ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

A BIOMETRICS BASED USER-CENTRIC AUTHENTICATION APPROACH FOR USER FRIENDLY SECURITY SYSTEM

Lakshmisree C S,
Computer Science and Engineering Department,
Karpagam University, Coimbatore.
lakshmisreenivasc@gmail.com

Abstract— Authentication is the act of confirming the truth of an attribute of a datum or an entity. Biometric authentication for personal identification is very popular now days. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioural characteristics such as a fingerprint or a voice sample. The characteristics are measurable and unique.

In this paper, I propose a simple yet effective biometrics based authentication solution. This method involves introducing a reference subject(RS), Securely fusing t the user's biometrics with the RS, generating BioCapsule(BC) from the fused biometrics, and employing BCs for authentication. The BioCapsule is the difference between the user and the Reference Subject for Authentication without revealing a user's original biometric information. This secure fusion based approach is secure against various attacks. It supports replaceability and protect user's privacy. The new BC based approach is verified through experiments and detailed comparison with existing approaches.

Keywords—Biometrics,Authentication, Reference Subject, Biometric template, BioCapsule, Replaceability.

I. INTRODUCTION

User Authentication is a method of identifying the user and verifying that the user is allowed to access some restricted service. Authentication processes may vary from simple password based authentication system to costly and computation intensified authentication systems. Passwords are more than just a key. They serve several purposes. They ensure our privacy, keeping our sensitive information secure. Passwords authenticate us to a machine to prove our identity-a secret key that only we should know.

Authentication is a critical part of any trustworthy computing system; it ensures that only individuals with verified identities can log on the system or access system resources. Identity theft is a growing concern in our digital society. Traditional authentication methods such as passwords and identity documents aren't sufficient to ensure security. Such surrogate representations of identity can be easily forgotten, lost, guessed, stolen or shared. A central theme of authentication is to authenticate users using characteristics intrinsically linked with human users rather than some external factors. A promising direction emerging from this effort

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

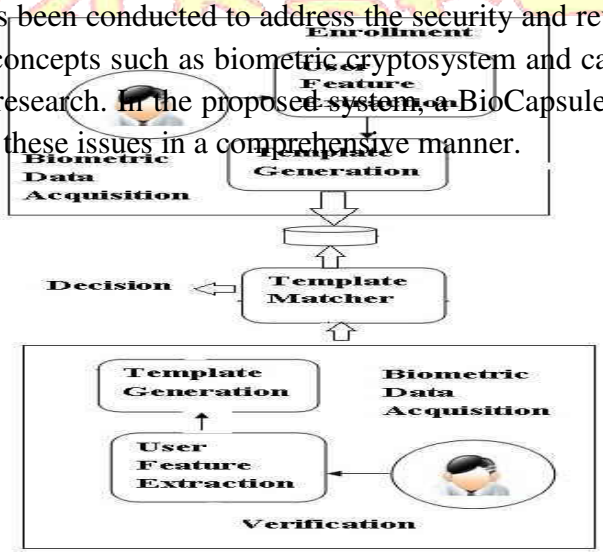
is biometrics. As a result, biometrics is becoming a promising authentication or identification method for system security.

Biometrics is defined as the unique (personal) physical/logical characteristics or traits of human body. These characteristics and traits are used to identify each human. Any details of the human body which differs from one human to other will be used as unique biometric data to serve as that person's unique identification (ID), such as: retinal, iris, fingerprint, palm print and DNA. Biometric systems will collect and store this data in order to use it for verifying personal identity. The combination of biometric data systems and biometrics recognition/ identification technologies creates the biometric security systems. This approach offers a convenient, accurate, irreplaceable and high secure alternative for an individual.

Biometric systems can be used in two different modes. Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the biometric data obtained from the user is compared to the user's data already stored in the database. Identification occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all.

Before the user can be successfully verified or identified by the system, he/she must be registered with the biometric system. User's biometric data is captured, processed and stored. As the quality of this stored biometric data is crucial for further authentications, there are often several biometric samples used to create user's master template. The process of the user's registration with the biometric system is called enrolment.

Intensive research has been conducted to address the security and revocability of biometrics , as well as user privacy; concepts such as biometric cryptosystem and cancelable biometrics(CB) have emerged from this research. In the proposed system, a BioCapsule and the use BC for user authentication to address these issues in a comprehensive manner.



ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

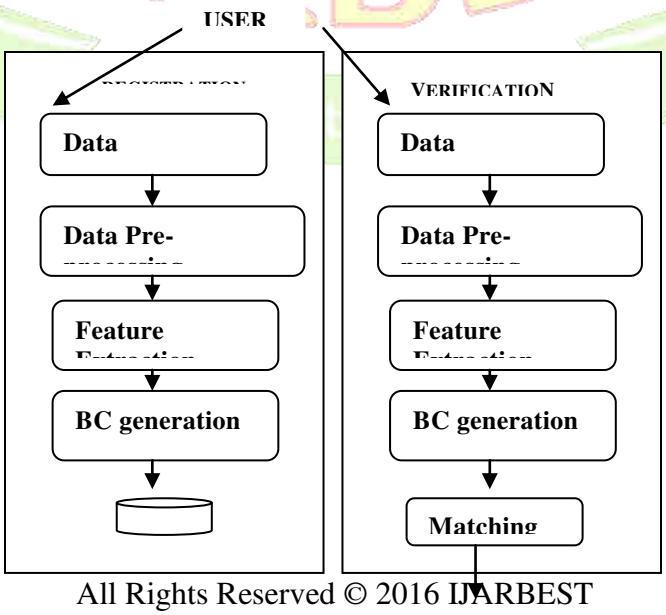
Fig: 1 Conventional Biometric System

II. BIOMETRIC AUTHENTICATION

The proposed authentication system contains two stages as shown in figure below. In registration phase, the user biometrics is sampled and fused with RS biometrics; from the fused biometrics a user's BC is generated and stored (in system database). Upon a verification request, user biometrics is resample and fused with the RS biometrics. Again from the fused biometrics a user BC is derived which is further compared to the stored BC. If the two BCs are close enough according to some distance metric, the user is authenticated as the individual.

In this approach, we present a unique BC generation method based on secure fusion of the user biometrics and the RS biometrics. The fusion process applies to different stages of biometric processing such as signal, feature or template level. The fusion based BC construction is more usable and flexible, while also secure, resilient to different attacks, and tolerant to the disclosure of both the RS and BC.

The process of selecting and setting Reference Subject in the system is given as follows. The Reference Subject can be a physical or logical. A physical RS is some object from which RS biometrics can be sampled on the fly, and a logical RS can be a biometric image. RS is a system wide object and managed by the authentication system, not by a user which frees user's burden on carrying or memorizing something.



Y/N

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Fig : 2 New BC based Authentication

The diagram for a system with RS at the authentication server is shown below. The user's biometrics is captured via camera of the client and sent to authentication server. Through some preprocessing , the user biometrics is fused with RS biometrics. The server matches the generated BC against BC stored in the BC database for an authentication decision.

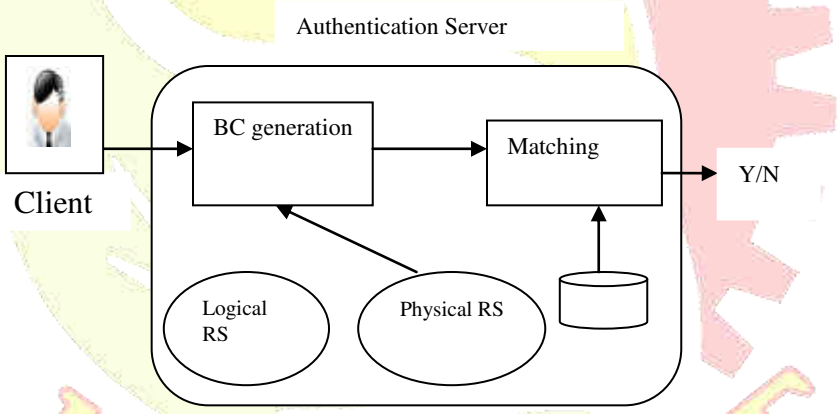
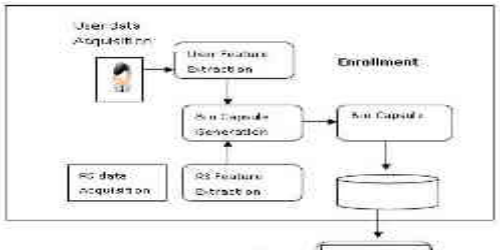


Fig : 3 Authentication system

III . DETAILED DESCRIPTION

The conventional biometric authentication collects biometric data from an enrolling user and extracts a biometric feature set from the biometric data; from the feature set a template is generated. Different from conventional biometric authentication approaches, during the enrolment phase, the proposed approach selects a reference feature set and computes the difference between the user's feature set and the reference feature set, then from the difference generates a BioCapsule to uniquely represent the enrolling user. In the verification phase, a query biometric feature set from a user and the same reference feature set are used to generate a query BioCapsule which is compared against the registered BioCapsule. If the registered BioCapsule and the query BioCapsule are within a certain distance, the user is successfully authenticated.



ST

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

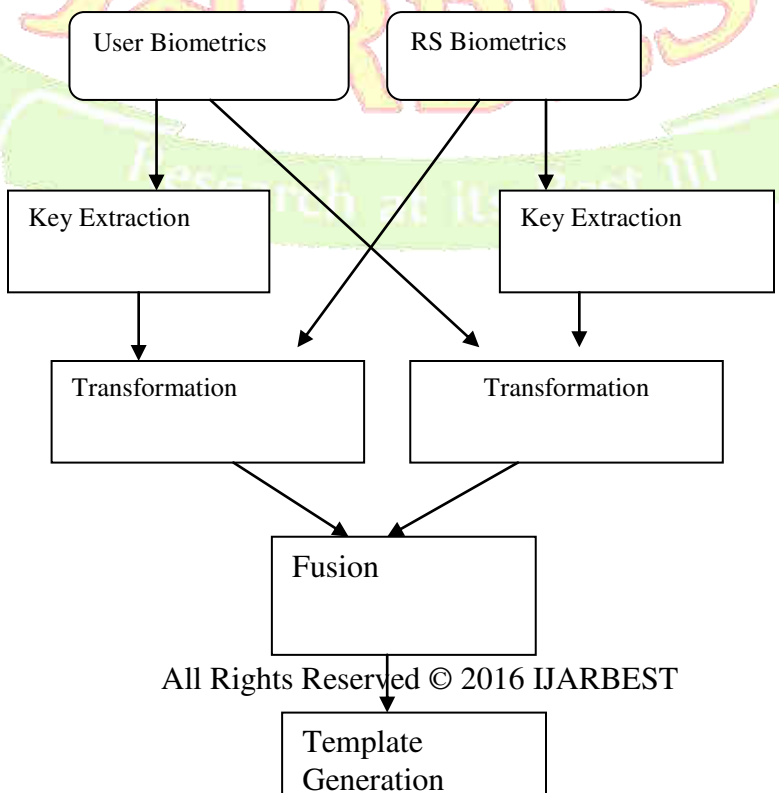
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

IV. BC DESIGN DESCRIPTION

The design criteria for the BC follow the requirements of biometric protection and design rationale for such BC generation includes the following: (a). The user and the RS are treated equally and the BC bears no hints that the user is weighted more than the RS; (b). Introduce user intrinsic key extraction for generating a user specific RS, thus reducing the risk resulting from sharing the common secret. (c). Extract keys such that key stability and distingushability can be balanced; (d). Make it difficult to get the user's biometric or RS by reversing a user's BC along with RS's biometric.

The BioCapsule(BC) generation model is shown in above figure. From user (Reference Subject) biometrics, user (Reference Subject) key is extracted and it is used for RS(user) biometrics transformation. Transformed user biometrics and RS biometrics are fused, and from fused biometrics a BC is generated. One critical property of biometric systems is diversity and cross matching resistance. It is likely that the user utilizes the same biometric across systems, thus it should be possible to build different versions of biometric credentials based on the same biometrics.



ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Fig : 5 BC generation model

A. KEY EXTRACTION

To create a personalized RS, a user intrinsic key is extracted from the user's biometrics and used as the transformation parameters to the RS. We Propose a light weight key extraction considering the following criterion.

1. To facilitate usability, the key is directly generated from the user biometrics, thus avoiding the need for a user to memorize a password or carry a token to provide transformation parameters.
2. Since the keys are not used for authentication, the BC approach does not require 100% stable and user distinct keys.
3. The conflict between key stability and distinguish ability should be optimally balanced, since it will create further impact on the fusion of biometrics.

Scheme-1.*The proposed key extraction scheme ExtK comprises the following procedures as shown in Fig. 4:*

• Extract iris signature: 1) Obtain processed iris described as a m−by−n matrix) as Fig. 4 (a). 2) Compute the grayscale-invariant local texture pattern (LTP)[22] (Fig. 4 (b)). The LTP computation starts with the definition of two windows: T window (X −by−Y) and B window which is the center of $(x - by - y)$ *in window T. The LTP for each pixel at coordinates* (i, j) *inside B is the pixel value Ii j subtracted by the mean AT of the pixel value of window T such as* $LTPi\,j = |Ii\,j - AT|$, $(i, j) \in B$. *Ii j is the grayscale value of the pixel at* (i, j) *in B, and AT is the mean grayscale value inside T. There is* $AT = 1N \Sigma(x,y) \in T$ *Ixy, with N thetotal number of pixels contained within T. 3) Generate a*

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

temporary signature (Fig. 4 (c)) ˜ s ∈Rm by averaging the LTP values of rows.

• Compute the mean V of the temporary signature. Given a system mean parameter M, obtain the iris signature by
s = (˜s−V)+M, with V obtained by V = 1m Σ ˜ s.
• Encode the iris signature s to a key (Fig. 4 (d)).

Encoding is an essential part of the key extraction. Each iris signature component si(1 ≤ *i* ≤ *m*) *is an average of a row of LTP values, thus theoretically* 0.0 ≤ *si*≤ 255.0 *(due to the pixel value range of grayscale image). However, the (iris) biometric pattern would not have dramatic contrast on local areas(indicated by the results of [22]). Practically, the iris signature component could possibly range from* 0.0 *to* 18.0 *(a tighter boundary used by our experiments). To encode such a si, we create an encoding book which is a mapping Map :{*0.0−18.0*} → {*−1,1*}n considering the tenth decimal part of si. This encoding book is created in system initialization and stored in the system as the system parameters. Am×n-length key is obtained by applying Map on s.*

The key extraction is applied on the preprocessed images. During the preprocessing, the iris image segmentation and polar transformation steps help migrate the scaling and distortion problems of biometric images. During the key extraction, LTP average computation is a rotation invariant process. So image scaling, rotation and distortion are migrated in the key extraction, and relatively stable keys can be produced. Moreover, the method of encoding will have an impact on the key stability and distingishability.

B. SECURE FUSION

Our goal of fusion aims to increase the security of the biometrics. Through the fusion, the RS biometrics hides the user biometrics, thus providing biometric security and preserving privacy. Our fusion equally treats the user and the RS and the BC bears no hints that the user is weighted more than the RS.

Scheme-2.On biometric inputs Fu, Fr, Ku and Kr where Fu,Fr∈ {Fi}n (f L ≤ Fi ≤ fU) and Ku,Kr∈ {Ki}n (Ki = 1,−1), through “secure fusion” the fused biometrics $F^{u,r}$(or $\{F_i^{u\,r}\}n$) is obtained by $F_i^{u,r}= (F_i^u \cdot Kri+F_i^r \cdot K_i^u \bmod (fU− f L))− f L$, (1) within F_i^u is one component of the user biometrics, F_i^r is one component of the RS biometrics, K_i^u is one key bit of the user key

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

and K_i^r is one key bit of the RS key. It is obvious that $F^{u,r} \in \{Fi\}n$ ($f^L \leq Fi \leq f^U$).

C. INTEGRATION OF SECURE FUSION WITH BIOMETRIC PROCESSES

The proposed fusion mechanism is a general procedure, which can be integrated with the existing biometric processes to generate BCs. And to show how the fusion fits into the biometric system. Figure shows a model of the integration of secure fusion with existing biometric processes at feature level. The model uses traditional preprocessing, feature extraction and template generation approaches without modification; it applies the secure fusion before the template generation and after the feature extraction. This property not only makes the proposed fusion more deployable but also keeps the same domain of inputs and outputs, thus theoretically enabling the fusion at other levels.

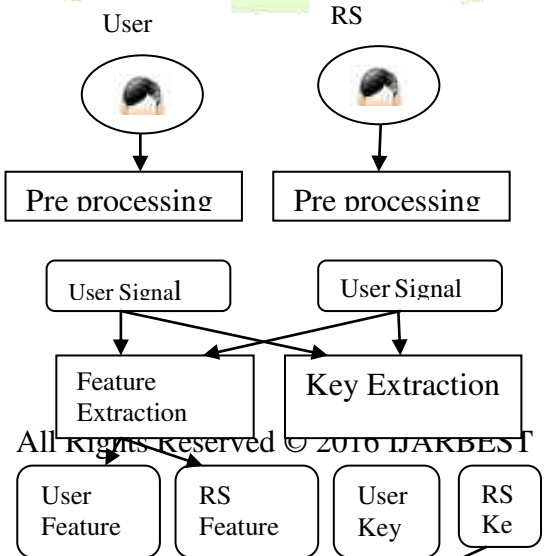
Scheme-3.*Given user biometric data D^u and RS biometric data D^r, a f eature−BCE ("BioCapsule Extractor") scheme is composed of the following procedures:*

• *Extract the user key K^u and the RS key K^r from D^u and D^r using* Scheme-1.

• *Extract features using 2D Gabor from biometric data by feature extraction procedure ExtF and obtain user biometric feature $F^u = ExtF(D^u)$ and RS biometric feature $F^r = ExtF(D^r)$.*

• *Fuse the user feature and the RS feature using K^u and K^r by the procedure defined in* Scheme-2. *Obtain $F^{u,r}$.*

• *Quantize the fused feature Fu,r into a BioCapsule BC^u.*



ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

V. CONCLUSION

In this paper, we proposed a user-friendly, secure, privacy preserving and revocable secure-fusion based biometric authentication method. The proposed approach involves key extraction: the extracted key is used in a "secure fusion" for mixing the user's biometrics and a reference subject's biometrics, and the fused biometrics is fed into an existing biometric system to generate a BioCapsule for authentication. The proposed BC mechanism has many desired features:

1) security analysis shows that the approach is secure and able to defeat various attacks, thus the security of the user biometrics is guaranteed
   and the user privacy is preserved;
2) experimental results prove the revocability of the proposed approach;
3) both security analysis and experimental results justify the cross-matching resistance of the proposed approach;
4) comparisons with existing approaches and the experimental results show comparable performance to traditional approaches and other BCS
   and CB systems;
5) the BC mechanism is generally applicable to typical biometric modules verified through experiments,
   thus, it can be fed into newly designed biometric systems to continuously enhance the authentication accuracy in the long run;

6) the cross-matching resistance enables the interoperability of the BC system, and it supports "one-click sign-on" across multiple systems by using a distinct RS; and
7) the system does not require user training, and is both easy to use and transparent to end-users since they are not required to remember a password or carry a token.

These features make the proposed BC mechanism a user centric authentication approach. We will continue to extend our study to other biometrics (e.g., face) and investigate the integration of the fusion at different biometric processing levels. We are also interested in extending the application of the proposed BC mechanism in a broader context, for instance, active and non-intrusive authentication.

VI. REFERENCES

[1]. Yan Sui, XukaiZou, Eliza Du, Feng Li, Design and analysis of a highly user-friendly,secure, privacy-preserving, and revocable authentication method, IEEE TRANSACTIONS.

[2]. http://en.wikipedia.org/wiki/usability.

[3] A. Ahmed and I. Traore. A new biometric technology based on mouse dynamics. *IEEE Transactions on Dependable and Secure Computing*, 4(3):165 –179, july-sept. 2007.

[4] T. Boult. Robust distance measures for face-recognition supporting revocable biometric tokens. In *7th International Conference on Automatic Face and Gesture Recognition*, pages 560–566, april 2006.

[5]. T. Boult, W. Scheirer, and R. Woodworth. Revocable fingerprint biotokens: accuracy and security analysis. In *IEEE Conference onComputer Vision and Pattern Recognition*, pages 1–8, june 2007.

[6]. X. Boyen. Reusable cryptographic fuzzy extractors. In *roceedings of the 11th ACM conference on Computer and communications security*, CCS '04, pages 82–91, New York, NY, USA, 2004. ACM.

[7]. J. Bringer, H. Chabanne, G. Cohen, B. Kindarji, and G. Zemor. Theoretical and practical boundaries of binary secure sketches. *IEEE Transactions on Information Forensics and Security*, 3(4):673–683, Dec. 2008.

[8]. I. Buhan, J. Breebaart, J. Guajardo, K. de Groot, E. Kelkboom, and T. Akkermans. A quantitative analysis of indistinguishability for a continuous domain biometric cryptosystem. In *Data Privacy Management and Autonomous Spontaneous Security*, volume 5939 of *Lecture Notes in Computer Science*, pages 78–92. 2010.

[9] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis. Constructing practical fuzzy extractors using QIM.*Technical Report TR-CTIT- 07-52*, 2007.

[10] R. Cappelli, A. Lumini, D. Maio, and D. Maltoni. Fingerprint image reconstruction from standard templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 29(9):1489–1503, sept 2007.

[11]. CASIA-IrisV1. http://biometrics.idealtest.org/.

[12]. A. Cavoukian and A. Stoianov. Biometric encryption.*Encyclopedia of Biometrics Springer*, 2009.

[13]. E. Chang, R. Shen, and F. Teo. Finding the original point set hidden among chaff. In *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, ASIACCS '06, pages 182–188, New York, NY, USA, 2006. ACM.

[14]. K. Cheung, A. Kong, D. Zhang, M. Kamel, and J. You. Revealing the secret of facehashing.*Lecture Notes on Artificial Intelligence, ICB 2006*, 3832:106–112, 2006.

[15]. K. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, and H. Lam. An analysis on accuracy of cancellable biometrics based on biohashing.*Lecture Notes on Artificial Intelligence, KES 2005*, 3683:1168–1172, 2005.