ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

A Review on Multi-Biometric Cryptosystem for Information Security

Bharti Kashyap[1], K. J. Satao[2]

M.Tech. Scholar, Computer Science and Engineering, Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India[1]

Professor, Computer Science and Engineering, Head Department of Information Technology, Rungta College of Engineering and Technology, Bhilai, Chhattisgarh, India[2]

Abstract: Multi-biometric system provides very important and secured methodology for enhancing the security level of information technology. The uniqueness of biometrics for any specific human being makes the identification system more secure.The traditional cryptosystem suffers from several problems such as key management, key privacy. Combining cryptography with biometrics removes such kind of problems and used for key generation. Here key may be generated by using two or more biometric factors.

Keywords*:* Biometrics; Encryption; Decryption; Cryptosystem; Multibiometrics

I. INTRODUCTION

Information Security is a method of protecting information from unauthorized access. Authentication plays very important role in the field of information security. Biometric cryptosystem is a technique in which Biometric features are used to generate encryption keys to encrypt data that may improve the security of data. The term biometrics is defined as "Automated recognition of individuals based on their behavioural and biological characteristics"[5]. It is used for secure identification and verification. At the time of verification or identification (identification can be handled as a sequence of verifications and screenings) the system processes another biometric input which is compared against the stored template, yielding acceptance or rejection [6].

Conventional cryptography uses encryption key, which are just bit strings long enough, usually 128 bit or more. These keys, either "symmetric," "public," or "private," are an essential part of any cryptosystem, for example, Public Key Infrastructure (PKI). A person cannot memorize such a long random key, so that the key is generated, after several steps, from a password or a PIN that can be memorized. The password management is the weakest point of any cryptosystem, as the password can be guessed, found with a brute force search, or stolen by an attacker. On the other hand, biometrics provides a person with unique characteristics which are always there[23]. Combining cryptography with biometrics removes such kind of problems and used for key generation.

Biometric template protection schemes which are commonly categorized as biometric cryptosystems (also referred to as helper data-based schemes) and cancellable biometrics (also referred to as feature transformation) are designed to meet two major requirements of biometric information protection [5]:

- Irreversibility: It should be computationally hard to reconstruct the original biometric template from the stored reference data, i.e., the protected template, while it should be easy to generate the protected biometric template.
- Unlinkability: Different versions of protected biometric templates can be generated based on the same biometric data (renewability), while protected templates should not allow cross-matching (diversity).

Biometric cryptosystems are designed to securely bind a digital key to a biometric or generate a digital key from a biometric[7], offering solutions to biometric-dependent key-release and biometric template protection [8,9]. Replacing password-based key release, Biometric cryptosystem brings about substantial security benefits. It is significantly more difficult to forge, copy, share, and distribute biometrics compared to passwords [5].

II. BIOMETRICS

Biometrics [18] is the identification of an individual using a distinctive aspect of their biology or behaviour. Two same type of biometric property [19] (traits) of different person can't be matched. It is divided in two characteristic (i) Physiological and (ii) behavioural. Behavioural aspect includes speech, keyboard typing, Signature and Physiological includes fingerprint, hand, eyes and face.

A. Fingerprint

This is very old style to authenticate any one like in forensic experts do in criminal cases. Fingerprint scanners are probably the most commonly used biometric systems. Similar systems include hand geometry or palm prints. Figure print of two humans never matched.

B. Face

The human face is also a feature that can be used by biometric systems. Human face recognition by analyzing the size and position of different facial features is being pushed for use at several airports to increase security.

Copyright to IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

Another possible approach is to make infrared recordings and analyze the resulting facial thermo gram.

C. Signature

Another behavioural aspect of a person usable by biometrical analysis [11] is the signature. The dynamic aspects can be seen as a set of unique features of a person. Other possible movable biometric input could be the rhythm and pattern of a person's walk.

D. Voice

A more behavioural individual aspect of humans are their voices. Everybody has a special mode and tone while speaking. Voice recognition tries to analyze these features and use them to identify a person.

E. Eye Iris

Another static property of individuals are eyes. One can either use pictures of the person's iris or use a retina scanner that scans blood vessels to create an individual data set.

Biometrics [20] make easier the jobs remember the all user id and passwords which are used in different web and system services used by human being for example: an identification system using biometrics would be: you approach an ATM with no card, no claimed identity, and no PIN. The ATM scans your iris and determines who you are and gives you access to your money or The ATM scans your iris and uses it as a password to authenticate you are the right owner of the card and therefore give you access to your money.

III. BIOMETRIC ENCRYPTION TECHNOLOGIES

The following are core Biometric Encryption schemes. The more detailed, files held by government and other various up-to-date overviews of Biometric Encryption technologies are presented organizations in [19,21].

A. Mytech 1

This is the first Biometric Encryption scheme [22]. It was developed using optical processing, but can also be implemented digitally. The key is linked to a predefined pattern, s(x), which is a sum of several delta-functions. Using s(x) and a fingerprint, f(x), one can create a filter, H(u) ¼ S(u) / F(u), in Fourier domain (S(u) and F(u) are the Fourier transforms of s(x) and f(x)). It is difficult to obtain either S(u) or F(u)from the stored filter H(u). On verification, if a correct fingerprint, F' (u)≈ F(u), is applied to the filter, it will reconstruct a correct output pattern, s'(x)≈ s(x) so that the key will be regenerated from the locations of the output correlation peaks. Unfortunately, this scheme turned out to be impractical in terms of providing sufficient accuracy and security.

B. Mytech 1

This is the first practical Biometric Encryption scheme [23]. Unlike Mytec1, it retains phase-only parts of S(u) and F(u) in the filter, H(u). The phase of S(u) is randomly generated, but not stored anywhere. As a result, the output pattern, c(x), is also random. The key, normally 128 bit long, is linked to c(x) via a lookup table and Error Correction Code. The filter, H(u), the lookup table, and the hashed key are stored in the helper data.

The system is error tolerant and translation invariant. The published version [23] used a simple repetition ECC, which makes the system vulnerable to several attacks, such as Hill Climbing [24].

However, a closer examination of the Mytec2 scheme shows that if the randomness of H(u) and c(x) is preserved on each step of the algorithm, the scheme is a variant of so-called ''permutation-based fuzzy extractor" as defined in [25]. Therefore, if a proper Error Correction Code (preferably, single block) is used instead of the repetition Error Correction Code, the system will be as secure as those types of fuzzy extractors.

C. Error Correction Code(ECC) Check Bit

This scheme, which was originally called ''private template,'' is a secure sketch (i.e., a key generation)[26]. A biometric template itself serves as a cryptographic key. To account for the template variations between different biometric samples, an (n, k, d) error correcting code is used. A number of (n-k) bits, called check bits, are appended to the template to map the k-bit template to an n-bit codeword. The check bits are stored into the helper data along with the hashed value of the template. The scheme is impractical, since it is required that $n < 2k$ from the security perspective. Such ECC would not be powerful enough to correct a realistic number of errors for most biometrics, including iris scan.

D. Biometrically Hardened Passwords

This technique was developed for keystroke dynamics or voice recognition [27]. A password that the user types or says is fused with a key (via a secret sharing scheme) extracted from a biometric component, thus hardening the password with the biometrics. The technique was made adaptive by updating a ''history file'' (which is, in fact, helper data) upon each successful authentication. However, the types of biometrics used did not allow for achieving good accuracy numbers.

E. Fuzzy Commitement

This is conceptually the simplest, yet the most studied, Biometric Encryption scheme [10]. A biometric template must be in the form of an ordered bit string of a fixed length. A key is mapped to an (n, k ,d) Error Correction Code code word of the same length, n, as the biometric template. The code word and the template are XORed, and the resulting n-bit string is stored into helper data along with the hashed value of the key. On verification, a fresh biometric template is XORed with the stored string, and the result is decoded by the Error Correction Code. If the codeword obtained coincides with the enrolled one (this is checked by comparing the hashed values), the k-bit key is released. If not, a failure is declared.

In a ''secure sketch'' (i.e., key generation) mode [7], the enrolled template is recovered from the helper data on verification, if a correct (yet different) biometric sample is presented.

Copyright to IJARCCE
DOI 10.17148/IJARCCE.2015.4577

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

The scheme seems to be one of the best for the biometrics where the proper alignment of images is possible, such as iris scan [28,29] and face recognition. For iris, the reported results are FRR(False Rejection Rate) = 0.47% at FAR(False Acceptance Rate) < 10–5 for a 140-bit key mapped to 2048-bit code word [13], and FRR = 5.6% at FAR < 10–5 (42-bit key) [29] for a poorer quality, yet more realistic, iris database.

F. Error Correction Code(ECC) Syndrome

In this spinoff of the Fuzzy Commitment scheme, called as Error Correction Code syndrome of (n-k) size is stored in the helper data[25, 19]. On verification, the enrolled template is recovered (i.e., the scheme works in the secure sketch mode).

G. Bio- Hashing (With Key Binding)

An ordered biometric feature set is transformed into a new space of a lower dimension by generating a random set of orthogonal vectors and obtaining an inner product between each vector and the biometric feature set [31]. The result (called ‘‘Bio hash’’) is binarized to produce a bit string. The random feature vectors are generated from a random seed that is kept secret, for example, by storing it in a token. The key is bound to the Bio hash via Shamir secret sharing with linear interpolation, or by using a standard Fuzzy Commitment scheme. Very good

H. Quantization using Correction Vector

This method, which was also called ‘‘shielding functions’’, is applied to continuously distributed and aligned biometric features [30]. For each feature, a residual is calculated, which is the distance to the centre of the nearest even-odd or odd-even interval, depending on the parity of the key bit. The correction vector comprising all the residuals are stored into the helper data. On verification, a noisy feature is added to the residual and is decoded as 1 or 0, if the resulting interval is odd-even or vice versa. The scheme can work with or without (if a noise level is low) a subsequent ECC. In general, storing a correction vector could make the scheme vulnerable to score-based attacks.

I. Fuzzy Vault

This is, probably, the only Biometric Encryption scheme that is fully suitable for unordered data with arbitrary dimensionality, such as fingerprint minutiae [6, 15]. A secret message (i.e. a key) is represented as coefficients of a polynomial in a Galois field, for example, GF(216). In the most advanced version[15], the 16-bit x-coordinate value of the polynomial comprises the minutia locations and the angle, and the corresponding y-coordinates are computed as the values of the polynomial on each x. Both x and y numbers are stored along side with chaff points that are added to hide real minutiae. On verification, a number of minutiae may coincide with some of the genuine stored points. If this number is sufficient, the full polynomial can be reconstructed using an Error Correction Code (e.g., Reed-Solomon ECC) or Lagrange interpolation. The polynomial reconstruction means that the secret has been successfully decrypted. The scheme works both in the key binding and the key generation (secure sketch) mode. The version of[15] also stores fingerprint alignment information. The best results for fingerprints show FRR = 6% – 17% at FAR = 0.02%.

The more secure version of Fuzzy Vault [30] stores high degree polynomial instead of real minutiae or chaff points. However, there are difficulties in the practical implementation of this version.

Unlike other Biometric Encryption schemes, the fuzzy vault actually stores real minutiae, even though they are buried inside the chaff points. This could become a source of potential vulnerabilities. The system security can be improved by applying a secret minutiae permutation controlled by a user’s password [19].This ‘‘transform-in-the-middle’’ approach is applicable to most Biometric Encryption schemes.

IV. MULTIBIOMETRIC CRYPTOSYSTEM

Biometric cryptosystems are designed to securely bind a digital key to a biometric or generate digital key from a biometric[8].

Binding of multiple biometric cryptosystems may be used (e.g., Fingerprint, Iris and face) together is termed as Multibiometric cryptosystem. Nowadays Multibiometric systems are mostly used in many large-scale biometric applications. Multibiometric is a fusion of two or more single biometric traits like Finger Print, Iris. Due to the presence of multiple independent features these systems are expected to be more reliable.

Multibiometric systems are being increasingly deployed in many large scale biometric applications because they have several advantages such as lower error rates and larger population coverage compared to uni-biometric systems. However, Multibiometric systems require storage of multiple biometric templates (e.g., fingerprint, iris, and face) for each user, which results in increased risk to user privacy and system security. One method to protect individual templates is to store only the secure sketch generated from the corresponding template using a biometric cryptosystem. This requires storage of multiple sketches.

V. ADVANTAGES

As compared with traditional single biometric authentication, Multibiometric systems offer several advantages.

1) Improve accuracy: Combining the evidence obtained from different sources using an effective fusion scheme can significantly improve the overall accuracy of the biometric system. The presence of multiple sources also effectively increase the dimensionality of the feature space and reduce the overlap between the feature spaces of different individuals[1].

2) *Resistance to spoofing:* Multibiometric systems are more resistant to spoof attacks because it is difficult to simultaneously spoof multiple biometric sources[2].

3) Noisy Data: The availability of multiple sources of information considerably reduce the effect of noisy data. If

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

the biometric sample obtained from one of the source is not of sufficient quality during a particular acquisition, the samples from other source may still provide sufficient discriminatory information to enable reliable decision-making[3].

Multibiometric systems give anti-spoofing measures by making it difficult for an intruder at the same time spoof the multiple biometric traits of a legitimate user. What is more, unlike passwords or tokens, compromised biometric templates are not revocable. Due to this understanding, template security is necessary to protect both the privacy of the users and the unity of the biometric systems [4].

VI. KEY GENERATION METHOD

Cryptographic systems require a secret key or a random number which must be tied to an individual through an identifier. This identifier indeed could be a globally unique user id or biometric data. Generating user ID-based key or random number is straightforward and the techniques could easily be found in literature.[32] But generating user-based cryptographic keys includes several of approaches.

A. User Dependant Key Generation

PRNG (pseudo random number generator). The resulting
pseudorandom number can be used directly as a key or adjusted with user-dependent data. User-dependent key may consist of user ID or biometric data. In order to make the key depends on a specific user, two ways could be applied. First the key generation algorithm could be modified by using the user dependent data. Second PRNG could be modified. PRNG
Modification is accomplished using a front-end or back-end approach. In front-end manner, the definition of the seed value (which is used to create a random key) is extended to include a user-specific data component. In back-end manner, pseudorandom numbers are treated as intermediate values and processed further. In this section we will describe three methods where user-specific data is biometric data. Biometric template of user is denoted by T which

1) Method 1: This method is based on pairing the biometric data with random numbers. The seed v*alue of* PRNG consists of a secret random value R and T, seed=(R, T). In order to eliminate any structure in the seed a complex function f is applied. Then the seed value is defined as seed=f(R, T) where f is the one-to-one mixing function. By the way, created pseudorandom numbers are not
adversely affected by the composition of the seed value.

2) Method 2: In this method R and T are inputs to a more complex function that generates an n-bit pseudorandom number S which could be used directly as a key or as an input to key generation algorithm.
The al*gorithm is as follows:*

- Generate a secret pseudorandom number R by using PRNG.
- Let Z=H(R,T) || H(R+1,T) || H(R+2,T) || ... || H(R+a ,T) where a=[n/h]-1. Here H is a strong collision-resistance one way hash function (such as SHA-1). H generates an h bit output from any length input. The symbol "||" denotes the concatenation operation.
- Let S be n specific (eg, leftmost) bits of Z.

Since H is a strong collision-resistance one-way hash function it is not feasible to derive either R or T from Z. This increases the security of the scheme. In practice this method is designed for the user to store the value of R and generate S from R and T on demand. S might be an encryption key. In this case, R might be encrypted and stored within a cryptographic subsystem.

3) Method 3:

In this method R and T are combined via simple function (XOR) to generate an n-bit secret pseudorandom number S. The algorithm is as follows:

- Let Z=H(R,T) || H(R+1,T) || H(R+2,T) || ... || H(R+a,T) where a=[n/h]-1.
- Let X be n specific bits of Z.
- Let R be an n-bit secret pseudorandom number, where R is either specified by the system or generated in his step using a PRNG.
- S=R (XOR) X.

4) Method 4: Whenever the user needs to encrypt or decrypt with S, T must

As can be seen, due to the hash function collision probability the previous three methods do not guarantee that a key or random number derived for a user will be unique. The probability of two users ending up with the same pseudorandom number is still present and will be quite small if n and h are chosen to be large. In this method, the user can prove or cannot deny that a key is one belonging to, or generated in, his/her designated space of keys or random numbers. In this method we assume that the value to be generated is n-bit long where (n > t). The algorithm is a two step process:

- Divide the space 2n into 2t subspaces. Note that each subspace correspond to a particular individual based the specific biometric data.
- Choose n-bit value at random from the user's subspace. The first step of the algorithm is realized by taking the first t bits from the biometric data representation and allow the remaining n - t bits to take any value. It would be advantageous to employ a mixing function to mix the user-dependent key or random number so that the secret entropy in it will be uniformly distributed over the entire key or random number.

VII. RELATED WORKS

Nagar et al. [1] proposed the feature level fusion of multibiometric templates. For higher level security, the multiple traits of an individual are combined into a single secure sketch. There are three phases in this paper. First phase is to obtain biometric characteristics and convert to

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

binary string, and in second phase is to combining the above biometric traits and third phase is securely sketching. Fuzzy vault and fuzzy commitments are algorithms used in this paper for decoding. The former uses a Berlekamp-massae algorithm and latter decoding depends on the crossover probabilities.

Juels et al. [11] proposed fuzzy commitment scheme for providing authentication for biometric systems. It is used in biometric data for error tolerance. It converts the data into hash functions and stores the data in a server. This deals with the leading problems in authentication of biometric systems.

Yau [12] proposed classifier fusion problem which is the process of merging fingerprint and speech biometric decisions. They suggest constructing the various combinations of hyperbolic functions by network model. The suggested hyperbolic function is to demonstrate the approximation capability. At last it is exercised to combining the fingerprint and speech identification and verification to generate the best results.

Fu et al. [13] proposed a method of Multibiometric cryptosystem, by binding the multiple features of biometrics to cryptography. There are two levels of combining, i.e. combining at the biometric level and combining at the cryptographic level. Shannon entropy is used to afford security. Accuracy and efficiency was also evaluated and it was compared with other systems.

Zhang et al. [14] proposed an encryption scheme and authentication scheme. This scheme is referred as mSEAS.

The authentication and encryption scheme is based on the Multibiometric data, with the intention of considering the privacy, unforg Multi-biometric system provides very important and secured methodology for enhancing the security level of information technology. The traditional cryptosystem suffers from several problem such as key management, key privacy. Use of biometric templates removes such kind of problem and provides faster and little complex procedure for encryption of private messages by private key. Here private key is generated by using two or more biometric factor .Elliptic Curve Cryptography is used as a cryptographic algorithm that provides key generation and encryption, decryption of messages, and authentication. In addition it establishes the fuzzy extractor algorithm. By means of biometric string reader the information is excerpted. This can be used in environment of biometric authentication.

Jain [15] observed the various types of score normalization technique. Hand geometry, fingerprint, face traits were used in this paper for authentication. Normalization techniques like z-score, min-max, tanh methods were used. This performs better, strong and efficient when compared to other systems.

Sumathi [16] proposed the Multibiometric authentication using Discrete wavelet transform (DWT). A new novel technique based on DWT for identification of user. It utilizes support vector machine for the absolute result. The efficiency of the system is analysed in terms of False Acceptance Rate and Genuine Acceptance Rate.

Veeramachaneni [17] proposed an adaptive multimodal biometric management algorithm for multimodal biometric. It is a developing approach that moves towards the biometric security of sensor management. It is adaptive because, depends on the user requirement it alters in time. To make use of the best results in the system performance it selects the fusion rule. It also uses the sensor operating points.

U. Mahalakshmi1[18] proposed a method for generating a onetime password using Multibiomtric cryptosystem. Secured authentication is based on Multibiometric cryptosystems. For Multibiometric, the various traits of an individual are used. Elliptic curve cryptography (ECC) technique is used to generate curve and key. For providing a secured authentication this paper incorporates the use of one time password (OTP). The proposed system can be applied in financial based application services. When a user provides his Multibiometric traits the images are resized and fused into a single image. A matrix is generated using fixed points from the fused image, elliptic curve and key is generated using parameters. Also in this, the curve is overlapped with fused image and one time password (OTP) is generated .

VIII. CHALLENGES

Technologically,[32] Biometric Encryption is much more challenging than conventional biometrics, since most Biometric Encryption schemes work in a ‘‘blind’’ mode (the enrolled image or template are not seen on verification). As Biometric Encryption advances to the next phase of creating and testing a prototype, the following issues need to be addressed:

- Biometric modalities that satisfy the requirements of high entropy, low variability, possibility of alignment, and public acceptance should be chosen. At present, the most promising biometric for Biometric Encryption is iris followed by fingerprints and face.
- The image acquisition process (the requirements are tougher for Biometric Encryption than for conventional biometrics) must be improved. Biometric Encryption must be made resilient against attacks.
- The overall accuracy and security of BE algorithms must be improved. Advances in the algorithm development in conventional biometrics and in Error Correct Codes should be applied to Biometric Encryption.
- Multimodal approaches should be exploited. Biometric Encryption applications should be developed.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 5, May 2015

IX. CONCLUSION

The use of biometrics will become an increasingly essential part of our lives, changing the traditional method of transactions like tokens, usernames and passwords. E-transactions are the way of the future. Financial institutions and banks, along with many other organisations, are being forced to modify the techniques with which they carry out business. These technological changes have brought with them E-transaction hackers and identity theft. These cyber crimes have become common and are only expected to increase. However, a more efficient means of protecting identities and transactions is required to be implemented and the best method of providing such secure identification at this time is by employing biometric systems. Using multiple biometrics in one application is one of most interesting aspects of the research.

REFERENCES

[1] Nagar A, Nandhakumar K et al. (2012). Multibiometric cryptosystem based on feature level fusion, IEEE Transaction on Information Forensics and Security, vol 7(1), 255–268.

[2] Abhishek Nagar, Karthik Nandakumar, and A. K. Jain, "Multibiometric Cryptosystems based on Feature Level Fusion", *IEEE transactions on Systems, manand cybernetics*, vol. 07, no. 01, pp.255-268, February 2012.

[3] Anil K. Jain, Arun Ross, Umut Uludag "Biometric template security – challenges and solutions", http:// biometrics.edu M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, "High resolution fiber distributed measurements with coherent OFDR," in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

[4] Abaza Ayman, and Ross Arun, "Quality Based Rank-Level Fusion in Multibiometric Systems," in *Proc. third IEEE Interna`tional Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Washington DC, USA, September 2009. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/.

[5] A survey on biometric cryptosystems and cancelable biometrics Christian Rathgeb* and Andreas Uhl,Springer 2011.

[6] Jain AK, Ross A, Prabhakar S: An introduction to biometric recognition. IEEE Trans Circ Syst Video Technol 2004, 14:4-20.

[7] Cavoukian A, Stoianov A: Biometric encryption. Encyclopedia of Biometrics Springer; 2009.

[8] Cavoukian A, Stoianov A: Biometric encryption: the new breed of untraceable biometrics. Biometrics: Fundamentals, Theory, and Systems Wiley, London; 2009

[9] Jain AK, Ross A: U Uludag, Biometric template security: Challenges and solutions. Proc of European Signal Processing Conf (EUSIPCO) 2005.

[10] Juels A, and Wattenberg M (1999). A fuzzy commitment scheme, Proceedings of the Sixth ACM Conference On Computer and Communications Security, Singapore, 28–36.

[11] Yau W (2004). Combination of hyperbolic functions for multimodal biometrics data fusion, IEEE Transaction on System, Man, Cybernetics, vol 34(2), 1196–1209.

[12] Fu B, Yang S X et al. (2009) Multibiometric cryptosystem: Model structure and performance analysis, IEEE Transactions on Information Forensics Security, vol 4(4), 867–882.

[13] Zhang M, Yang B et al. (2011) Multibiometric based secure encryption and authentication scheme with fuzzy extractor, International Journal of Network Security, vol 12(1), 50–57.

[14] Jain A, Nandakumar K et al. (2005) Score normalization in multimodal biometric systems, The Journal of Pattern Recognition Society, vol 38(12), 2270-2285.

[15] Sumathi S, Hemamalini R (2012). Multibiometric authentication using DWT and score level fusion, European Journal of Scientific Research, vol.80(2), 213–223.

[16] Veeramachaneni K, Osadciw L A et al. (2005). An adaptive multimodal biometric management algorithm, IEEE Transactions on systems, Man, and Cybernetics—Part C: Applications and Reviews, vol 35(3), 344–356.

[17] U. Mahalakshmi1 and V. S. Shankar Sriram "An ECC Based Multibiometric System for Enhancing Security". INDJST Vol 6 (4) April2013.

[18] Koichiro Niinuma, Unsang Park and Anil K. Jain, "Soft Biometric Traits for Continuous User Authentication," IEEE Transactions on Information Forensics and Security, Vol. 5, No. 4, pp. 771-780, Dec. 2010.

[19] Anil K. Jain, Patrick Flynn and Arun A. Ross, "Handbook of Biometrics," Springer Science, ISBN-13: 978-0-387-71040-2, 2008.

[20] Massimo Tistarelli, Stan Z. Li and Rama Chellappa, "Handbook of Remote Biometrics for Surveillance and Security," Springer Science, ISBN 978-1-84882-384-6, 2009 .

[21] Cavoukian, A., Stoianov, A.: Biometric Encryption: The New Breed of Untraceable Biometrics. In: Boulgouris, N.V., Plataniotis, K.N., Micheli-Tzanakou, E. (eds.): Biometrics: fundamentals, theory, and systems. Wiley, London (2009)

[22] Tomko, G.J., Soutar, C., Schmidt, G.J.: Fingerprint controlled public key cryptographic system. U.S. Patent 5541994, July 30, 1996 (Filing date: Sept. 7, 1994

[23] Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., Vijaya Kumar B.V.K.: Biometric Encryption (Chapter 22). In: Nichols, R.K. (ed.): ICSA Guide to Cryptography, McGraw-Hill New York, (1999)

[24] Adler, A.: Vulnerabilities in Biometric Encryption Systems. In: Audio-and video-based Biometric Person Authentication (AVBPA2005). Lecture Notes in Computer Science, vol. 3546, pp. 1100–1109. Springer, New York (2005).

[25] Dodis, Y., Reyzin, L., Smith, A.: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and other Noisy Data. In Cachin, C., Camenish, J., Proc. Eurocrypt 2004, pp. 523–540 Springer-Verlag, NY (2004).

[26] Davida, G.I.,Frankel,Y.,Matt,B.J.:On enabling secure applications through off-line biometricidentification. In:Proceedingsof the IEEE 1998Symposium onSecurity andPrivacy, pp. 148–157, Oakland, CA (1998).

[27] Monrose, F., Reiter, M.K., Wetzel, S.: Password hardening based on keystroke dynamics. Int. J. Inform. Secur. 1(2), 69–83 (2002)

[28] Hao, F., Anderson, R., Daugman, J.: Combining Crypto with Biometrics Effectively. IEEE Trans. Comput. 55(9), 1081–1088 (2006)

[29] Bringer, J., Chabanne, H., Cohen, G., Kindarji, Z'emor, G.: Optimal iris fuzzy sketches. In: IEEE First International Conference on Biometrics: Theory, Applications, and Systems, BTAS'07, Washington, DC, 27–29 Sept, (2007).

[30] Tuyls, P., Škori • , B., Kevenaar, T. (eds.): Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting. Springer, London (2007).

[31] Teoh, A.B.J., Ngo, D.C.L., Goh, A.: Personalised cryptographic key generation based on FaceHashing. Comput. Secur. 23, 606–614 (2004).

[32] Ann Cavoukian and Alex Stoianov " Biometric Encryption Chapter from the Encyclopedia of Biometrics ". Office of the Information and Privacy Commissioner, Toronto, Ontario, Canada