A Review on Biometric Cryptosystems

Jisha Nair.B.J.

Research Scholar - M.Phil (CS),
RVS College of Arts & Science, Sulur,TamilNadu,India

Ranjitha Kumari.S

Associate Professor, Department of Computer Science
RVS College of Arts & Science, Sulur,TamilNadu ,India

Abstract—Conventional person authentication methods based on passwords and identity documents fail to meet the tough security and performance needs of critical societal applications like e-commerce and international border crossing. This in turn has encouraged active research in the field of biometric recognition. Biometrics is the science of establishing the identity of the person based on physical or behavioral attributes such as fingerprint, face, vein, ear and iris etc. Biometric systems are based on the premise that the physical and behavioral attributes can be uniquely associated with an individual [1]. Cryptography is intended to ensure the secrecy and authenticity of message. Cryptographic key used for securing information during encryption and decryption will usually be long and is very difficult to remember. Protecting the confidentiality of this key is a major concern [7]. This can be efficiently solved by Biometric Cryptosystems. Biometric cryptosystems combine biometrics and cryptography to benefit from the strengths of both fields. In such systems, while cryptography provides high security levels, biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens. Instead of storing cryptographic keys, keys will be generated dynamically with the help of biometrics to secure the template and biometric system. Biometric cryptosystems can be used for biometric template security. In this literature review, several aspects of biometrics cryptographic schemes are discussed.

Keywords— Biometrics, Cryptography, Key binding, Key generation ,Key release, Multibiometrics, Levels of Fusion

I. INTRODUCTION

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person. The relevance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual's identity in the context of several different applications.

Examples of these applications include sharing networked computer resources, granting access to nuclear facilities, performing remote financial transactions or boarding a commercial flight. The proliferation of web-based services (e.g., online banking) and the deployment of decentralized customer service centers (e.g., credit cards) have further underscored the need for reliable identity management systems that can accommodate a large number of individuals [2].

The main task in an identity management system is the determination of an individual's identity (or claimed identity). Such an action may be necessary for a variety of reasons but the primary intention, in most applications, is to prevent impostors from accessing protected resources. Traditional methods of establishing a person's identity include knowledge based (e.g., passwords) and token-based (e.g., ID cards) mechanisms, but these surrogate representations of identity can easily be lost, shared, manipulated or stolen thereby compromising the intended security.

With the proliferation of information exchange across the Internet, and the storage of sensitive data on open networks, cryptography is becoming an increasingly important feature of computer security. In general, data will be secured using a symmetric cipher system, while public-key systems will be used for digital signatures and for secure key exchange between users. 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. Because of the large size of a cryptographically strong key, it would clearly not be feasible to require the user to remember and enter the key each time it is required[8]. Instead, the user is typically required to choose an easily remembered password that is used to encrypt the cryptographic key. This encrypted key can then be stored on a computer's hard drive. To retrieve the cryptographic key, the user is prompted to enter the password, which will then be used to decrypt the key

There are two main problems with the method of password security. First, the security of the cryptographic key, and hence the cipher system, is now only as good as the password. Due to practical problems of remembering various passwords, some users tend to choose simple words, phrases, or easily remembered personal data, while others resort to writing the password down on an accessible document to avoid data loss. Obviously these methods pose potential security risks. The second problem concerns the lack of direct connection between the password and the user. As a password is not tied to a user, the system running the cryptographic algorithm is unable to differentiate between the legitimate user and an attacker who fraudulently acquires the password of a legitimate user.

As an alternative to password protection, biometric authentication offers a new mechanism for key security by using a biometric to secure the cryptographic key. Instead of entering a password to access the cryptographic key, the use of this key is guarded by biometric authentication. When a user wishes to access a secured key, he or she will be prompted to allow for the capture of a biometric sample. If this verification sample matches the enrollment template, then the key is released and can be used to encrypt or decrypt the desired data. Thus, biometric authentication can replace the use of passwords to secure a key. This offer both convenience, as the user no longer has to remember a password and secure identity confirmation, since only the valid user can release the key.

In this literature review, analyses of various biometric crypto keys are discussed (Section II). A brief summary of biometric based keys and classifications are also discussed (Section III). Multibiometrics and fusion at various levels are analyzed as these technologies can be combined to have a more secure and reliable multi biometric cryptographic systems based on various levels of fusions (Section IV).Survey of various literatures on biometric cryptosystems is given. (Section V). Issues and challenges of designing such systems and stipulates on some of the promising directions for further research for a successful blending of the biometric and cryptographic techniques are mentioned .(Section VI)

II. BIOMETRICS AND CRYPTO KEYS

Biometrics offers a natural and reliable solution to certain aspects of identity management by utilizing fully automated or semi-automated schemes to recognize individuals based on their biological characteristics. By using biometrics it is possible to establish an identity based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password. In some applications, biometrics may be used to supplement ID cards and passwords thereby imparting an additional level of security. Such an arrangement is often called a dual-factor authentication scheme.

A number of biometric characteristics have been in use in various applications (see Fig. 1). Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet all the requirements (e.g., accuracy, practicality, cost) of all the applications (e.g., DRM, access control, welfare distribution)

In traditional cryptosystems, user authentication is based on possession of secret keys [7]; the method fails if the keys are not kept secret (i.e., shared with non-legitimate users).

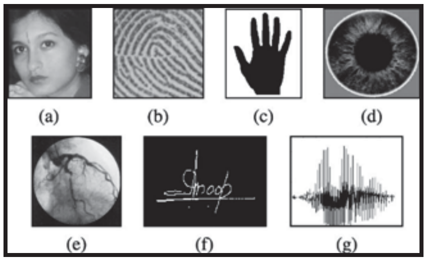


Fig. 1. Examples of biometric characteristics. (a) Face. (b) Fingerprint. (c) Hand geometry. (d) Iris. (e) Retina. (f) Signature. (g) Voice. From D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition

Further, keys can be forgotten, lost, or stolen and, thus, cannot provide non-repudiation [3][4]. Current authentication systems based on physiological and behavioral characteristics of persons known as biometrics, such as fingerprints, inherently provide solutions to many of these problems and may replace the authentication component of traditional cryptosystems[9].

Biometric cryptosystems are similar to password based key generation systems as they are used to secure cryptographic key or to directly generate cryptographic key from biometric features. Since the biometric measurements obtained during enrollment and authentications are different, these features cannot be used directly for the generation of cryptographic key generation. To facilitate key generation helper data or secure sketch of the biometric features are stored during enrollment. Therefore biometric cryptosystems are also known as helper data systems.

Biometric cryptosystems [5] were originally developed for the purpose of either securing a cryptographic key using biometric features or directly generating a cryptographic key from biometric features.

III. CLASSIFICATION OF BIOMETRIC CRYPTOSYSTEMS

Biometric cryptosystems are classified as key release, key binding and key generation systems depending on how the secure sketch is obtained. Secure sketch is public information about biometric features stored in databases during enrollment. Fuzzy vault[16] and fuzzy commitment[26] are the two most popular techniques used for constructing biometric cryptosystems.

A. Key Release based on biometrics

The basic idea of biometric-based keys is that the biometric component performs user authentication (user authorization), while a generic cryptographic system can still handle the other components of containment. Thus, in such systems, a cryptographic key is stored as part of a user's database record, together with the user name, biometric template, access privileges, and that is only released upon a successful biometric authentication. This method of integrating biometrics into a cryptosystem is referred as the method of biometric-based key release. The characteristics of the biometric key release system design are: 1) it requires access to biometric templates for biometric matching and 2) user authentication and key release are completely decoupled. (See Fig. 2.(a),(b)

B. Key Binding Biometric cryptosystems

When secure sketch is obtained by combining cryptographic key which is independent of biometric features with biometric template, it is referred as key binding biometric cryptographic systems [1] eg. Fuzzy Vault & Fuzzy commitment. This involves hiding the cryptographic key within the enrollment template itself via a trusted (secret) bit-replacement algorithm. Upon successful authentication by the user, this trusted algorithm would simply extract the key bits from the appropriate locations and release the key into the system. (see Fig.2.c)Unfortunately, this implies that the cryptographic key will be retrieved from the same location in a template each time a different user is authenticated by the system. Soutar et al. [12] proposed biometric encryption algorithm using image processing. This algorithm binds a cryptographic key with the user's fingerprint images at the time of enrolment. The key is then retrieved only upon a successful authentication. Thus, if an attacker could determine the bit locations that specify the key, then the attacker could reconstruct the embedded key from any of the other users' templates. If an attacker had access to the enrollment program then he could determine the locations of the key by enrolling several people in the system using identical keys for each enrollment. The attacker then needs only to locate those bit locations with common information across the templates.

C. Key Generation Biometric cryptosystems

If secure sketch is derived only from the biometric template and cryptographic key is directly generated from helper data and query biometric features, then it is called key generation biometric cryptosystems. (see Fig. 2.d) Eg. Secure sketch- Fuzzy extractor [15]. The data is derived directly from a biometric image. Bodo proposed such a method in a German patent. This patent proposed that data derived from the biometric are used directly as a cryptographic key[6]. However, there are two main problems with this method. First, as a result of changes in the biometric image due to environmental and physiological factors, the biometric template is generally not consistent enough to use as a cryptographic key. Secondly, if the cryptographic key is ever compromised, then the use of that particular biometric is irrevocably lost. In a system where periodic updating of the cryptographic key is required, this is catastrophic.

IV. MULTI BIOMETRIC CRYPTOSYSTEMS

High security applications and large scale identification systems place a strict accuracy requirement that cannot be met by biometric systems based on a single biometric identifier. Multi biometric systems overcome this limitation by accumulating evidence from more than one biometric trait,

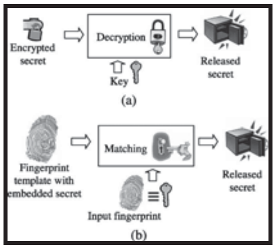
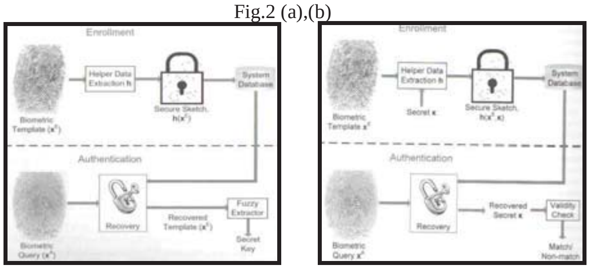


Fig.2 (a),(b)



(c) **(d)**

Fig. 2 : (a) In password-based authentication, a cryptographic key is the "secret" and the password is the "key." (b) In the fingerprint-based authentication, a cryptographic key is the "secret" and fingerprint is the "key." In both cases, the cryptographic key is released upon a successful authentication. (c)Authentication mechanism when biometric template is secured using a key Binding Biometric Cryptosystem (d) Authentication mechanism when biometric template is secured using a key Generation Biometric Cryptography. From D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar,*Handbook of Fingerprint Recognition &* Anil K Jain,Arun Ross,Karhik Nandakumar *Introduction to Biometrics*

(e.g., face, fingerprint, iris) in order to recognize a person or from multiple sources. Compared to uni biometric systems that rely on a single biometric trait, multi biometric systems can provide higher recognition accuracy and larger population coverage. The information from different sources can be fused in various levels to obtain a reliable identity decision. Four issues are to be considered while addressing multi biometric systems. Information source, mode of operation, level of fusion and fusion approach. Multibiometric systems can be classified into Multi-sensor, Multi-sample, Multi-algorithm, Multi-instance, and multi-modal. In the first four scenarios evidences are derived from single biometric trait and in the fifth scenario evidences are derived from multiple biometric traits[1].(see Fig.3)

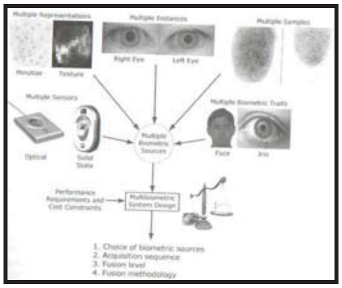


Fig.3 Multibiometric utilize information from multiple biometric sources to establish an identity.

Fusion of multi biometric indicate the improvement in security and reliability of the system.Various levels of fusion in Multi-biometric systems are given. (See Fig. 4).

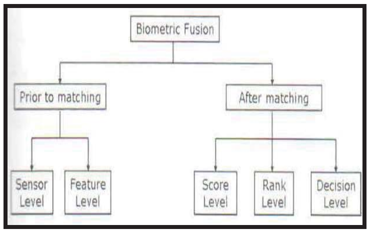
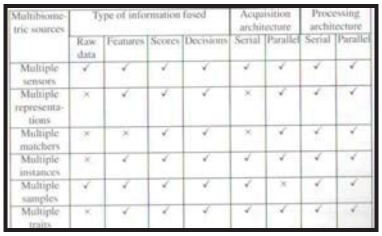


Fig. 4: Fusion can be done at various levels in multibiometric systems

Table 1



Multibiometric sources	Type of information fused				Acquisition architecture		Processing architecture	
	Raw data	Features	Scores	Decisions	Serial	Parallel	Serial	Parallel
Multiple sensors	✓	✓	✓	✓	✓	✓	✓	✓
Multiple representations	×	✓	✓	✓	×	✓	✓	✓
Multiple matchers	×	×	✓	✓	×	✓	✓	✓
Multiple instances	×	✓	✓	✓	✓	✓	✓	✓
Multiple samples	✓	✓	✓	✓	✓	×	✓	✓
Multiple traits	×	✓	✓	✓	✓	✓	✓	✓

Table 1. Dependencies between design choices in multibiometric system Indicates compatible design with check and non compatible with cross

Sensor Level fusion: Consolidation of evidences presented by multiple sources of raw data before they are subjected to feature extraction.
Feature Level fusion: Consolidation of evidences presented by two different biometric feature sets os same individual.
Score level fusion: Consolidation of match score output by different biometric matchers in order to arrive at a final recognition decision
Rank Level fusion: Consolidation of all the ranks output by individual biometric subsystems to derive a consensus rank for each identity.
Decision Level fusion: Consolidation is carried out at the abstract ordecision level when only decision outputs by the individual biometri matcher are available.

Dependencies of information choices and compatible design are given in table -1.While selecting biometric features care shoud be taken that one of the features should be very difficult to capture.Two or more biometric feature along with better cryptographic key generation scheme will provide secured biometric cryptosystems.

V. LITERATURE SURVEY

Over the past several years, there have been a number of research efforts aimed at addressing the issues related to inte- gration of biometrics into cryptosystems. Uludag et al. [6] presented several techniques that monolithically combine a cryptographic key with the biometric template of the user. It is stored in the database in such a manner that it cannot be exposed without a valid biometric authentication.

Cancellable biometrics gives a better performance of security with more than one template for the same biometric data. Russel Ang et al. [18] proposed the measurement of success of a particular transformation and matching algorithm for fingerprints.

Soutar et al. [12]–[14] proposed a key binding algorithm in an optical correlation-based fingerprint matching system. This algorithm binds a cryptographic key with the user's fingerprint images at the time of enrollment. The key is then retrieved only upon a successful authentication.

Davida *et al.* [10], [17] propose an algorithm based on the iris biometric. They consider binary representation of iris texture, called IrisCode [18], which is 2048 bits in length. The biometric matcher computes the Hamming distance be- tween the input and database template representations and compares it with a threshold to determine whether the two biometric samples are from the same person or not. The authors assume that the IrisCodes from different sampling of the same iris can have up to 10% of the 2048 bits (204 bits) different from the same iris's template IrisCode. The authors also assume that the IrisCodes of different irises differ in as many as 45% of the 2048 bits (922 bits).

Lifang Wu et.al [19] developed a biometric cryptosystem based on face biometrics. During encryption 128-dimensional Principal Component Analysis feature vector is initially obtained from the face image. Subsequently 128 bit binary vector is achieved by thresholding. Then the author selected distinguishable bits to generate bio-key. In addition an Error correcting code is produced using Reed –Solomon algorithm.

Monrose et al. [20] proposed a method to make passwords more secure by combining keystroke biometrics with pass- words. Their technique was inspired by password "salting," where a user's password (pwd) is salted by prepending it with an 8-bit random number (the "salt"), resulting in a hardened password (hpwd). A weakness of this work is that it only adds about 15 bits of entropy to the passwords, thus making them only marginally more secure.

Integrating biometric with cryptography is seen as a potential solution but any biometric cryptosystem must be capable of overcoming tiny changes present between different acquirement of similar biometric with purpose of generating reliable keys. Sashank Singhvi et al.,[11] developed a technique which exploits an entropy dependent feature extraction process integrated with Reed Solomon error correcting code.

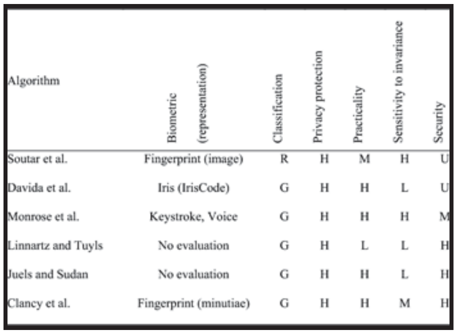
Monrose et al. [21]–[23], made some minor modifications to their original scheme, applied it to voice biometrics (which is more distinctive than keystroke biometrics), and were eventually able to generate cryptographic keys of up to 60 bits, which although much higher than the 15 bits achieved in their earlier work, is still quite low for most security applications.

Tuyls et al. [24], [25] assume that a noise-free template X of a biometric identifier is available at the enrollment time and use this to enroll a secret S to generate a helper data W

In their “fuzzy commitment” scheme [26], Juels and Wattenberg generalized and significantly improved Davida et al.’s methods [10], [17] to tolerate more variation in the biometric characteristics and to provide stronger security.

Juels and Sudan [16] prove the security of the fuzzy vault scheme in an infor mation-theoretic sense. Although the authors specifically mention application of their scheme to

Table 2



Algorithm	Biometric (representation)	Classification	Privacy protection	Practicality	Sensitivity to invariance	Security
Soutar et al.	Fingerprint (image)	R	H	M	H	U
Davida et al.	Iris (IrisCode)	G	H	H	L	U
Monrose et al.	Keystroke, Voice	G	H	H	H	M
Linnartz and Tuyls	No evaluation	G	H	L	L	H
Juels and Sudan	No evaluation	G	H	H	L	H
Clancy et al.	Fingerprint (minutiae)	G	H	H	M	H

In Table 2, a comparison of various algorithms: Soutar et al. [12]–[14], Davida et al. [10], [17], Monrose et al. [20]–[23], Linnartz and Tuyls [24], [25], Juels and Sudan [16], and Clancy et al. [27] are given. The third column in Table 2 indicates the key release (R) or key generation (G) classification. Practicality deals with the complexity of the algorithm.

biometric keys, it is not clear how robust the algorithm is to typical variations in the biometric signal.

Clancy et al. [27] propose a “fingerprint vault” based on the scheme of Juels and Sudan [16]. At the enrollment time, multiple (typically five) fingerprints of users are acquired. The fingerprint representation (minutiae position) is extracted from each fingerprint. Correspondence between the feature points (minutiae) extracted from the multiple prints is established based on a bounded nearest-neighbor algorithm. That is, when different prints of a finger are overlaid on top of each other, the minutiae in one print which are within a close spatial proximity of minutiae in other print are considered as the same.

VI. ISSUES & CHALLENGES

Password-based authentication systems do not involve any complex pattern recognition and, hence, they almost always perform accurately as intended by their system designers. The real challenge in biometric cryptosystems comes from the fact that biometric signal and their representations (e.g., facial image and its computer representation) of a person vary dramatically depending on the acquisition method, acquisition environment, user’s interaction with the acquisition device, and (in some cases) variation in the traits due to various pathophysiological phenomena. Lot of noise is introduced during data acquisition process. This same biometric may change between successive acquisitions (due to wound, ageing etc.) and noise can be introduced to a biometric signal by an acquisition device or the environment. While it is very convenient to use biometric traits for encryption, for instance someone using his fingerprint or palm prints to encrypt a document and securely send it over network, this is very difficult due to the aforesaid variability of the biometric signals and the fact that encryption and decryption operations cannot tolerate the change of even a single bit. In its most basic sense, generating a cryptographic key directly from a biometric trait, for instance fingerprints, has not been very successful, as it involves obtaining an exact key from a highly variable data. For instance Feng and Wah has only been able to generate a 40-bit private key from online signatures with an 8% equal error rate (the key extracted from a genuine signature is not correct or a forgery successfully extracts the key)

The greatest challenge is to design cryptosystems that generate non linkable templates, provides good trade-off between accuracy & security and utilize feature adaptation schemes that preserve accuracy and allow easy fusion of modalities.

VII. CONCLUSION

Biometrics are an essential component of any identity based security system because no other technology can replace the requisite functionality of "identifying the authorized person based on their inherent unique traits."
Integration of biometrics for effective user authentication within a cryptographic system makes sensitive sense. There are a number of challenges involved in combining biometrics into a cryptographic system, primarily due to remarkable variations in the representations of a biometric identifier and due to imperfect nature of biometric feature extraction and matching algorithms. While researchers have proposed many interesting and clever ideas for generation or binding of biometric keys, there are still many critical problems peculiar to the biometric domain have not been satisfactorily solved. Although the complexity of successful intrusion can be made formidable, but these systems can in practice be defeated using relatively simple strategies. A naive attack on a biometric system could be launched by successively presenting biometric samples from a representative population (either synthetically generated or actual samples) and the success of the attack is likely to be bounded by the weakest link in the security chain, In this regard, we believe it is more critical to focus on increasing the accuracy of the individual biometric matcher performance and on devising effective multi biometric strategies to deliver acceptable end-to-end system performance.

When crypto biometric systems eventually come into practical existence, there is a danger that biometric components may be used as an irrefutable proof of existence of a particular subject at a particular time and place. Mere incorporation of biometrics into a system does not in itself constitute a proof of identity. We need to understand how these foolproof guarantees can be theoretically proved in a deployed cryptosystem and how to institute due processes that will provide both technological and sociological freedom to challenge the premises on which nonrepudiation is ascertained.

REFERENCES

[1] Anil K Jain , Arun A Ross , Karthik Nandakumar , Introduction to Biometrics

[2] Anil K. Jain Michigan State University, USA Patrick Flynn University of Notre Dame,USA Arun A. Ross West Virginia University, USA , Handbook of Biometrics

[3] U. Uludag, "Secure biometric systems," PHD thesis, Michigan state university,2006.

[4] Uludag.U,Pankanti.S.Prabhakar.S,Jain.A.K"Biometric cryptosystems: issues and challenges " Proceedings of IEEE ,Vol 92,No.6,Pp 948-960 ,2004

[5] Ann Cavoukian and Alex Stoianov Biometric Encryption Chapter from theEncyclopedia of Biometrics

[6] A. Bodo, "Method for producing a digital signature with aid of a biometric feature," Germany: German patent DE 42 43 908 A1, 1994

[7] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall College, 2006.

[8] F.Ayoub and K Singh ," Cryptographic techniques and network security" IEEE proceedings of communications,Radar and Signal Processing,Vol 131,No.7 Pp 684-694 , 1984

[9] F Chafia ,C Salim and B Fraid ," Biometric crypto system for authentication" International Conference on Machine and Web Intelligence ,Pp434 -438,2010

[10] G. I. Davida, Y. Frankel, and B. J. Matt, "On enabling secure ap- plications through off-line biometric identification," in Proc. 1998 IEEE Symp. Privacy and Security, pp. 148–157.

[11] R Sashank Singhvi ,S.P. Venkatachalam ,P.M.Kannan and V .Palanisamy ," Cryptography key generation using biometrics" International Conference on Control ,Automation,Communication and Energy conservation" Pp 1-6, 2009

[12] C. Soutar, D. Roberge, S. A. Stojanov, R. Gilroy, and B. V. K. Vijaya Kumar, "Biometric encryption using image processing," in Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, 1998, pp. 178–188.

[13] "Biometric encryption enrollment and verification proce- dures," in Pr~~oc. SP~~IE, Optical Pattern Recognition IX, vol. 3386,1998, pp. 24–35.

[14] "Biometric encryption," in ICSA Guide to Cryptography, R. K. Nichols Ed. New York: McGraw-Hill, 1999.

[15] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy Extractors: Generate Strong Keys from Biometrics and Other Noisy Data," Cryptology ePrint Archive, Tech. Rep. 235, February 2006, A preliminary version of this work appeared in EUROCRYPT 2004.

[16] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," in Proc. IEEEInternational Symposium on Information Theory, Lausanne, Switzerland, 2002, p. 408

[17] G. I. Davida, Y. Frankel, B. J. Matt, and R. Peralta, "On the re- lation of error correction and cryptography to an offline biometric based identification scheme," in Proc. Workshop Coding and Cryp- tography (WCC'99), pp. 129–138.

[18] Russel Ang, Rei Safavi-Naini and Luke McAven "Cancellable key based fringerprint templates" Australasian Conference on Information Security and Privacy Pp 242-252,2005.

[19] Lifang Wu,Xingsheng Liu,Songlong Yuan and Peng Xiao," A Novel key generation cryptosystem based on face features" IEEE 10th IC on Signal Processing,Pp1675-1678,2010

[20] F. Monrose, M. K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," in Proc. 6th ACM Conf. Computer and Communications Security, 1999, pp. 73–82.

[21] F. Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Using voice to generate cryptographic keys," in Proc. 2001: A Speaker Odyssey, Speaker Recognition Workshop, 2001, pp. 237–242.

[22] “Cryptographic key generation from voice,” in Proc. 2001 IEEE Symp. ~~Secur~~ity and Privacy, pp. 202–213.

[23] F. Monrose, M. K. Reiter, Q. Li, D. P. Lopresti, and C. Shih, “To- ward speech-generated cryptographic keys on resource constraineddevices,” in Proc. 11th USENIX Security Symp., 2002, pp. 283–296.

[24] J.-P. Linnartz and P. Tuyls, “New shielding functions to enhance privacy and prevent misuse of biometric templates,” in Proc. 4th Int. Conf. Audio- And Video-Based Biometric Person Authentication, 2003, pp. 393–402.

[25] E. Verbitskiy, P. Tuyls, D. Denteneer, and J. P. Linnartz, “Reliable biometric authentication with privacy protection,” presented at the SPIE Biometric Technology for Human Identification Conf., Orlando,

[26] Ari Juels and M.Wattenberg , A Fuzzy Commitment t Scheme from proceeding of sixth ACM Conference on Computer and communication security November 1999

[27] T. C. Clancy, N. Kiyavash, and D. J. Lin, “Secure smartcard-based fingerprint authentication,” in Proc. ACM SIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop, pp. 45–52.