International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Integrated Framework for Anonymous Biometric Key Based Identity Management System

P Suresh, Radhika K R

Abstract-: ***Implementation of measures to ensure security of transactions while ensuring privacy of user credentials is an area of challenge in digital transactions over a network. Integration of biometric pattern matching into an identity management system (IMS) enhances security of transactions and improves ease of use. Privacy of users in a biometric based system is improved by using keys generated directly from feature sets instead of conventional stored templates. This paper proposes a framework for integrating biometric key based authentication into an IMS.The generated keys need to be long, reproducible with high integrity and need to possess sufficient entropy. Generation of keys directly from feature traits poses a challenge due to intra and inter user variations inherent to biometric data. A novel methodology for generating and integrating crytpo keys into an identity management system is proposed. The keys have been extracted from iris trait. 300 bits keys have been extracted from iris datasets. The results are promising and can be extended to multi-modal biometric feature sets.***

Keywords - Identity management system, user privacy, consistent keys, clustering.

I. INTRODUCTION

The rapid growth of internet has resulted in an exponential increase to on-line services. Amalgamation of ubiquitous wireless technology with smart mobile devices has ensured that internet is no longer limited to traditional web browsing and mail exchanges. Services such as e-commerce, ticketing, sharing of multimedia photos and videos, social networking etc have become pervasive in nature. Access to services requires users to establish a digital identity and get authenticated as a pre-requisite to being issued with authorised credentials. Identity recognition is an intuitive task to humans, while on the other hand there are significant challenges in automating the process using a machine. Users get identified in the digital world by submitting tokens that the subject possesses or a phrase or set of numbers that are known to the subject or by verifying the features (physiological or behavioural) of the subject, termed as biometrics. Users are issued with credentials on successful identification. These credentials are submitted to resolve the identity of users and access authorised service. Digital identities could be passwords, smartcards, certificates, tokens, biometrics or a combination of these. The increased number of on-line services pose a challenge to effective management of digital identities and credential management.

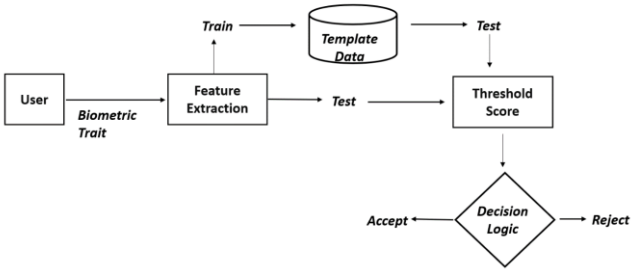

Fig 1. Biometric Authentication System

Identity Management Systems (IMS) support management of users, their identities, attributes and credentials. Proliferation of on-line services has increased the requirement of secure and efficient IMS. The key elements of a networked and centralised IMS are the end user, Service Provider (SP) and the Identity Provider (IdP). Users are the entities that avail services fromthe SP after presenting authenticated credentials to the SP. An IdP issues credentials to a user after authenticating the user based on the digital identity produced. The IMS framework ensures that on-line services are provided by SPs to only those users that have been issued valid and updated credentials by a trusted IdP. The protocol for interaction amongst users, IdP and SPs is defined in the IMS. The IMS maps each user of the system to a corresponding unique identity, which in turn defines the privilege and constraints of access control of the user to the system resource. An IMS must support multiple requirements of each element of the system which in some cases might be conflicting in nature. The requirements of various elements of an IMS are: 1) end-user requirement including support for Single Sign On (SSO), security, privacy, mobility and ease of operations; 2) networked operations including trusted identity management, revocable identity, network management, diagnostics and quality of service; 3) SP requirement; 4) administrative and legal requirements. One of the core functions of IMS is user authentication based on the digital identity presented by the end user.

Manuscript published on 30 September 2019
* Correspondence Author
P Suresh*, Research Scholar, BMS College of Engineering, Bangalore, India.
Radhika K R, Professor, Dept. of ISE, BMS College of Engineering, Bangalore, India.

Integration of biometrics as digital identity into the framework of an IMS holds a lot of promise with associated challenges[1][2]. Biometric data uniquely identify a user and authenticate them based on their physical or behaviouraltraits. Biometric systems have been developed based on fingerprints, face recognition, periocular, voice, hand geometry, handwriting, signature, iris, gait or a combination of the traits. Biometric traits, while identifying users uniquely also pose the challenge of intra-user variations.

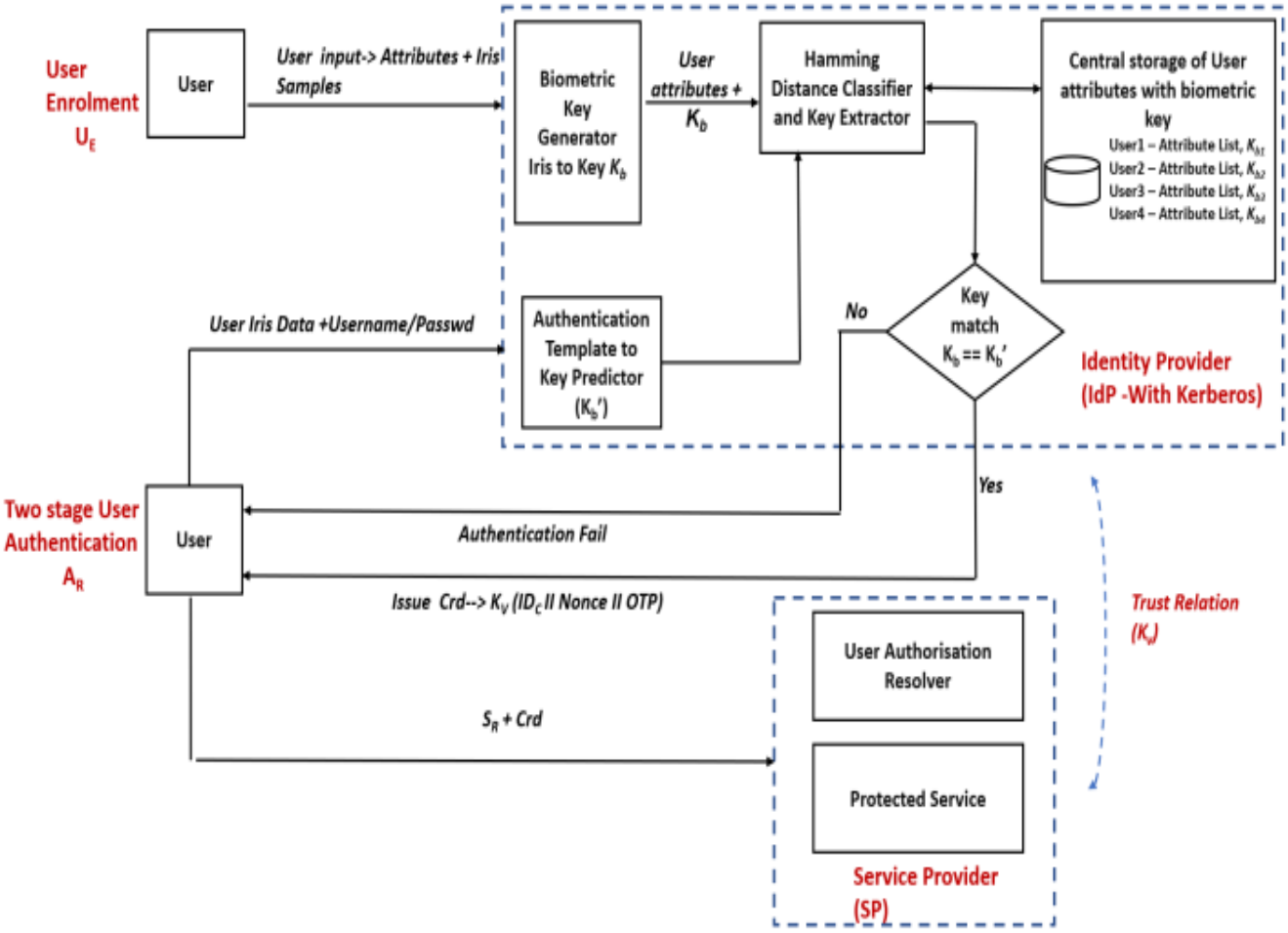

Fig 2. Protocol Flow in IMS

The 'trait data' from a biometric is obtained by sensors and then subjected to analyses in various domains, such as temporal, spatial and spectral domains. Analysis of the data results in meaningful compact representations termed as 'features', with this process being termed as feature extraction. The task of feature extraction is termed as the 'training' phase and is part of the enrolment phase of the system. The extracted features exhibit intra-user variations and are stored as a d-dimensional vector x1,x2,.....,xd. The mean $\bar{x_i}$ is calculated for each component of the d-dimensional feature vector. Each Xi is represented as $Xi=\bar{x_I} + \varepsilon i$, where εirepresents intra-user variations. The intra-user variations occur due to environmental and performance factors of biometric system. Mean values $\{\bar{x_1},\bar{x_2}.....,\bar{x_d}\}$ are stored as reference template corresponding to each user. The biometric template provides a discriminating basis for objectively comparing with other templates in order to determine identity of the user. The parameters from the stored models are recalled to compute the similarity between the 'test' data' presented by the user and the stored models during authentication phase. The 'test' phase includes the feature extraction of the test data followed by computation of similarity between the 'test' feature and the stored data models. A decision is taken in favour of the authentication claim or against it based on a decision logic and threshold. This is accomplished during the identification mode, wherein a template is created for a user and a match is searched for in the database of pre-enrolled templates. In a biometric system, the template storage is a critical point of vulnerability. Unauthorised and malicious tampering of the template database will adversely affect the functioning of the IMS. A critical area of research is the application of cryptographic principles to safeguard the security of templates. The safety of templates can be greatly enhanced by replacing the stored templates with crypto keys representing the biometric feature. The keys must be sufficiently long, consistent and must possess high degree of entropy. The main challenge to attaining cryptographic keys from biometric feature sets is due to the inherent intra-user dissimilarities and inter-user similarities within biometric features. The motivation is to evolve a framework for extraction of consistent keys directly from feature sets and use them in an IMS protocol.

The proposed framework for biometric key based IMS is shown in Fig 2. During the enrolment stage UE, users submit their biometric and along with a set of attributes to IdP. The centralised IdP has the following functional blocks

- Biometric key generator
- Hamming distance classifier and key extractor
- Template to Key predictor module
- Central storage module

The SP has the following functional blocks

- User authentication resolver
- Protected service module

IdP extracts biometric key and stores the generated key along with attribute list. The overall protocol flow of the IMS is shown in Fig 2. The events and activities of the centralised biometric based IMS with two stage authentication are listed as follows:

(i) User Enrolment UE: User enrolment takes place at the central IdP. As part of enrolment process the user is required to submit multiple samples of his biometric (iris) and the required set of attributes. The input set of iris samples are used to train a biometric to key generator system inside the Idp which in turn extracts a unique crypto key corresponding to the user. The larger the number of samples presented, the greater will be the accuracy of key extraction. The IdP stores the key extracted for a user along with the corresponding attributes in the central database. Thus, instead of storing the biometric template, crypto key extracted from the set of iris samples is stored. The Idp uses a hamming distance based classifier for refining the accuracy of the extracted key.

(ii) User Authentication AR: A two stage authentication procedure is adopted. The first stage requires the user requiring authentication to present a username and password. The IdP functions that has an integrated kerberos server carries out the first stage of authentication with the submitted username password. On successful first stage of authentication, the user is required to present his iris biometric sample. The presented sample is processed by the Template to Key Predictor module of the IdP. This modules compares the predicted key with the corresponding key of the user stored in the database during the enrolment phase. Hamming distance classifier is used to carry out the key comparison and decision making. If the second stage of authentication is successful, credentials are issued else an authentication failure notification is notified.

(iii) Issue of Credentials (Crd) : If the two stage authentication is successful, the IdP issues credentials to the user. The credential is Crd – KV(IDC || N once || OTP)

- KV - Secret trust key shared by IdP and SP
- IDC – ID of user
- Nonce - Unique one time random number
- OTP- Time based one time password

(iv) Service Request SR : On receiving the credentials, the user requiring services submits the same to the SP. The user authorisation module in the SP verifies the credentials and initiates service rendering from the protected resources module based on the submitted credentials.

A comprehensive protocol for an IMS is proposed with iris biometric trait used as the mode for authenticating the user. Keys are extracted from iris data and stored in the template as a crypto key representing the user instead of storing the complete feature set. The authentication of users is carried out with the crypto key as an identity. The rest of this paper proceeds as follows. Section II presents a survey on existing approaches to IMS and approaches to generation of cryptographic keys from biometric data along with associated literature survey. The proposed biometric trait for authentication in the IMS is iris. The state of art for iris recognition is covered in Section III. The proposed framework is presented in Section IV. The experiments carried out are described in Section V. Results are discussed in Section VI. Section VII concludes the paper and section VIII defines the roadmap for future work.

II. RELATED WORK

An effective and well defined IMS with established protocols is required to ensure security of identity and access management in distributed transactions. Design and specifications of an IMS depend upon the context of deployment. IMS systems are categorised based on identity management as centralised, federated and decentralised[3].

(i) Centralised : In the centralised architecture, a single, dedicated IdP manages identities for all users. Users need to trust the IdP and need to submit required user attributes to this IdP. Passport and Facebook Single Sign-On are examples of centralized systems.

(ii) Federated : In the federated system users choose the identity providers to be trusted with links. The trusted IdP is invariably part of the parent network / enterprise of the user. This system allows multiple enterprises to let subscribers use the same identification data to obtain access services across all enterprises in the group. Project Liberty supports this: identity providers with established business relations form circles of trust.

(ii) Decentralised : In the decentralised system, IdPs are trusted with attributes specifically released to them and there is no linking of identity across IdPs. Users create one or more identities with an IdP in the system. This architecture provides for distribution of sensitive attributes across distinct identity providers, a feature that ensures unlinkability of identities. Idemix, Shibboleth, Higgins, PRIME, OpenID, CardSpace, U-Prove, and P-IMS are examples of decentralised IMS.

Md Sadek Ferdous et al have carried out a comparative analysis of IMS evaluating them against parameters such privacy preservation, usability, security etc. Their study concluded that none of the IMS cater for all the ideally suited to meet the complete set of requirements[4]. Marcin et. al verified solutions based on federated identity with circle of trust amongst IdPs. They concluded that federated identity provides for enhanced security with better service for users[5]. Gines Dolera Tormo et. al defined the set of compliance requirements of an IMS into three broad categories:-

(i) System Requirements : The requirements must include confidentiality of digital identities, Single Sign On (SSO) capability, logging and auditing of transactions, strong authentication.

(ii) User-centric requirements : The IMS must cater for transparency with user with respect to identity and attribute management, user control over release of attribute information, ease of usability and automatic change management for user attributes.

(iii) Information management : Functionalities of the IMS must cater for attribute aggregation, revocation and defined disclosure levels.

In addition, threats to IMS were categorised as threats to trust level between the entities of the IMS, threats from attack to functioning of the system and threats to user privacy [6]. Future models of IMS design will need to have a huge emphasis towards ensuring user privacy in the online transactions [7][8]. Nitin Naik et. al carried out a study to evaluate IMS standards in mobile computing and communication environment. They evaluated Security Assertion MarkupLanguage (SAML), Open Authentication (OAuth), and OpenID Connect (OIDC). The conclusion of the study was that SAML had limitations with respect to usage in mobile communication due to legacy features not compatible with mobile computing and communication. OAuth was found to be suitable for an authorization only but not for an authentication while OpenID Connect was found to be the best choice [9].

Brent Carrara et. al highlighted the need to integrate biometric traits into authentication process of IMS to overcome the problem of transferability of credentials by users [10]. Johnson I Agbinya et. al attempted definition of digital identity with multimodal biometrics involving face and fingerprint traits along with other user attributes in digital IMS[11].

The proposed architecture as highlighted in Fig 1, integrates biometric traits in the user authentication process of the IMS. Biometric traits as an authentication measure in an IMS usher in advantages such as ensuring non-transferability and improved ease of use. Biometric template security is an area of concern in authentication systems employing biometric traits as a digital identity[12].

Researchers have attempted improving template security by using principles of cryptography. Cancelable biometric systems and bio-crypto systems have been used for enhancing template security. Salting and non-inverting modes of cancelable biometrics have been attempted. Biometric cryptosystems are categorised as key generation and key binding systems. Key generation systems generate a key that is a function of the biometric template whereas in key binding systems, the generated key is a function of biometric template and another secret key [13]. The motivation in this paper is to use keys generated directly from biometric traits as factor for authentication in the IMS.

Intra-user variations within biometric data pose major challenges in their usage as direct input to hash functions or as cryptographic keys. Generation of cryptographic keys from biometric data would first require the extraction of feature set followed by generation of unique reproducible keys with high entropy. The different traits exhibit different levels of uniqueness and permanence [14]. Attempts to generate unique keys from biometric traits have been made in the past.

Monrose et. al extracted cryptographic keys directly from keystroke patterns of users [15] using discretisation technique to convert keystroke features into a bit. Feature segments were converted based on a threshold. 12 bit strings were generated with a False Rejection Rate (FRR) of 48.6\%. The results were improved using voice samples for a specific password [16]. 46 bit strings were extracted with an FRR of 20\%.

Feng Hao et.al combined biometrics and PKI using online handwritten signature feature set to obtain a public-private key [17]. Intra-user variations were minimized by using dynamic time warping shape matching algorithm in the first stage to weed out simple forgeries. 40-bit private keys were generated from online signatures with an FRR of 8\%. Hao et. al generated 140-bit revocable keys iris biometric measurements using error correction combining Hadamard and Reed-Solomon codes [18]. The data set for the work comprised of 70 users with 10 samples each.

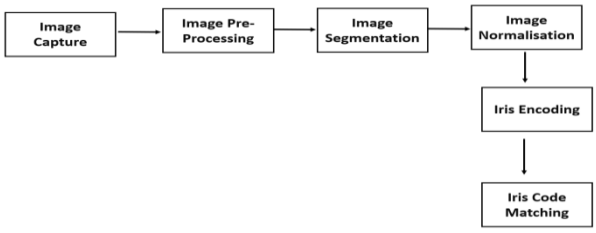

Fig 3. Human Iris Analysis

Michael Fairhurst et. al extracted features from live biometrics. 32 bit keys were generated with an FRR of 12.6\%. It was observed that signature being a behaviour biometric inherently has significantly high intra-user variations. This produces a constraint on generation of consistent keys. The problem was attempted to be solved by identifying features with lower variance [19].

Weigui Sheng et. al used fuzzy genetic clustering on dynamic features extracted from signature traits to capture intra and inter user variations [20]. Feature subsets with low variance were identified and subsequently encoded to generate the required keys. An FRR of 15.9\% for 20 effective bits was achieved. Weiguo Sheng et. al generated keys with onlinesignature data using semi-supervised clustering. Memetic algorithm was used to optimise the results [21]. It can be inferred that biometric traits enhance the security and ease of authentication while ensuring non-transferability. In order to use features extracted from biometric traits, it is pertinent to identify traits that are likely to give samples from the same user with lower variance. Such a trait will be able to produce usable and consistent keys. The literature survey on attempts made by researchers to extract keys directly from biometric traits led to the inference that traits that offer higher degree of uncorrelated features and lower intra-user variance hold higher promise. Behaviourial traits such as dynamic signature sets, keystroke dynamics and physiological traits such as facial recognition, voice etc do have distinct limitations in consideration for key extraction. It is inferred that iris traits have potential for generation of long and distinct keys with larger inter-user defined distance measure. The current work proposes use of iris traits for key extraction and usage in the framework of IMS.

III. IRIS RECOGNITION-STATE OF THE ART

Iris image as a distinguishing identity has significant advantage as the traits a high degree of inter-user variability. Iris recognition gained much attention in recent years as human iris has been shown to be remarkably individual [22, 23] and is now considered to be one of the most accurate biometric methods that are available for the unique identification of individuals. Advantages of iris recognition include permanence of the trait, uniqueness, easy integration on to a system, spoof resistant, non-invasive capture of trait and high accuracy whereas the disadvantages of the trait are the memory required for storage, cost of system and poor user acceptance. The disadvantages are being overcome by the use of smart phones for capture of iris traits and use of deep learning algorithms for recognition [24].

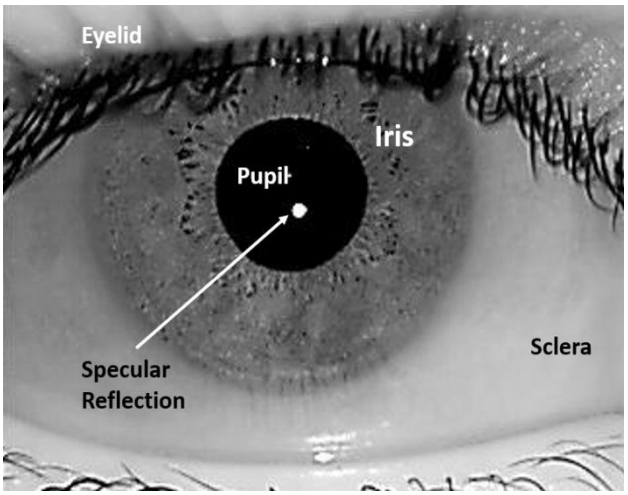

Fig 4. Sample Iris Image

Automated analysis of the human iris by a machine follows the steps shown in Fig 3. The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye and can be captured by a typical infrared camera. For the purpose of research and analysis, typical open datasets such as Multimedia dataset and IIT Delhi datasets have been used.The second stage of iris recognition is image pre-processing, which involves any modification to the original captured image that enhances the recognition process. Tasks such as adjustment of contrast of the image, detection and removal or marking of regions of specular reflections within the image form part of image pre-processing.

The third stage is segmentation which involves earmarking of region of interest within the given image. For iris recognition pupil-iris and iris-sclera boundaries are the regions of interest. Segmentation isolates the iris region in a digital eye image. The iris region as shown in Figure 4, is contained within two circles, the iris/sclera boundary and interior to the first, the iris/pupil boundary. The eyelids and eyelashes normally occlude the upper and lower parts of the iris region. As shown in the figure, specular reflections occurring within the iris region corrupt information pertaining to that portion region of the iris. Segmentation must ensure isolation of the desired circular iris region while excluding the artefacts. Segmentation is one of the critical steps in the iris recognition process as it delineates the iris region from the overall image presented to the algorithm.

Detection of the iris portion on the eye image entails isolating and demarcating the concentric circles delineating the iris portion. The algorithm must also identify and eliminate the occluding portions such as eyelashes, top and bottom eyelids and specular reflections. The standard techniques employed for segmentation include:-

1) Hough Transform: The algorithm determines and demarcates lines and circles in an image. Circular Hough transform deduces the radius and coordinates of the centre of pupil and iris regions. The edges of the circle are identified by computing the derivative of intensity values in an eye image and then delineating against a threshold to demarcate the edges of region of interest. The maximum in the region identified by the hough transform would be the radii of the inner and outer circles of the iris. Eyelids are demarcated by parabolic hough transform functions.

2) Daugman's integro-differential operator: In this method, as proposed by Daugman, the process of edge detection is carried out through integro-differential operators to identify the intensity gradients in an iris image.

$$max_{(}r, x_0, y_0)|G_\sigma(r) * \frac{\partial}{\partial x}\oint_{r,x_0,y_0}\frac{I(x,y)}{2r\pi}|$$

In the above equation, I(x,y) is the image of the eye being segmented to identify the iris region and r is the radius of search. G_σ (r) is the Gaussian smoothing function that is convolved with each neighbourhood of the pixel. The Gaussian smoothing function reduces the noise within the image thereby reducing the erroneous detection due to noise-related gradients. The integro-differential operator functions on the same lines of Hough transform using first derivatives of the image to obtain geometric parameters.

3) Active Contour models : Active contours are based on defined internal and external forces by deforming internally or moving across an image until balance is reached.These models have been used for localising the pupil in the eye images. The algorithms mentioned above were based on systems operating on iris images captured with near infra-red cameras. With the introduction of iris capture through smartphones in recent years, iris images are being captured for recognition in visible wavelength. Segmentation algorithms for visible wavelength images have been developed using colour component analysis, Zernike moments, knowledge based approaches, iterative refinement approaches, convolutional deep learning approach and multi-spectral analysis [25][26][27]

At the end of segmentation step, the iris portion from the image of eye is isolated. The next step is normalisation, in which the segmented iris portion is transformed to fixed dimensions in order to enable comparisons between different sets of data. The iris portion of the eye stretches due to pupil dilation under different levels of illumination. The normalisation process produces iris regions having constant

dimensions thereby enabling comparison of characteristics of same iris under different conditions. During this process, the segmented iris is unwrapped from polar state to Cartesian form.

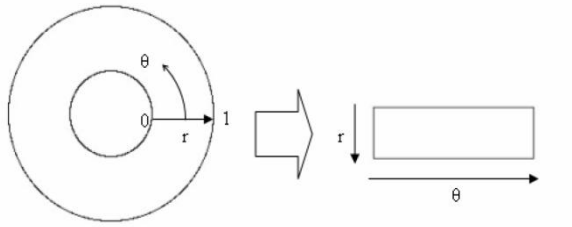

Fig 5. Daugman Rubber Sheet Model

As shown in Fig 5, the rubber sheet model caters for pupil dilation and size inconsistencies to produce a normalized representation with constant dimensions. The iris region is modeled as a stretchable rubber sheet anchored at the iris boundary.

The normalised model is then subjected to encoding of the texture features of the iris. Feature extraction methods employed on iris are:

1) Wavelet encoding
2) Gabor filters
3) Log-gabor filters
4) Zero crossings of the 1D wavelet
5) Haar wavelet
6) Laplacian of Gaussian filters
7) Fast Fourier Transform

The extracted features are then encoded suitably to obtain pattern in 0 and 1 bits, unique to each user trait [28][29]. The final step in the iris recognition process is the matching of iris code for identification. The proposed approach uses the encoded iris as the crypto key corresponding to a user and this encoded key is verified as am authentication measure based on a distance measure based classifier.

IV. PROPOSED MODEL & RESULTS

A Methodology

The methodology employed in each stage for analysis of iris trait, crypto key code generation and code matching is shown in flow chart Fig. 6.

For the purpose of this work Indian Institute of Delhi (IITD) and Multimedia University (MMU)databases have been used.

- IIT Delhi Database: The IIT Delhi iris dataset consists of images collected at IIT Delhi. The traits have been captured using a JIRIS JPC1000 digital CMOS camera from 224 users. The captured images are in bitmap format. The 1120 images are from 176 males and 48 females. All images are at a resolution of 320×240 pixels and have been acquired in the indoor environment.
- MMU Database: There are two MMU iris datasets; each collected using a different camera. MMU datasets offer a wide selection of ethnicities and image quality. They contain only 1,445 bitmap images at a resolution of 320×240 pixels.

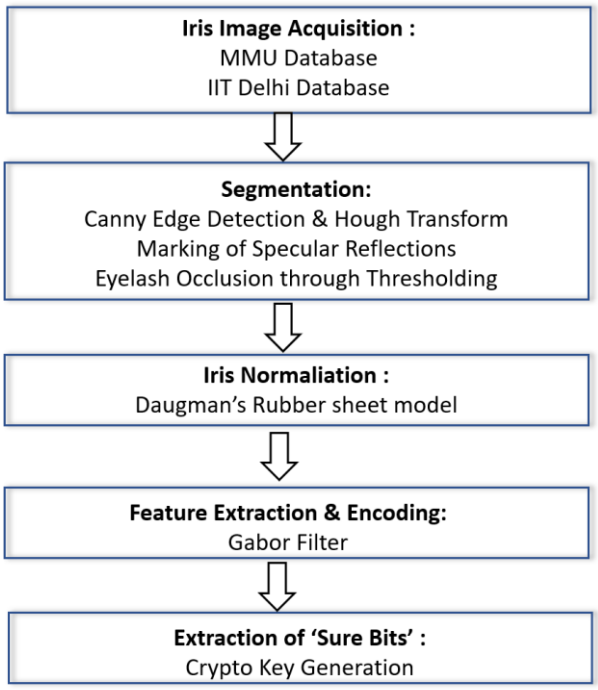

Fig 6. Flowchart - Implementation

The different stages in the transformation of iris image in getting the template is shown in Fig 7. During training phase,the iris image of a user is input into the system. In the first step, the iris portion is segmented and noise artefacts due to specular reflections, eyelashes and eyelids are masked. In the second step, the segmented iris is normalised as per the Daugman rubber model by converting the cartesian coordinates into polar coordinates. Gabor filter masks constructed by modulating a sine/cosine wave with a Gaussian are run over the normalised iris image and encoded into bits as per Table I. The 2D gabor filter over an image domain (x,y) is represented by the equation as shown below:

$$G(x,y) = e^{-\pi[(x-x_0)^2/\alpha^2+(y-y_0)^2/\beta^2]}e^{-2i\pi[u_0(x-x_0)+v_0(y-y_0)]}$$

where (x_0,y_0) specify the position in the image, (α,β)specify the width and length and (u_0,v_0)specify the modulation frequency.

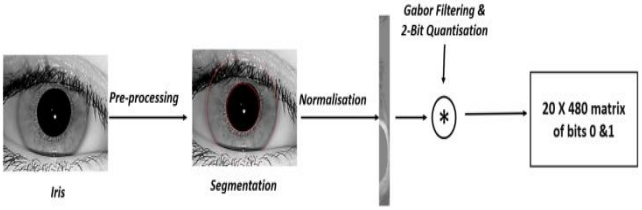

Fig 7. Formation of Iris Template

Each pair of encoded bits is the result of convolution of the normalised image with Gabor function. The result will both have real and imaginary part which can each have either positive or negative part. This implies that there are four possible combinations for each complex number to beencoded. The code possibilities are listed in Table I. This coding convention results in a 20 X 480 matrix to be generated for the iris.

Table I- Encoding of Iris Patterns

Value Range	Code
+ve real, +ve imaginary	11
-ve real, +ve imaginary	01
-ve real, -ve imaginary	00
+ve real, -ve imaginary	10

Conventional systems work on the code matrix generated as the basis for comparison with a distance based measure to take a decision on the level of similarity. The proposed work extracts crypto keys from training instances of iris traits based on a confidence measure.

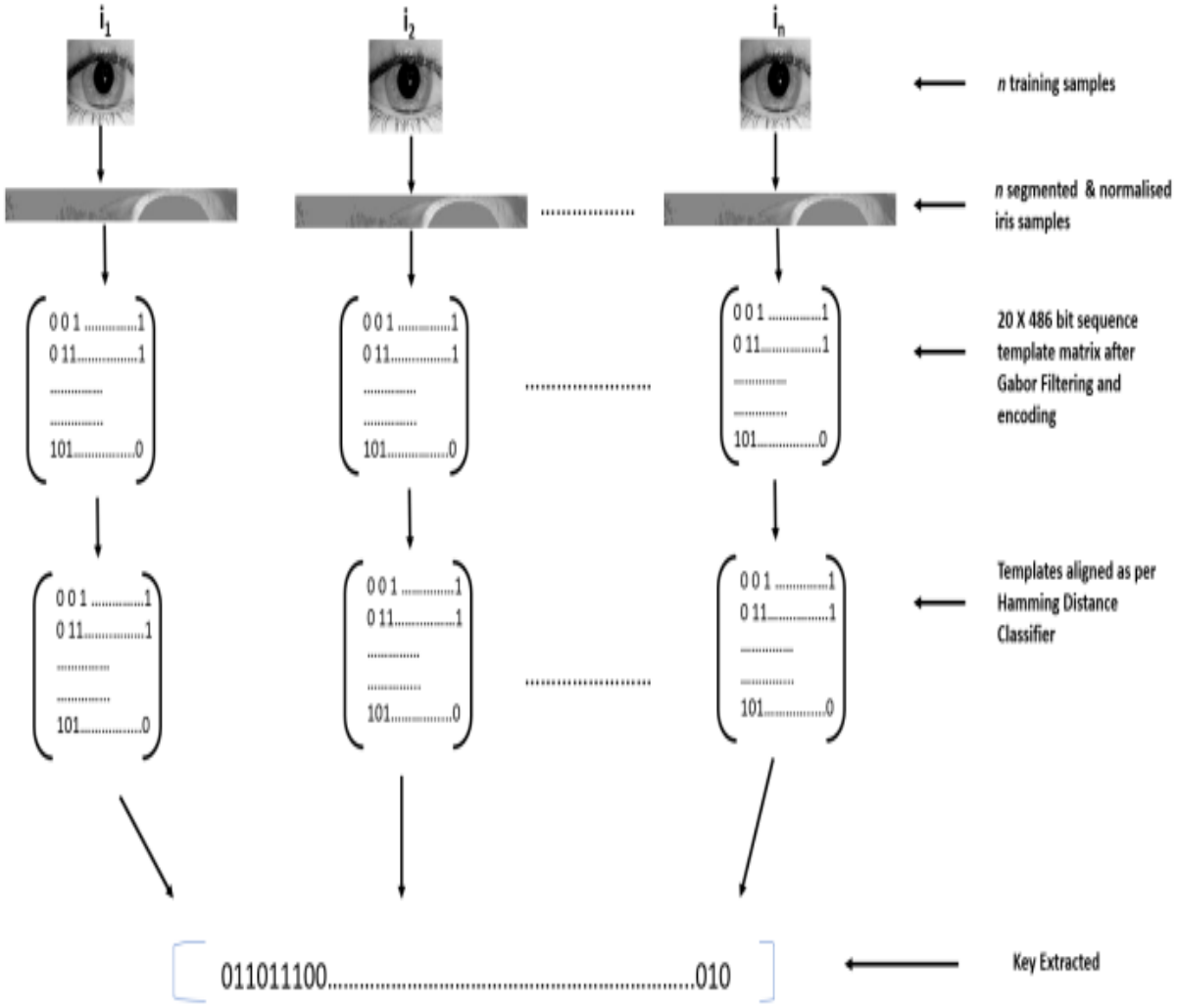

Fig 8. Extraction of Key

The methodology followed for generating keys from n training samples of iris is depicted in Fig 8.The segmented and normalised iris images are subjected to Gabor filtering and encoding to obtain 20 X 480 binary matrices. One of the user sample's encoded matrix is kept as a reference and code matrix of all other training samples are aligned by left or right shift till a minimum hamming distance is obtained with respect to the reference template of the training set. From the aligned set of code matrices for each user, a crypto key is extracted based on the degree of sureness of the bits. These sure bits are concatenated to represent the key corresponding to the user.

In order to validate the usability of the key as a representation, the FRR and FAR figures for template comparison as against key based comparison is carried out.

V RESULTS

The normalised iris region was convolved with Gabor filters and with Hamming distance as the matching metric, bits were generated based on surety across multiple training instances. The procedure adopted resulted in 300 bit unique and consistent crypto keys for each user, which in turn can be used for authentication and authorisation in an IMS system.

The crypto keys resulted in the same FAR and FRR as that of the original biometric template. An FAR of 0% and FRR of 99.05% could be achieved consistent equally with both biometric template and the equivalent derived crypto-keys.

VI. CONCLUSION

The generation of crypto keys corresponding to the iris biometric of a user gives rise to direct application in an IMS system with enhanced security and ease of operation. The results are encouraging and can be further refined by adopting the results with multi-modal biometric systems. Different heuristics can be employed to vary the unique crypto key of a user. The heuristics can be at the algorithmic level used to derive he crypto key or by varying the weighted inputs of the different biometric input modes used.

REFERENCES

1. J. Torres, M. Nogueira and G. Pujolle , "A survey on identity management for the future network" , IEEE Commun. Surveys Tuts. , vol. 15 , no. 2 , pp.787 -802 , 2013.
2. Nazia Mastali, Johnson I. Agbinya, "Authentication of Subjects and Devices Using Biometrics and Identity Management Systems for Persuasive Mobile Computing: A Survey Paper," in Proceedings of 2010 Fifth International Conference on Broadband and Biomedical Communications, Dec 15-17, 2010, Malaga, Spain. doi: 10.1109/IB2COM.2010.5723618
3. E. Birrell and F. B. Schneider, "Federated Identity Management Systems: A Privacy-Based Characterization," in IEEE Security & Privacy, vol. 11, no. 5, pp. 36-48, Sept.-Oct. 2013. doi: 10.1109/MSP.2013.114
4. Md. Sadek Ferdous, Ron Poet, "A comparative analysis of Identity Management Systems ", in 2012 International Conference on High Performance Computing & Simulation (HPCS), 02-06 July 2012 doi: 10.1109/HPCSim.2012.6266958.
5. Marcin Niemiec and Weronika Kolucka-Szypula. "Federated Identity in Real-life Applications", 2015 European Conference on Networks and Communications (EuCNC). DOI: 10.1109/EuCNC.2015.7194124.
6. Gines Dolera Tormo, Felix Gomez Marmol, Gregorio Martinez Perez, "Identity Management in Cloud Systems," Security, Privacy and Trust in Cloud Systems, Part II: Cloud Privacy and Trust, Springer, pp. 177-210, 2014
7. Alkhalifah, A.; D'Ambra, J., "The role of Identity Management Systems in enhancing protection of user privacy", in Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on , vol., no., pp.144-149, 26-28 June 2012 doi: 10.1109/CyberSec.2012.6246091.
8. Yuan Cao, and Lin Yang. "A Survey of Identity Management Technology", 2010 IEEE International Conference on Information Theory and Information Security, Doi: 10.1109/ICITIS.2010.5689468.
9. Nitin Naik, Paul Jenkins and David Newell. "Choice of Suitable and Access Management Standards for Mobile Computing and Communication", 2017 24th International Conference on Telecommunications (ICT),3-5 May 2017,Limassol, Cyprus, DOI: 10.1109/ICT.2017.7998280.
10. Carrara, Brent, and Carlisle Adams. "On achieving a digital identity management system with support for non-transferability", Privacy Security and Trust (PST), 2010 Eighth Annual International Conference on. IEEE, 2010.
11. Johnson I Agbinya, Nazia Mastali, Rumana Islam and Jackson Phiri. "Design and Implementation of Multimodal Digital Identity Management System Using Fingerprint Matching and Face Recognition", Proceedings of the 6th International Conference on Broadband Communications & Biomedical Applications, November 21 - 24, 2011, Melbourne, Australia, DOI: 10.1109/IB2Com.2011.6217932.
12. K. Nandakumar and A. K. Jain. "Biometric Template Protection: Bridging the performance gap between theory and practice," in IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 88-100, Sept. 2015. doi: 10.1109/MSP.2015.2427849
13. P Suresh and Radhika, K.R., "Bio-metric credential system: Multimodal cancelable anonymous identity management", in Advance Computing Conference (IACC), 2015 IEEE International , vol., no., pp.353-356, 12-13 June 2015 doi: 10.1109/IADCC.2015.7154729.
14. Anil K. Jain, Karthik Nandakumar, Arun Ross., "50 years of biometric research: Accomplishments, challenges, and opportunities", Pattern Recognition Letters, Volume 79, 1 August 2016, Pages 80-105, ISSN 0167-8655, http://dx.doi.org/10.1016/j.patrec.2015.12.013.
15. Fabian Monrose, Michael K. Reiter, and R. Wetzel., "Password Hardening Based on Keystroke Dynamics", Proceedings Sixth ACM Conf. Computer and Comm. Society (CCCS), 1999.
16. Fabian Monrose, Michael K. Reiter, Qi Li, Suzanne Wetzel., "Cryptographic Key Generation from Voice", Proceedings of 2001 IEEE Symposium on Security and Privacy, May 2001.
17. F. Hao and C.W. Chan., "Private Key Generation from On-line Handwritten Signatures", Inf. Manage. Comput. Security, vol. 10, no. 4, pp. 159–164, 2002.
18. F. Hao, Ross Anderson and John Daugman., "Combining Crypto with Biometrics Effectively", IEEE Transactions on Computers, Vol. 55, No. 9, September 2006.
19. Michael Fairhurst, Sanaul Hoque, Gareth Howells, Farzin Deravi., "Evaluating Biometric Encryption Key Generation", Proceedings of the Third COST 275 Workshop, 2005.
20. Weiguo Sheng, Gareth Howells, Michael Fairhurst and Farzin Deravi., "Template-Free Biometric-Key Generation by Means of Fuzzy Genetic Clustering", 2008 IEEE Transactions on Information Forensics and Security, Vol 3, No. 2, DOI: 10.1109/TIFS.2008.922056.
21. Weiguo Sheng, Shengyong Chen, Gang Xiao, Jiafa Mao and Yujun Zheng., "A Biometric Key Generation Method Based on Semisupervised Data Clustering" IEEE Transactions on Systems Man and Cybernetics: Systems, 2015, DOI: 10.1109/TSMC.2015.2389768.
22. John G. Daugman., "High Confidence Visual Recognition of Persons by a Test of Statistical Independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, VOL. 15, NO. 11, November 1993.
23. John Daugman., "How Iris Recognition Works", IEEE Transaction on Circuits and Systems for Video Technology, VOL. 14, NO. 11, JANUARY 2004, DOI: 10.1109/TCSVT.2003.818350.
24. Qi Zhang, Haiqing Zheman Sun and Tieniu Tan., "Deep Feature Fusion for Iris and Periocular Biomerics on Mobile Devices", IEEE Transactions on Information Forensics and Security, Vol. 13, No. 11, November 2018, DOI: 10.1109/TIFS.2018.2833033.
25. T Schlett, C Rathgeb and C. Busch., "Multi-spectral Segmentation in visible Wavelengths", 2018 International Conference on Biometrics, DOI: 10.1109/ICB2018.2018.00037.
26. Cunjian Chen and Arun Ross., "A Multi-Task Convolutional Neural Network for Joint Iris Detection and Presentation Attack Detection", 2018 IEEE Winter Conference on Applications of Computer Vision Workshops, DOI: 10.1109/WACVW.2018.00011.
27. Pattabhi Ramaih Nalla and Ajay Kumar., "Toward More Accurate Iris Recognition Using Cross-Spectral Matching", IEEE Transactions on Image Processing, Vol 26, No. 1, January 2017, DOI: 10.1109/TIP.2016.2616281.
28. Gene Itkis, Venkat Chandar, Benjamin Fuller, Joseph P. Campbell and Robert K. Cunningham., "Iris Biometric Security Challenges and Possible Solutions", Sep 2015, IEEE Signal Processing Magazine, DOI: 10.1109/MSP.2015.2439717.
29. Nenad Nestorovic, P. W. C Prasad, Abeer Alsadoon, A. Elchouemi., "Extracting Personal Identification Number From Iris", IEEE, 2016 15th RoEduNet Conference: Networking in Education and Research, DOI: 10.1109/RoEduNet.2016.7753220.