16*, 50-62.

[8]. Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancellable biometrics. *EURASIP Journal on Information Security, Springer*, *3*, 1-25.

[9]. Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An Introduction to Biometric. *Biometric Systems Technology, Design and performance evaluation,* 1-20.

[10]. Malek, O., Venetsanopoulos, A., Androutsos, D., & Zao, L. (2015). Sequential Subspace Estimator for biometric authentication. *Elsevier Neuro computing, 148,* 294-309.

[11]. Al-Waisy, A. S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., & Nagem, T. A. M. (2017). A multi-biometric iris recognition system based on a deep learning approach. *Pattern Analysis and Applications, Springer, 21***,** 783-802.

[12]. Subban, R., Susitha, N., & Mankame, D. P. (2017). Efficient iris recognition using Haralick features based extraction and fuzzy particle swarm optimization. *Cluster Computing*, *21*(1), 79-90.

[13]. Zonoozi, M. H. P., Jahanshahi, D. A., & Dehaqi, A. M. (2019). Twins' biometric fusion and introducing a new dataset. *5th Conference on Knowledge-Based Engineering and Innovation, Iran University of Science and Technology, Tehran, Iran, IEEE*, 306-310.
[14]. Bowyer, K. W., Hollingsworth, K. P. & Flynn, P. J. (2013). A Survey of Iris Biometrics Research. *Advances in Computer Vision and Pattern Recognition, Springer*: pp. 15-54.
[15]. Daugman, J. (2003). The importance of being random: statistical principles of iris recognition. *Pattern Recogn, 36,* 279-291.
[16]. Li, Y. H., & Savvides, M. (2013). An automatic iris occlusion estimation method based on high-dimensional density estimation. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 35*(4), 784-796.
[17]. Bhattacharyya, D., Das, P., Bandyopadhyay, S. K., & Kim, T. (2008). IRIS Texture Analysis and Feature Extraction for Biometric Pattern Recognition. *International Journal of Database Theory and Application, 1*(1), 53-60.
[18]. Maheswari, S. U., Anbalagan, P., & Priya, T. (2008). Efficient Iris Recognition through Improvement in Iris Segmentation Algorithm. *International Journal on Graphics, Vision and Image Processing*, *8*(2), 29-35.
[19].O'Gorman, L. (1998). An overview of fingerprint verification technologies. *Information Security Technical Report*, *3*(1), 21-32.
[20]. Greenberg, S., Aladjem, M., & Kogan, D. (2002). Fingerprint image enhancement using filtering techniques. *Real-Time Imaging*, *8*(3), 227-236.
[21]. Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., & López-Gutiérrez, R. M. (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications*, *42*(21), 8198-8211.
[22]. Chikkerur, S., Cartwright, A. N., & Govindaraju, V. (2007). Fingerprint enhancement using STFT analysis. *Pattern Recognition, 40(*1), 198-211.
[23]. Sepasian, M., Balachandran, W., & Mares, C. (2008). Image enhancement for fingerprint minutiae-based algorithms using CLAHE, standard deviation analysis and sliding neighborhood. In *Proceedings of the World congress on Engineering and Computer Science*, 1-5.
[24]. Atighehchi, K., Ghammam, L., Barbier, M., & Rosenberger, C. (2019). GREYC-Hashing: Combining biometrics and secret for enhancing the security of protected templates. *Future Generation Computer Systems*, *101*, 819-830.
[25]. Muthukumar, A. & Kavipriya, A. (2019). A biometric system based on Gabor feature extraction with SVM classifier for Finger-Knuckle-Print. *Pattern Recognition Letters, Elsevier, 125,* 150-156.
[26]. Lam, L., Lee, S. W., & Suen, C. Y. (1992). Thinning Methodologies: A Comprehensive Survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *14*(9), 869-885.
[27]. Blanton, M., & Aliasgari, M. (2013). Analysis of Reusability of Secure Sketches and Fuzzy Extractors. *IEEE Transactions on Information Forensics and Security, 8*(9), 1433-1445.
[28]. Lee, Y. J., Park, K. Y, Lee, S. J., Bae, K., & Kim, J. (2008). A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System. *IEEE transactions on systems, man, and cybernetics*, *38*(5), 1302-1313.
[29]. Kumari, P., & Seeja, K. R. (2019). Periocular biometrics: A survey. *Journal of King Saud University – Computer and Information Sciences*, 1-12.
[30]. Hammad, M., Liu, Y., & Wang, K. (2018). Multimodal Biometric Authentication Systems Using Convolution Neural Network based on Different Level Fusion of ECG and Fingerprint. *IEEE Access,* 6, 26527-26542.
[31]. Sadhya, D., Singh, S. K., & Chakraborty, B. (2016). Review of key-binding-based biometric data protection schemes. *IET Biometrics,* 5(4), 263–275.
[32]. Clancy, T. C., Kiyavash N., & Lin, D. J. (2003). Secure smartcard-based fingerprint authentication. *Proc ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop*, 45-52.
[33]. Juels, A., & Wattenberg, M. (1999). A fuzzy commitment scheme. *Sixth ACM Conference on Computer and Communications Security, ACM Press*, 28-36.
[34]. Juels, A., & Sudan, M. (2002). A fuzzy vault scheme. *IEEE Int. Symp. on Information Theory*, 1-7.
[35]. Benhammadi, F., & Bey, K. B. (2014). Password hardened fuzzy vault for fingerprint authentication system. *Elsevier Image and Vision Computing*, *32,* 487-496.
[36]. Al-Tarawneh, M. S., Woo, W.L., & Dlay, S.S. (2008). Fuzzy Vault Crypto Biometric Key Based on Fingerprint Vector Features. *2008 6th International Symposium on Communication Systems, Networks and Digital Signal Processing*, 452-456.
[37]. Dang, T. K., Truong, Q., C., Le, T. T. B., & Truong, H. (2016). Cancellable fuzzy vault with periodic transformation for biometric template protection.*IET Biometrics, 5*(3), 229-235.
[38]. Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. *Hindawi Publishing Corporation, EURASIP Journal on Advances in Signal Processing,* 1-17.
[39]. Li, P., Yang, X., Cao, K., Tao, X., Wang, R., & Tian, J. (2010). An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. *Journal of Network and Computer Applications*, *33*(3), 207-220.
[40]. Marino, R. A., Alvarez, F. H., & Encinas, L. H. (2012). A crypto-biometric scheme based on iris-templates with fuzzy extractors.*Elsevier, Information Sciences, 195,* 91-102.
[41]. Eskander, G. S., Sabourin, R.,& Granger, E. (2014). A bio-cryptographic system based on offline signature images. *Elsevier, Information Sciences, 259,* 170-191.
[42]. Amirthalingam, G., & Radhamani, G. (2016). New chaff point based fuzzy vault for multimodal biometric cryptosystem using particle swarm optimization.

Elsevier Journal of King Saud University-Computer and Information Sciences, *28*, 381-394.
[43]. Adamovic, S., Milosavljevic, M., Veinovic, M., Sarac, M., & Jevremovic, A. (2017). Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. *IET Biometrics*, *6*(2), 89-96.
[44]. Yang, W., Wang, S., Zheng, G., Chaudhry, J., & Valli, C. (2018). ECB4CI: an enhanced cancelable biometric system for securing critical infrastructures. *Springer Science and Business Media, LLC*, *74*, 4893–4909.
[45]. Chitra, D., & Sujitha, V. (2018). Security analysis of prealigned fingerprint template using fuzzy vault scheme. *Cluster Comput, 22*, 12817–12825.
[46]. Elrefaei, L. A., & Al-Mohammadi, A. M. (2019). Machine vision gait-based biometric cryptosystem using a fuzzy commitment scheme. *Journal of King Saud University, Computer and Information Sciences,* 1-14.
[47]. Ponce-Hernandez, W., Blanco-Gonzalo, R., Liu-Jimenez, J., & Sanchez-Reillo, R. (2020). Fuzzy Vault Scheme Based on Fixed-Length Templates Applied to Dynamic Signature Verification. *IEEE Access*, *8*, 11152-11164.
[48]. https://www.fulcrumbiometrics.com/Biometric-Fingerprint-Scanners-s.

How to cite this article: Tantubay, Neeraj and Bharti, Jyoti (2020). A Survey of Biometric Key-Binding Biocrypto-System using different Techniques. *International Journal on Emerging Technologies*, *11*(1): 421–432.