Dilip Menariya, D. B. Ojha / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 5, September- October 2012, pp.328-332

A vital application of security with biometric templates

Dilip Menariya1 and D. B. Ojha2
1Department of Computer Science
Mewar University Chittorgarh, Raj.India
2Department of Mathematics
Mewar University Chittorgarh, Raj.India

Abstract

In this Paper, We will discuss high level of biometric templates security is critical issue in personal base authentication system due to addition of error in transmission channel. Therefore we propose the framework of security of biometric template, based on the concept of encryption with secret key, based on braid group for unauthorized user access, Fuzzy error correction code determine and encounters error if any error is introduce during the transmission between users to database server We store the biometric templates in encrypted form both without the fusion of score level and decision level in database server Stenography is related to hide biometric templates with help of secret key based on braid groups.

Section 2 of this paper describe the state of Biometric System, and section 3 as our proposed method and finally Section 4 the Conclusion

Keywords:
Cryptography, Fuzzy Commitment Scheme, Biometric System Templates, Registration Phase, Verification Phase, Braid Groups

1.Introduction:

In Ancient times the people recognized each other by face, voice and their tongs movement. Today's scenario is different due to large increase in our population. As a byproduct of Biometric system is activity in our day to day communication ,we need more secure and authenticated communication. This requirement challenged us of think on biometric facilitation[5].Large number of government organizations, industry and non government organizations to must attain security with accuracy and error free Communication .The various properties exhibited by biometric system are uniqueness collectability, performance, acceptability and circumvention [3]

Various cryptography approaches are used for protection of biometric templates some are based on the hardware, some are software base, but common encryption technique AES and RAS cannot be used, because of large number of interclass variation in the biometric templates [5][6][16].Personal base authentication system use behavioral or physiological feature to identify one person form other. Many application for biometric system are available and all of them fall into two main functionality verification and identification [5][6][7].

A large number of errors in biometric templates are encountered in day to day communication due to environments change. Many approaches used to solve the noise problem which is one approach Fuzzy commitment scheme is one the scheme for solving the noise problem in biometric templates of a biometric recognition system, Jules and Wattenberg's Fuzzy Commitment Scheme[3]has been published to handling difference occurring
between two captured of biometric data, using error correcting code.

1.1 Related work

A handful of papers have been published so far in the area of key generation for biometric secure templates [3,4,10,12,13] Further more amount of work suggest biometric data gathering one or more actual biometric analysis and combine their results which increase the reliability of the biometric system[1][2]

2.Preliminaries

2.1 Biometric System

Biometric System measure and analyzes biological data and provide capability of identifying person based on Their intrinsic characteristics that can be physical such hand shape, a fingerprint, facial characteristics, voice, or DNA and proving that the aim is same that is registered in the biometric security system as a biometric template Basically Biometric–Based Personal authentication systems have five major components 1.Sensor, 2.Feature-Extractor, 3.Template Database Server, 4.Matcher, 5.Decesion Module. Sensor is the interface between users and Biometric System and its function is to scan biometric traits of the user. Feature extractor module process the scan biometric traits to extract the silent feature set, in some case Feature. Extractor is followed by quality assessment module for checking the sufficient quality of scan biometric traits In Biometric–Based Personal authentication systems works in two steps

Step1.Registered: In the first step the scan biometric traits of user R are processed and then stored in the database Server in Encrypted or secure form

Step2. Verification: In this step again new scan biometric traits of user R 'is captured and processed its then process for Comparing it with already Registered scan biometric traits as template and if both R and R' is matches then it is valid for Validation in biometric system otherwise Verification is invalid in biometric system Basically two types of errors are introduce In the Biometric–Based Personal authentication systems[14]

1. False Reject: Valid user (Probability of un matching of two traits R and R' of same user)
2. False Acceptance: Invalid User (Probability of matching of two traits R and R' of same user)

2.2 Error Correction Code

2.2.1 Definition: A Metric space is a set B with a distance function dist B X B→B^+= {0, ∞), which obeys the usual properties (symmetric, triangle inequalities, Zero distance between equal points) [13].

2.2.2 Definition : Let $B(0,1)^n$ be a code set which consists of a set code words b_i of length n ,The distance metric between any two code words b_i and b_j in B is defined By

dist (b_i , b_j)=$\sum_{r=1}^{n} |b_{ir} - b_{jr}|$ b_i , b_j Є C

This is known as Hamming Distance [13].

2.2.2 Definition: An Error Correction Function f for a code B Defined as

F(b_i)={b_j/dist(b_i ,b_j) is the minimum, over B-{b_i }}. Here, b_j= *f*(b_i) is called the nearest neighbor of b_i[16].

2.2.3 Definition: the measurement of nearness between two code word v and v' is defined by nearness (v,v')=dist(v.v')/n,.it is obvious that 0 ≤ nearness(v.v') ≤ 1[13].

2.2.4 Definition: the fuzzy membership function for a code v' to be equal to given v is defined as[17]

FUZZ (v') =0 if nearness (v,v') =z ≤ z_o ≤1)
=z otherwise

2.3 Braid Group

Emil Artin[11] in 1925 defined B_n ,the braid group of index n, using following generators and relations: Consider the generators σ_1 , σ_2 ……. , σ_n where σ_i represents the braid in which the$(i+1)^{st}$ string crosses over the i^{th} string while all other

Otherwise rejected strings remain uncrossed. The defining relations are

$\sigma_i \sigma_j = \sigma_j \sigma_i$ $|i-j| \geq 2$,
$\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ For $|i-j|=1$

An n-braid has the following geometric interpretation: It is a set of disjoint n-strands all of which are attached to two horizontal bars at the top and at the bottom such that each strands always heads downward as one walks along the strand from the top to the bottom. In this geometric interpretation, each generator σ_i represents the process of swapping the i^{th} strand with the next one (with i^{th} strand going under the $(i+1)^{th}$ one). Two braids are equivalent if one can be deformed to the other continuously in the set of braids. *Bn* is the set of all equivalence classes of geometric n-braids with a natural group structure. The multiplication *ab* of two braids *a* and *b* is the braid obtained by positioning *a* on the top of *b*. The identity *e* is the braid consisting of *n* straight vertical strands and the inverse of *a* is the reflection of a with respect to a horizontal line. So σ^{-1} can be obtained from by switching the overstrand and under-strand. Δ=(σ_I, σ_2,…….. σ_{n-1}) (σ_I, σ_2,…….. σ_{n-2}) (σ_I, σ_2) (σ_I)is called the fundamental braid. We describe some mathematically hard problems in braid groups. We say that *x* and *y* are conjugate if there is an element *a* such that *y* =axa^{-1} . For *m* <*n*; B_m can be considered as a subgroup of B_n generated by σ_I, σ_2,…….. σ_{m-1}

3. Proposed Scheme

Here we propose biometric based Authentication system using the concept of braid group based cryptosystem for security purpose and fuzzy commitment schema for error correction. We describe the complete process step of biometric Authentication system will achieve the high security and accuracy

Step 1: Scanning Scan the biometric traits of users using sensor at the user side 1. False Reject: Valid user (Probability of un matching of two traits R and R' of same user)

Step2: Quality Assessment Checking
This process is to check the quality is sufficient of scanned traits of user for further processing

Step3: Process for convert scans biometric traits of users to Message Bits
First the scan biometric traits images decomposed into w/8 *h/8 blocks where each one contain a fix number of pixel where w=height and h=height

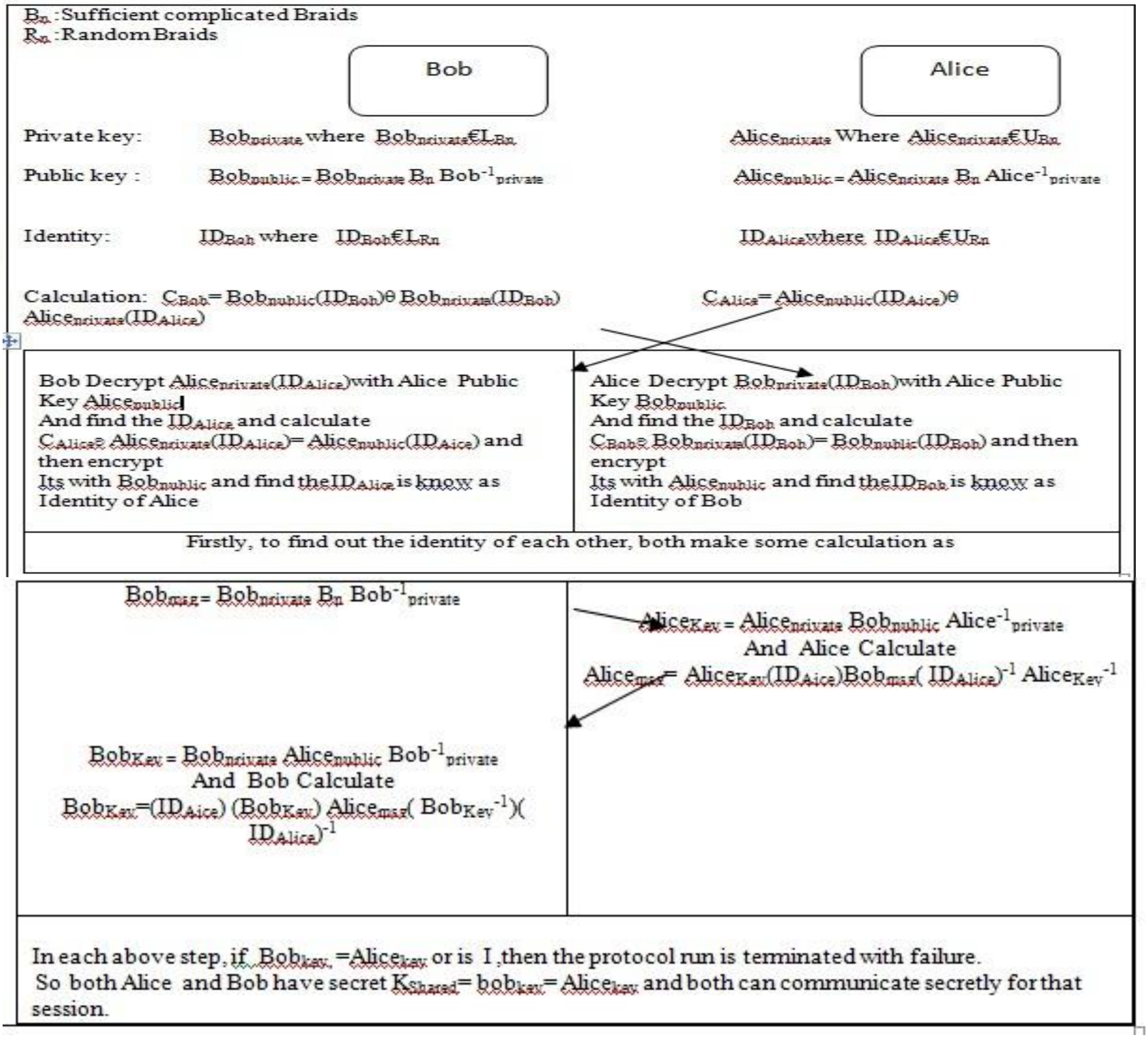
Step 4: Feature Extraction: At this step the silent feature are extracted from transformed block of biometric traits and generate the biometric templates as set of blocks

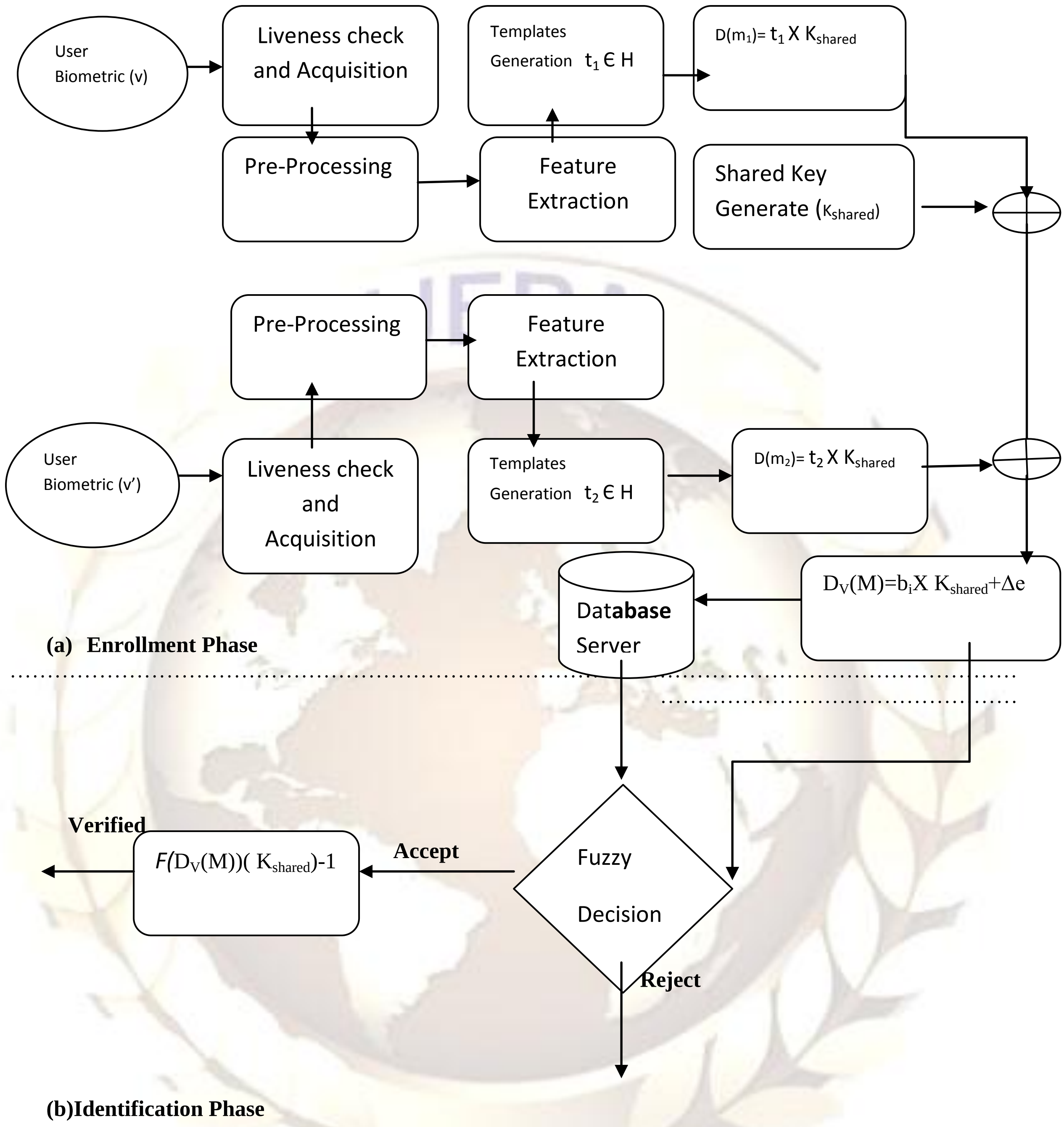
Step 5: Cryptographic key generation based on braid Group
Our scheme is made up of Five algorithms: setup, encryption, decryption, enrollment, verification

Initially set up phase: the environment is set up initially for generating public and private key,the secret key according to the algorithms using braid group at time t_o where event time is function $E=\{t_i,a_i\}$ of time and event algorithms and publish secret key between two parties requires for secures communication starting

Encryption: According to the commit phase, Bob commits to a Message m€ M to Alice, send as: c=commita lg(XOR,g(m1), $F_{kshared}$ (m),R) where $F_{kshared}(m)=m_1K_{shared}+e$, m is the K-bit message , $m=m_1\Delta m_2$, $F_{kshared}$ (m) is an n-bit unreadable text ,R is random braid (R can be changed in every Message that sent),e=h(m2),here h is an invertible function which maps m_2 in to an n-bit error vector of weight α

Decryption: in the open Phase Alice open the commitment at time t_2 which was sent by Bob at time $t_1$using the inverse procedure of commita lg(a_2)and Alice make a calculation c' using with help of secret key c'=commita lg(XOR,g(m1), $F_{kshared}$ (m),R)and check its time t3 result is same as the sent by Bob
Fuzzy decision Making
If (near(c,c') ≤Zo) if result is less than Accept otherwise reject





Figure(1)

Enrollment/Identification Phase of Biometric System

In the Identification phase

Biometric template's of user is u' at receive at receive side and compared it with one is stored previously in database if they are matching then user is validate for the system

In the Registration Phase

User biometric scan traits as biometric template as encrypted using secret key and send to Database server where database server found encrypted biometric templates with error are introduce in transmission channel so finally $E_v(M)$=Ma+@e

Step 6 error correction codes

If Error introduce in transmission of biometric template we can correct using fuzzy error correcting code if any error are introduce during the transmission of biometric templates

Receiver check the dist(t(c),c')>0 he realize that there is an error occur during transmission .receive applies the error correction function c':f(c)
The receive will compute nearness (t{c},f{c}=dist{t{c},f(c')}/n
Fuzz(c')=0 if nearness(c,c')=Z<Z<1
=z otherwise

4. Conclusion

This paper presents fuzzy commitment Method for error correcting code and braid group to compute a cryptographic key for biometric data .The method not only meet the security requirements, but also produce comparable accuracy to well-known K-NN classification method. Experiments on real biometric data, particular fingerprints and voice, are being conducted and will be reported in the near future.

REFERENCES

[1] K. NandaKumar (2008), "Multibio-metric Systems: Fusion Strategies and Template Security", PhD Thesis, Department of Computer Science and Engineering, Michigan State University, January.

[2] Anil K. Jain and Arun Ross (2004),"Multibiometric systems,"Communi-cations of the ACM, January, Volume 47, Number 1.

[3]. A. Juels and M. Wattenberg (1999), "A fuzzy commitment scheme", In Proceedings of the 6th Security, pp.28-36, November.ACM Conference on Computer and Communication

[4] M. Blum (1982), "Coin flipping by telephone: a protocol for solving impossible problems", Proc. IEEE Computer Conference, pp. 133-137.

[5] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, A. Ross (2004), "Biometrics: A Grand Challenge", Proc. of the International Conference on Pattern Recognition, Vol. 2, pp. 935–942, August.

[6] J. Wayman, A. Jain, D. Maltoni, D. Maio(2005),Biometric Systems:Technology, Design and Performance Evaluation, Springer-Verlag,.

[7] D. Maltoni, D. Maio, A. K. Jain, S.Prabhakar (2003), Handbook of Fingerprint Recognition, Springer,.

[8] A. Adler (2004), "Images can be regenerated from quantized biometric match score data", Proc. Canadian Conf. Electrical Computer Eng., pp.469-472.

[9] Sunil V. K. Gaddam, Manohar Lal (2010), "Efficient Cancellable Biometric A Multi- Biometric Template Security: An Application of Code-Based Cryptosystem

[10] Deo Brat Ojha, Ajay Sharma (2010), "A fuzzy commitment scheme with McEliece's cipher", Survey in Mathematics and Its Application Vol.5pp73-83.

[11] F. J. MacWilliams and N. J. A. Sloane (1991), Theory of Error-Correcting Codes. North Holland.

[12] A. A. Al-saggaf, H. S. Acharya (2007), "A Fuzzy Commitment Scheme", IEEE International Conference on Advances in Computer Vision and Information Technology, 28-30 November– India.

[13] Andrew Burnett, Adam Duffy, and Tom Dowling (2004) "A Biometric Identity Based Signature Scheme", eprint.iacr.org/2004/176.pdf

[14]. V. Pless (1982), Introduction to theory of Error Correcting Codes, Wiley, New York.

[15] T. van der Putte and J. Keuning (2000), "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned". Proceedings of the Fourth Working Conference on Smart Card Research and Advanced Applications.

[16] J. Bringer and H. Chabanne (2008), "An Authentication protocol with encrypted biometric data", Proc. Int. con cryptology. Africacrypt. pp-109-124,.