# Recent developments on Crypto Key generation techniques based on Biometric features: A Survey

[1]Samta Tembhekar, [2]Yogeshwari Sarode, [3]Priyanka Tekadpande
[1]Assistant Professor,[2]Assistant Professor,[3]Assistant Professor
Information Technology Department,
Kavikulguru Institute of Technology and Science, Ramtek,India

***Abstract :*** In Today's world, valuable information is stored in a server system and moreover personal information is being shared over open network. Further, internet is growing with fast speed where the network threats and unauthorized access problems are increasing. Therefore security of confidential data plays major role in providing, integrity during the process where information has to be sent across an internet. Therefore the cryptographic system is designed to overcome these issues. Several biometrics like fingerprint, iris, retina, etc., are used in rendering security to the information or key. The generation of cryptographic key from biometrics is used generally to secure the system. In this paper, we reviewed various techniques related with Cryptographic key generation based on Biometric parameter such as iris, fingerprint, etc. A brief introduction on the current techniques is also presented in this survey.

***IndexTerms*–Crypto-Key, Biometrics, security, Feature extraction, iris, fingerprint.**

## I. INTRODUCTION

Biometric authenticationmethods used today forvarious sender receiver identification purposes such as fingerprint-iris recognition, face detection, signature identification, voice authentication,hand geometry etc.. With an increasing complexity related with data storage, ethical hackingin cybercrime,these fields are now playing amajor role in security application. Securing data storage using biometrics is the hot research area in the field of computer science. Several biometrics like fingerprint, iris, face, signature voice are used for generating a secure cryptographic key and to improve security of confidential data. With an increased number of hackers and attackers, the demand of securing data over a public network between communicating sender-receiver becomes a challenging task, due to lack of proper authentication process. Encrypting the data with a cryptographic key ensures denied access of confidential data to unauthorized user. Today, there are several algorithms for biometric-cryptographic key generation with the help of user features such as iris, fingerprint, and face etc. It is a difficult task for the user to remember large password. Moreover the password of authorized user can be sometimes guess and cracked by hackers and attackers. Due to thisissue, authentication ofdata with the help of biometric cryptographic key is widely researched. Biometric features such as iris and fingerprint are unique characteristic of a human which does not change throughout the lifetime of a person. The utilization of biometric as a key is to increase security in a more effective way, reduce human mistakes during identification, increase user convenience and automation of security function.

## II. CRYPTOGRAPHY

Cryptography is the process of transformingconfidential data into a secret code when sender sends it to the receiver over a public network. This secret code is also known as "cipher text". Different encryption algorithms are used to produce cipher text. Cryptography converts confidential data into a unreadable format for an unauthorized user and ensures it to be kept secret, allowing it to be transmitted over a public network without allowing unauthorized user to decode it into original format. Cryptography also allows senders and receivers to authenticate each other through the use of key pairs. There are various types of algorithms for encryption, some common algorithms include.

A. Secret Key Cryptography: It is also called as symmetric encryption, where a single key is used for both encryption and decryption process.
B. Public Key Cryptography: It is termed as asymmetric encryption which uses two types of keys. One key is the public key that anyone can access. Another key is the private key which can be accessed by only the sender during transmission process. The sender encrypts the information using the receiver's public key. The receiver decrypts the message using its own private key. The sender encrypts plain text using a private key, while the receiver uses the sender's public key to decrypt it. Thus, the receiver knows who sent it.
C. Hash Functions: It is also called one-way encryption which does not use any key. Instead, Hash functions are used to for data transmission.

Cryptography should posses following properties:

1. Confidentiality: The information cannot be understood by users other than sender or receiver.
2. Integrity: The information cannot be modified or edited during transferring between sender and receiver over Internet or open network.
3. Non-repudiation: The sender of the information cannot refuse at a later regarding the originality of the information.
4. Authentication: The sender and receiver can both confirm each other's identity and the source/target of the information.
5. Access Control: Only the legal user is able to access the information

## III. CRYPTO-KEY GENERATION

In Biometric based approach, a unique cryptographic key is directly acquired from the biometric data of the user. The encryption process proceeds with the extraction of the biometric samples of fingerprint of the user. Biometric key is then extracted with the help of these features or parameters, which can be used to encrypt a plaintext message. Many algorithms are available for generation of crypto-key as illustrated in Fig I.

Firstly, the input images are acquitted from user's Biometric Samples such as iris, fingerprint, signatures, face etc. Then these image samples are pre- processed using some morphological operations such as dilation and erosion to filter out unwanted noise. Then various techniques are used to such as crossing point number to extract the target features from these segmented images samples of the user. Finally the features are used to generate crypto-key using the different algorithms. The generated Cryptographic key will be unique for each and every user and then theses Crypto-keys may be stored in the database for proper authentication of authorized users.

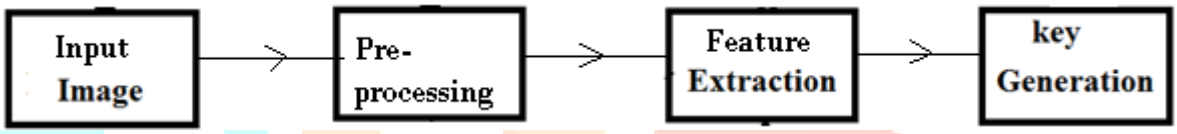


Fig. 1. Key Generation Process

Many algorithms are available for securing data. However, regardless of whether a user deploys a symmetric or a public-key system, the security is dependent on the secrecy of the secret or private key, respectively. The design of combining biometric authentication with cryptography has been developed with the help of fingerprint.

## IV. RELATED WORK

Arun Ross et al [1] presented a novel technique to perform fusion at the feature level by considering two biometric modalities - face and hand geometry. This technique may lead to substantial improvement in multimodal matching performance. After simulation, experimental results shows that it is well suitable for real time application in the areas such as biometric systems, face and hand geometry.

Gang et al [2] presented a lattice mapping based fuzzy commitment method for cryptographic key generation from biometric data. This approach outputs high entropy keys, and also conceals the original biometric data such that it is impossible to recover the biometric data even when the stored information in the system is open to an attacker. Simulated results have showed that its authentication accuracy is comparable to the well-known k-nearest neighbor classification.

Feng et al. [3] proposeda secure way to integrate the iris biometric into cryptographic applications. A repeatable binary string, i.e a biometric key, is generated from iris codes To solve errors issues, author studied the error patterns within iris codes and devised a two-layer error correction technique that combines Hadamard and Reed-Solomon codes. The key was generated from a subject's iris image with the aid of auxiliary error-correction data, which do not reveal the key and can be saved in a tamper-resistant token, such as a smart card. The reproduction of the key dependent on two factors: the iris biometric and the token. The attacker has to procure both of them to compromise the key. The proposed technique was which showed good success rate.

Jagadeesan et al. [4] proposed an efficient approach based on multimodal biometrics such as Iris and fingerprint for generating a secure cryptographic key. First, the features, minutiae points and texture properties are extracted from the fingerprint and iris images respectively. Then, the extracted features are fused at the feature level to obtain the multi-biometric template. Finally, a multi-biometric template is used for generating a 256-bit cryptographic key. After simulation, experimental results have showed that the 1 / 5 Cryptographic Key Generation from Multiple Biometric Modalities. Fusing Minutiae with Iris Feature generated 256-bit cryptographic key is said to be capable of providing better user authentication and better security.

Saritha et al. [5] proposed a new cryptographic key generation method using dual finger vein images. This new approach simplified the key generation process and reduced the complexity involved in a traditional cryptosystem. Finger vein were a hidden biometric trait that resides underneath the skin surface which is invisible to the naked eye. Cryptographic keys of different sizes can be generated using

this method with minimal amount of time complexity and space complexity. These keys can be used in many real time applications for secure data transmission.

Vincenzo et al. [6] presented new approach that deals with modern computing systems security issues, focusing on biometric based asymmetric keys generation process. Conventional PKI systems are based on private/public keys generated through RSA or similar algorithms. This approach embeds biometric information on the private/public keys generation process. Also, the corresponding private key depends on physical or behavioural biometric features and it can be generated when it is needed. Starting from fingerprint acquisition, the biometric identifier is extracted, cyphered, and stored in tamper-resistant smartcard to overcome the security problems of centralized databases. Biometric information is then used for user authentication and for public/private keys generation. Experimental results have shown that the asymmetric keys generation distinctive power depends on biometric authentication accuracy, assuring unique asymmetric keys for each authenticated user.

Rathgeb et al [7] proposed a new method of a generic treatment of how to generate biometric keys from binary biometric templates is presented. A context-based analysis of iris biometric feature vectors based on which stable biometric keys are extracted was proposed. Most reliable bits in binary iris codes were detected and utilized to construct keys from fuzzy biometric data. The proposed key-generation scheme was adapted to diverse iris biometric feature extraction algorithms, evaluated on a comprehensive database and compared against existing iris biometric cryptosystems. The scheme is also extended to provide fully revocable biometric keys, long enough to be applied in generic cryptosystems. After simulation, experimental results showed good results.

Kanadeet al.[8] proposed a simplified protocol to securely share such crypto-biometric keys. Another protocol is also proposed to generate and share session keys which are valid for only one communication session. This protocol achieved mutual authentication between the client and the server without the need of trusted third party certificates. This protocol also facilitated easy online updating of templates. The stored templates were cancelable. The protocols werethen evaluated for biometric verification performance on a subset of the NIST-FRG02 face database.

Nemanja et al. [9] presented a novel approach to the design of robust multimodal biometric cryptosystems. The goal behind the system was robustness, privacy of user's biometric templates and stable cryptographic key generation. The framework presented employs two modalities and a look-up table. The hashes of cryptographic keys generated from a biometric template during the enrollment phase are stored in the look-up table with cancelable templates generated from the sample belonging to different modality of the same subject. During the operation phase, the system releases the key, only if the hash of the key generated from the provided biometric sample is found in the look-up table, and the similarity score between corresponding cancelable templates is less than a predefined threshold. The performation of this approach is evaluated with the CASIA biometric template database.

Lifang et al. [10] proposed a biometric cryptosystem based on face biometrics. At encryption stage, 128-dimensional principal component analysis (PCA) feature vectors are extracted from the face image. And a 128 bit binary vector is obtained by thresholding. Then the distinguishable bits are selected to form bio-key and the optimal bit order number is saved in a look-up table. Furthermore, an error-correct-code (ECC) is generated using Reed-Solomon algorithm. The message is encrypted using symmetric DES with bio-key. In decryption phase, a 128-dimensional PCA features vector extracted from the query face image. Then a bio-key is generated using the look-up table generated at encryption stage. The final key is obtained using both bio-key and Error correct code (ECC). Finally, the symmetric DES decryption algorithm is implemented to obtain message using final key. After simulation, results show that algorithm is effective.

Nguyen et al [11] proposed a solution that uses Biometric Encryption Key (BEK) to encrypt Private Key and protect Private Key in a secure way for both of two this kind of information. The author has also presented the BEK generation algorithm and the BioPKI system to support this solution.

Gong et al [12] proposed an iris feature-based PKI key generation through general approach for distinguishable iris feature generation and a PKI key generation mechanism. This method was different as compared to traditional approaches of using pseudo random number to generate cryptographic keys. Thereby, a longer and more distinguishable bit stream can be generated for PKI key generation.

Saad et al. [13] presented an efficient approach to secure cryptographic key generation from iris and face biometric traits. Features extracted from preprocessed face and iris images are fused at the feature level and the multimodal biometric template is constructed from the Gabor filter and Principal Component Analysis outputs. This template is used to generate strong 256-bit cryptographic key. Experimental results confirmed efficiency of the approach.

Gokulakumar et al. [15] proposed an efficient methodology of fusion of iris and face for identification and verification. In this approach, the image of the face taken is normalized and converted into binaries. The iris is localized from the facial image. Then series of operations such as segmentation, normalization, feature encoding is performed and it is converted into binary format. These bits are compressed and crossed over into a combined biometric key. This combined biometric key is used to bind the each bit of the

cryptographic key. This binded version of the key is used for enrollment and to release the key. Instead of storing the actual key, its hashed version is stored in order to conceal the cryptographic key to provide a secure comparison method for key verification. This binded version of the key is released only if this matches with the valid image. During enrollment, these features are used to bind a cryptographic key. The operation involved is the binary XOR. Thus, an unauthorized image is discarded who does not possess the original face features used during enrollment. In contrast, a genuine subject with the correct face features will be accepted. By this spoofing can be avoided, since two kinds of keys are needed to encrypt the data and these keys are generated at once. This reduces the false acceptance rate and false rejection rate thereby the total success rate seems to be high.

## V. DISCUSSION

The security is an important aspect several applications where security plays vital role. Cryptographic techniques are widely used in many fields to secure confidential data during its storage and transmission. Authentication can be achieved using shared key which will be compared to a stored template to provide authentication of the individual. In security applications, there are several techniques based on biometricssuch as iris recognition, face recognition, fingerprints, hand, voice etc.Among the all the biometric features, iris and fingerprint are the unique biometric identifier and also has high identification accuracy.

## VI. CONCLUSION

Size oflarge key makes it difficult for user to remember cryptographic keys. To address this problem, numerous proposals have been suggested to generate a cryptographic key from user biometrics features. There is another issue which has not received adequate attention in the previous approaches; howeverthey arenecessary for real time applications. In this paper, differenttechniques are analyzed to generate cryptographic keys, and point out limitations and drawbacks of traditional approach. In this paper, we reviewed various techniques related with Cryptographic key generation based on Biometric parameter such as iris, fingerprint, etc. A brief introduction on the current techniques is also presented in this survey.

## REFERENCES

[1] Arun Ross and Rohin Govindarajan, "Feature Level Fusion in Biometric Systems", in proceedings of Biometric Consortium Conference (BCC), September 2004.

[2] Gang Zheng, Wanqing Li and Ce Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping", in Proceedings of the 18th International Conference on Pattern Recognition, vol.4, pp. 513 - 516, 2006.

[3] Feng Hao, Ross Anderson and John Daugman, "Combining Crypto with Biometrics Effectively", IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081 - 1088, September 2006.

[4] Jagadeesan, T.Thillaikkarasi, Dr.K.Duraiswamy "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature" International Journal of Computer Applications, 2010 .

[5] Saritha Reddy Venna 1, Ramesh Babu Inampudi, "A Novel Method for Cryptographic Key Generation Fusing Dual Finger Vein Images",International Journal of Computer Science and Information Technologies, Vol. 7 (6) , 2016, 2569-2573.

[6] Vincenzo Conti, Salvatore Vitabile, Filippo Sorbello," Fingerprint Traits and RSA Algorithm Fusion Technique, Sixth International Conference on Complex, Intelligent, and Software Intensive Systems, 2012."

[7] Rathgeb and A. Uhl, "Context-based biometric key generation for Iris", IET Computer Vision, Vol. 5, No. 6, Pp. 389 – 397, 2011.

[8] S Kanade, D Petrovska-Delacretaz, B Dorizzi, in ˜ Proceedings of Fourth IEEE International Conference on Biometrics: Theory Applications and Systems (BTAS), Washington, DC, USA, 2010. Generating and sharing biometrics based session keys for secure cryptographic applications, (2010), pp. 1–7.

[9] Nemanja Maček1, Borislav Đorđević , Jelena Gavrilović , Komlen Lalović, "An Approach to Robust Biometric Key Generation System Design", Acta Polytechnica Hungarica Vol. 12, No. 8, 2015.

[10] Lifang Wu, Xingsheng Liu, Songlong Yuan and Peng Xiao, "A novel key generation cryptosystem based on face features", IEEE 10th International Conference on Signal Processing (ICSP), Pp. 1675 – 1678, 2010.

[11] Nguyen Thi Hoang Lan and Nguyen Thi Thu Hang, "An approach to protect Private Key using fingerprint Biometric Encryption Key in BioPKI based security system", 10th International Conference on Control, Automation, Robotics and Vision (ICARCV), Pp. 1595 – 1599, 2008.

[12] Yazhuo Gong, Kaifa Deng and Pengfei Shi, "PKI Key Generation Based on Iris Features", International Conference on Computer Science and Software Engineering, Vol. 6, Pp. 166 – 169, 2008.

[13] Saad Abuguba, Milan M. Milosavljević and Nemanja Maček," An Efficient Approach to Generating Cryptographic Keys from Face and Iris Biometrics Fused at the Feature Level", International Journal of Computer Science and Network Security, VOL.15 No.6, June 2015.

[14] Aparna A, Ajish S. "Cryptographic Key Generation based on Contextual Information: A Review ", International Journal of Computer Applications Volume 134 - No.15, January 2016 .

[15] Gokulakumar.A.S, Venkataraghavan.C, Kavya priya.S, Suganya.T , "encryption-of-cryptographic-key-technique-bycrossover-of-iris-and-face-biometric-key", International Journal of Innovative Research in Computer and Communication Engineering