INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

IMPLEMENTATION OF FUZZY VAULT USING IRIS TEXTURES

[1]Ramesh Kumar Sharma, [2]Surjeet Kumar, [3]Satyendra Nath Mandal, [4]Arun Prasad Burnwal

[1]Department. of Computer Science and Engineering, Bengal College of Engineering and Technology Durgapur (W.B), India-713212, sharmarameshdhn@gmail.com
[2]Department. of Computer Science and Engineering, Bengal College of Engineering and Technology Durgapur (W.B), India-713212, surjeetk05kgec@gmail.com
[3]Department. of Information Technology, Kalyani Government Engineering College, Kalyani, Nadia (W.B), India-741235, satyen_kgec@rediffmail.com
[4]Department of Mathematics, GGSESTC, Bokaro, Jharkhand, India-827013, apburnwal@yahoo.com

Abstract: - Combination of cryptography and Biometrics to provide high security. Biometric templates play the main role in authenticating the individual identification. Biometric traits like fingerprint, retina and iris have certain merits when compared to other biometrics. Iris provides high speed of comparison and it is well suited for one-to-many identification. The iris templates are more stable or have more template longevity. Iris templates need not be updated frequently, a single enrolment can last a lifetime .This paper explores the biometric based authentication is blended with cryptography output called fuzzy vault which provides a high security. The proposed algorithm aims at generating a secret encryption key from iris textures and data units for locking and unlocking the vault. The algorithm has two phases: The first to extract binary key from iris textures, and the second to generate fuzzy vault by using Lagrange interpolating polynomial projections.

Keywords: Biometric template; IRIS; Fuzzy vault; Polynomial reconstruction; MATLAB coding.

1. Introduction

This paper explores the biometric based authentication. The word biometrics is derived from the Greek words namely “Bio” meaning life and “metrics” meaning measurements. No doubt, IRIS is the biometric traits most widely deployed for authentication. IRIS provides high speed of comparison and it is well suited for one to many identification. IRIS biometric is more reliable and accurate as compared to the other biometric [1], [2], [3]. Current cryptographic algorithms require their keys to be very long and random for higher security, that is, 128 bits for Advanced Encryption Standards [4]. These keys are stored in smart cards and can be used during encryption/decryption procedures by using proper authentication. There are two major problems with these keys: One is privacy and second is data protection.

One of the most prominent solutions to solve this issue is the fuzzy IRIS vault, which allows error tolerant IRIS authentication while preserving the privacy of the biometric features. It belongs to the class of biometric template protection techniques. Biometric templates play the main role in authenticating the individual identification and is based on the fuzzy vault scheme of juels and sudan. Which applies Reed-Solomon decoding to redundantly bind the biometric template to a randomly selected secret polynomial.

The IRIS templates are more stable throughout life and iris templates need not be updated frequently. A single enrolment can last a lifetime. IRIS authentication is based on minutiae, which is specific features of the iris pattern.
Rest of this paper is organized as follows: Section 2 provides background of the proposed method. Section 3 addresses the preliminary of the proposed. The details of the proposed method is describes in Section 4. Section 5 describes experimental results. Finally, Section 6 concludes the paper.

2. Background

The fuzzy vault has been proposed by Juels and Sudan in theoretical security analysis for the general fuzzy vault scheme by giving estimate for the number of candidate polynomials that would fit with a given vault. It is an error tolerant authentication scheme based on the set of private attributes u1. . . . .u2.while the reference data store the vault allow performing the authentication check , it does not reveal these attributes. These scheme deploys a variant of reed-Solomon decoding and also hides the private user data among a large number of random chaff points. There are two operations in fuzzy vault i.e. Encoding and Decoding.

1. Locking the Vault: While encoding, a secret key is locked by an unordered set G from the biometric sample. A polynomial P is then constructed by encoding the secret key and evaluated by all the elements of the unordered set. A random chaff point set C, which is 10 times the genuine points is taken. Then the union of the chaff point set C which do not lie on polynomial and the unordered set G is performed to create a vault V i.e. V = G U C This union of the chaff point set hides the genuine point set from the attacker and thus securing the secret data and user biometric template simultaneously.

2. Unlocking the vault: While decoding, the secret key S can be retrieved from the vault by providing query template which is represented by another unordered set G‟. The set G‟ had to be almost equal to set G. If the difference between set G and set G' was very small i.e. substantial overlap, then the user can identify many points in V that lie on P. If sufficient number of points can be identified then the polynomial P can be exactly reconstructed by using an error correction scheme and thus generating the secret data securely/decoding the secret keys securely. If G‟ does not overlap substantially with G, it is infeasible to reconstruct P and the authentication is unsuccessful. This crypto-biometric system is known as fuzzy because the vault will get decoded even for very near values of G and G' and the secret key S can be retrieved. Therefore fuzzy vault is more suitable for biometric data which show inherent fuzziness as biometric data contain the intra-variations of the same person. Also, the fuzzy vault scheme requires pre-aligned biometric templates that are properly aligned with the input biometric data.

3. Preliminaries

Fuzzy logic is the basic preliminary of this proposed method. Fuzzy logic [5], [6], [7], [8] is part of soft computing method [9], [10] which is a part of artificial intelligence technique [11], [12]. It was introduced by Zadeh which became mathematical discipline [13] to express human reasoning in rigorous mathematical notation. It is a multi-valued logic that allows intermediate values to be defined between conventional evaluations like true/false, yes/no, high/low, small/big, short/long etc. Many authors [14], [15], [16], [17], [18] used fuzzy logic in ad-hoc network.

Fuzzy logic considers as an intelligent system [19], [20], [21] and has been shown to yield promising results for many applications that are difficult to be handled by conventional techniques [22], [23]. Fuzzy logic is used to convert crisp data to fuzzy data by the help of fuzzification method and process this data by the helps of inference engine after processing data convert it again into crisp data by the helps of defuzzification. Inference is an assumption or conclusion that is rationally and logically made, based on the given facts or circumstances. So it is based off of facts, so the reasoning for the conclusion is often logical. And inference engine is used to apply reasoning to compute fuzzy outputs. The main ethics of fuzzy logic system can easily implement human experiences and preferences vie membership functions and fuzzy rules, from a qualitative description to a quantitative description that is suitable to solve any complex problem. Fuzzy membership functions can have different shapes depending on the designer's preference and/or experience. The fuzzy rules [24], [25], [26]] which describe the control strategy in a human-like fashion, there are four modes of derivation of fuzzy control rules: (1) expert experience and control engineering knowledge, (2) behaviour of human operators, (3) derivation based on the fuzzy model of a process, and (4) derivation based on learning.

4. Proposed Method

The proposed method involves mainly two phase - one is feature extraction and the other is polynomial projection to generate vault. A random key combined with lock/unlock data both of 128 bit are extracted from iris textures and are projected on to a polynomial with cyclic redundancy code for error checking. To these projections, chaff points are added and scrambled to obtain vault. The proposed method is attempted to provide security, diversity and revocability to unibiometric and multibiometric templates by a hybrid approach. The security of the proposed fuzzy vault method is measured by min-entropy which is expressed in terms of security bits. The proposed method considers fuzzy vault scheme to provide security to biometric templates. The fuzzy vault is password hardened to impart revocability to biometric templates.

4.1. IRIS Localization

First the eye image [27], [28], [29] is required then we converted to gray scale and its contrast is enhanced using histogram equalization. Algorithm based on thresholding and morphological operators, is used to segment the eye image and to obtain region of interest. Initially the pupil boundary and limbic boundary were found to fix the iris area. Many algorithms are available today to fix these boundaries. But one of the easiest and simple algorithms is by using morphological operations. By using bit plane method, we can find the pupil boundary. The LSB bit plane is used to determine the pupil boundary. Similarly the limbic boundary can be obtained by calculating standard deviation windows in vertical and horizontal directions. Further the iris image is normalized to a standard size of (87x360) using interpolation technique.

4.2. Morphology Operation

Thinning is a morphological operation that is used to remove selected foreground pixels from binary images. It can be used for several applications, but is particularly useful for skeletonization . In this mode it is commonly used to tidy up the output of edge detectors by reducing all lines to single pixel thickness. Thinning is normally only applied to binary images, and produces another binary image as output. The thinning operation is related to the hit-and-miss transform. Here, eye image is converted into binary image which is help for password creation and protection. It is shown in Figure 1 (a) and (b).

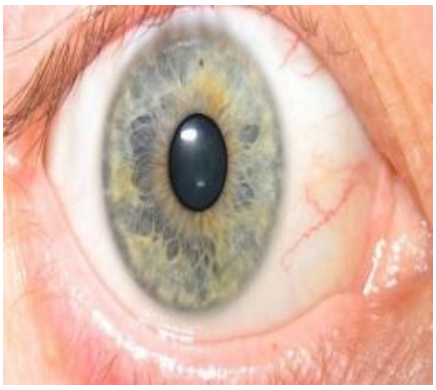


Figure 1: (a) Eye image.

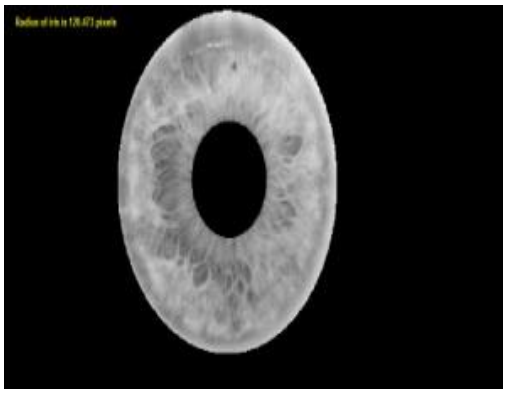


Figure 1: (b) Binary image.

4.3. Requirements for Biometrics

Physical and Behavioural biometrics should possess certain characters that make them suitable to be employed in biometric system s. Requirements are separated as theoretical and practical and are as follows:

1. **Universality:** Each person should have the biometric characteristics.
2. **Uniqueness:** Each person has a unique identification.
3. **Permanence:** The characteristics remain the same over life time.
4. **Collectability:** Easy to measurement.
5. **Performance:** To check verification accuracy, error, computing speed.
6. **Acceptability:** Degree of approval of a technology.
7. Circumvention: The degree of security of the system given fraudulent attacks.

Biometric samples captured during enrolment phase are stored in the form of templates. Biometric templates play important role in the biometric authentication process. The iris-based technique has a much higher verification accuracy than other biometric.

4.4. Advantages of using Biometrics

1. No need to memorize passwords.
2. Unique physical or behavioural characteristic.
3. Cannot be borrowed, stolen, or forgotten.
4. Requires physical presence of the person to be identified.
5. Better than password/PIN or smart cards.

Bio-cryptography techniques protect a secret key using biometric features or by generating a key from biometric features. In such systems, some public information is stored. Both the secret key and biometric template are hidden in the public information. However, it is computationally impossible to extract the key or template from the public information directly. There are two subcategories of bio-cryptography techniques: key binding and key generating. If public information is derived from binding the secret key and biometric template, it is key binding. Example fuzzy vault [30], [31], [32], [33].

4.5. Fixing the Center & X/Y Coordinates

Black hole search method is used to detect the center of pupil. The center of mass refers to the balance point (x, y) of the object where there is equal mass in all directions. Both the inner and outer boundaries can be taken as circles and center of pupil can be found by calculating its center of mass. The steps of black hole search method are as follows:

1. Find the darkest point of image in global image analysis.
2. Determine a range of darkness designated as the threshold value (t) for identification of black holes.
3. Determine the number of black holes and their coordinates according to the predefined threshold. Calculate the center of mass of these black holes.
4. Ex and Ey denotes the x, y coordinates of center which satisfy I(x,y)<t.

$$Ex = \{\Sigma_{x=0 \text{ to } w-1} \Sigma_{y=0 \text{ to } H-1} X \} / WH$$
$$Ey = \{\Sigma_{x=0 \text{ to } w-1} \Sigma_{y=0 \text{ to } H-1} Y \} / WH$$

where W and H are the sum of detected coordinates x, y and t is the threshold value. The radius can be calculated from the given area (total number of black holes in the pupil), where radius $=\sqrt{area/\prod}$. From the center of the pupil, the x, y coordinates of every node is found and used to form lock/unlock data as shown in Figure 2 (a) and (b). The x and y coordinates of nodes (8 bits each) are used as [x|y] to obtain 16 bit lock/unlock data unit u.

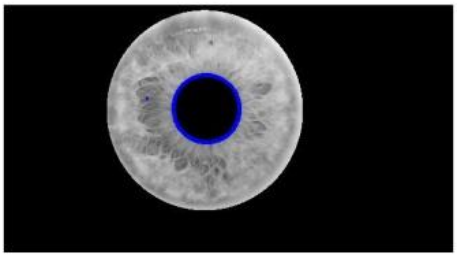


Figure 2: (a) Showing pupil boundary.

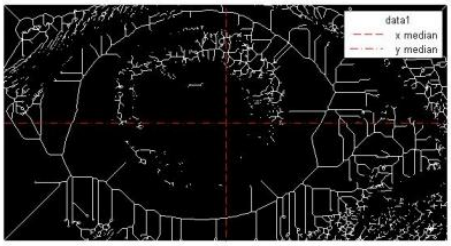


Figure 2: (b) Iris showing x/y coordinates.

The following steps illustrate the encoding process of the fuzzy vault: -

Step 1:

Feature extraction from fingerprint or Iris or Retina.

Step 2:

Encoding Process

(i) 128 bit random secret S is generated.

(ii) 128 bit secret data is combined with 16 bit CRC to form 144 bit SC.

(iii) SC is divided into nine 16 bit segments to obtain polynomial Coefficients.

(iv) SC is represented as a polynomial.

$p(u) = c8u8 + c7u7 + ……..+ c1u1 + c0$

(v) x and y coordinates of the minutiae act as locking/ unlocking unit (u = x|y) of the vault .

(vi) Two sets namely Genuine set (G) and chaff set(C) are generated.

$G = [(u1,p(u1)), (u2,p(u2)),…….. (uL, p(uL))]$

$C = [(c1,d1),(c2,d2) …..(cM,dM)].$

$cj \bullet ui,(j = 1,2,…….M, i = 1,2, …L)$

$dj \bullet p(ci), (j = 1,2,….M. i = 1,2,… L)$

$VS = Listscrambled (G U C)$

Where

'u' is genuine point

'p(u)' is the projection of the genuine point

'c' is the chaff point which is not in genuine point set

'd' is the dummy value which is not in p(u)

'm' is the number of chaff points

'l' is the number of genuine points

4.6. Diagram for Fuzzy Vault Construction

The locking and unlocking process of the feature points from the biometric modalities in the fuzzy vault is illustrated in the schematic diagram that shows a sample Iris template which is shown in Figure 3.

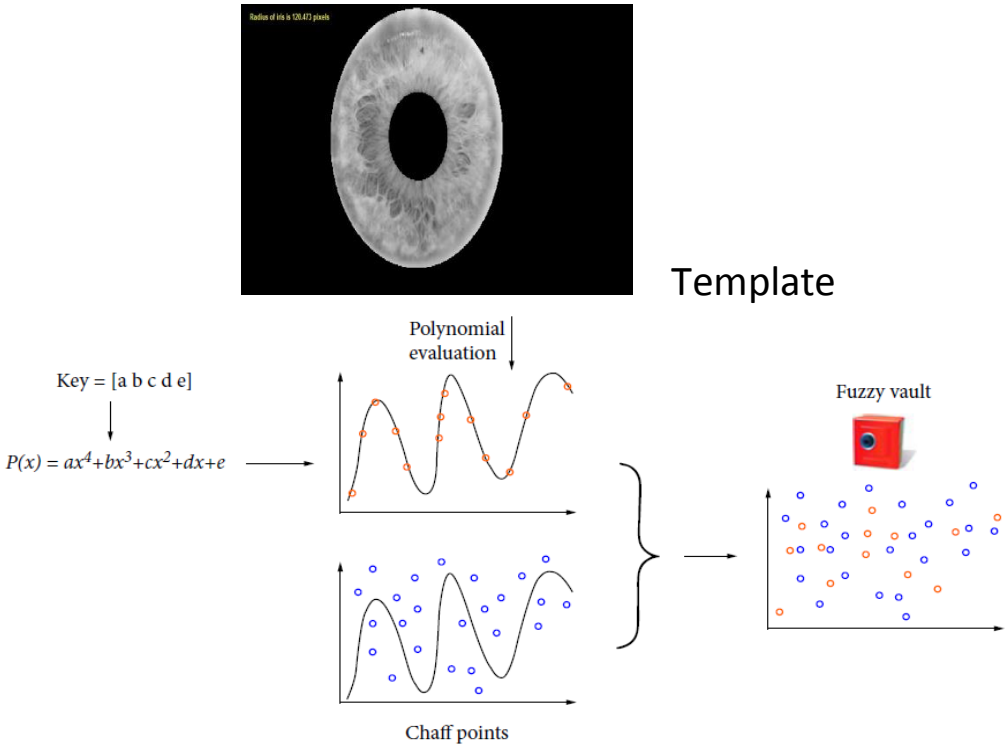


Figure 3: Procedure of fuzzy vault encoding.

The following steps illustrate the Decoding process of the fuzzy vault: -

i. Query minutiae set (Q) is compared with the vault.

ii. Genuine point set is isolated and polynomial is reconstructed.

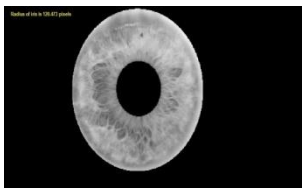
iii. Coefficients are mapped back and SC* is obtained.

iv. SC* is divided by the CRC primitive polynomial.

v. If the remainder < > 0 then.

Query template does not match and the secret decoded is not correct and sample is from an imposter. else if the remainder = 0 then

Query template matches and secret gets decoded successfully and sample is from a genuine user. For checking errors the polynomial is divided with CRC primitive polynomial. A zero remainder means no errors. The details procedure of fuzzy vault decoding is shown in Figure 4.



Query iris

Key = [a b c d e]

P(x) = ax4+bx3+cx2+dx+e

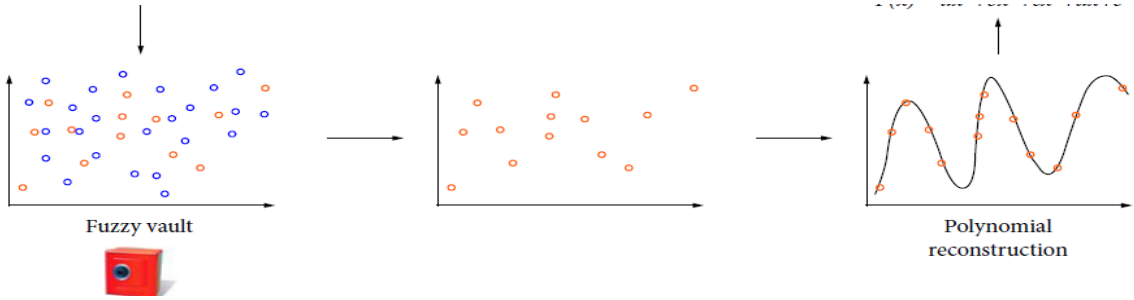


Figure 4: Procedure of fuzzy vault decoding.

5. Experimental Results

The proposed method is simulated using MATLAB simulator. For the vault implementation, a unique point from biometric modality is extracted. Secret message is generated as a 128 bit random stream. The 16 bit CRC is appended to transformed key S to get 144 bit SC. The primitive polynomial considered for CRC generation is shown in Figure 5.

$$g_{crc}(a) = a^{16} + a^{15} + a^{2} + 1$$

Figure 5: Primitive polynomial for CRC generation.

In the minutiae set, the minutiae points whose Euclidian distance is less than D are removed. A 16 bit lock/unlock unit 'u' is obtained by concatenating x and y (each 8 bits) coordinates. The 'u' values are sorted and first N of them are selected. The Secret (SC) is divided into 9 non overlapping segments of 16 bits each. Each segment is converted to its decimal equivalent to account for the polynomial coefficients (C8, C7 …C0). All operations take place in Galois Field GF. The projection of 'u' on polynomial 'p' is found. Now the Genuine points set G is ((ui, P(ui)). Random chaff points are generated which are 10 times more in number than that of the genuine points. Thus two sets namely the Genuine set (G) and chaff set (C) are generated. The 144 bits are converted to polynomial p(u) as –

p(u)=180*int64(u^8)+1638*int64(u^7)+52868*int64(u^6)+59549*int64(u^5)+14256*int64(u^4)+3167*int64(u^3)+40820*int64(u^2)+3160*int64(u)+int64(10280)

The indices of x and y coordinates of nodes are used for projections. The co-ordinates of nodes in Figure 2 (b) are:

(98, 56) = 2 (inch)
(160, 65) = 3
(150,128) = 4
(333, 8) = 5

(231, 223) = 6
(296, 193) = 7
(465, 109) = 8
(406, 233) = 9
(549, 161) = 10

Add these two co-ordinates then convert into inch. After that put in these inches value into the polynomial p(u)=int64().

X=[2 3 4 5 6 7 8 9 10];
Y=[5978176 59401850 320687240 1220786830 3711187088 9644682506 22328026600 47294632190 93352750880];

Plot(x,y);
Output show – Genuine point in Figure 6.

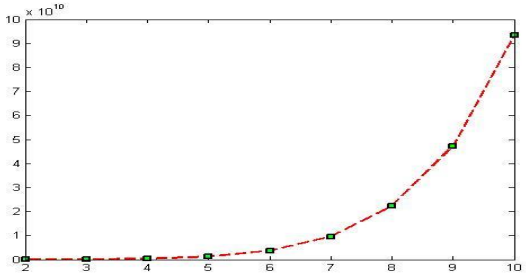


Figure 6: Genuine point.

Using these indices, genuine points are generated to which chaff points are added later to form vault. The ratio of chaff points and original points is taken as 10:1 so that the combinations are large in giving high security.

6. Conclusion

Fuzzy vault, constructed for iris templates, is superior to that of other biometric templates. When compared with other biometrics, iris provides stable structures irrespective of acquisition characteristics. But histogram processing is needed for contrast enhancement of iris after acquiring. Also pre alignment of templates is not necessary since nodes are always constant in iris texture. The time complexity and space complexity of algorithm are high due to long integers involved in genuine set calculation since the size of each template is 32 x 32. Also multiple combinations are to be verified. Quantizing the iris features to 8 x 8 level can minimize these complexities.

REFERENCES

[1] Chuan Chin Teo, Hong Tat Ewe "An efficient One Dimensional Fractal Analysis for Iris Recognition" *WSCG*'2005, January 31-Feb4,2005,Plzen,Czech Republic.
[2] LiMA, Tieniu, "Efficient Iris Recognition by Characterizing Key Local Variations", *IEEE trans., Image Processing*-2004.
[3] Robert Ives, Delores Etter, Yingzi Du, "Iris Pattern Extraction using Bit Planes and Standard Deviations", *IEEE conference on Signals, systems and computers*, 2004.
[4] NIST, Advanced Encryption standard (AES),2001. http://csrc.nist.gov/publications/fips/fips 97/fips-197.pdf
[5] A. Burnwal, A. Kumar, and S. K. Das, "Assessment of fuzzy set theory in different paradigm," *International Journal of Advanced Technology & Engineering Research*, 2013, vol. 3, no. 3, pp. 16–22.
[6] S. K. Das, S. Tripathi, and A. Burnwal, "Design of fuzzy based intelligent energy efficient routing protocol for WANET," *in Computer, Communication, Control and Information Technology (C3IT), 2015 Third International Conference on, IEEE*, 2015, pp. 1-4, DOI: 10.1109/C3IT.2015.7060201.
[7] A. Kumar, R. K. Sharma, and A. Burnwal, "Energy Consumption Model in Wireless Ad-hoc Networks using Fuzzy Set Theory," *Global Journal of Advanced Research*, 2015, vol. 2, no. 2, pp. 419-426.
[8] S. K. Das, S. Tripathi, and A. Burnwal, "Intelligent energy competency multipath routing in wanet," *in Information Systems Design and Intelligent Applications*, Springer, 2015, pp. 535-543, DOI: 10.1007/978-81-322-2250-7_53.
[9] S. K. Das, A. Kumar, B. Das, and A. Burnwal, "On soft computing techniques in various areas," *Computer Science & Information Technology (CS & IT)*, 2013, vol. 3, pp. 59-68, DOI : 10.5121/csit.2013.3206.

[10] S. K. Das, S. Tripathi, and A. Burnwal, "Some relevance fields of soft computing methodology," *International Journal of Research in Computer Applications and Robotics*, 2014, vol. 2, pp. 1-6.
[11] A. Burnwal, A. Kumar, and S. K. Das, "Survey on application of artificial intelligence techniques*," International Journal of Engineering Research & Management*, 2014, vol. 1, no. 5, pp. 215–219.
[12] A. Kumar, A. Kumar and A. P. Burnwal, "Correlation of artificial intelligence techniques with soft computing in various areas", *International Journal of Indestructible Mathematics & Computing*, 2017, vol. 1, no. 1, pp. 27-34.
[13] A. Burnwal, A. Kumar, and S. K. Das, "Assessment of mathematical modeling in different areas," *International Journal of Advanced Technology & Engineering Research*, 2013, vol. 3, no. 3, pp. 23–26.
[14] S. K. Das, A. K. Yadav and S. Tripathi, "IE2M: Design of intellectual energy efficient multicast routing protocol for ad-hoc network," *Peer-to-Peer Networking and Applications*, 2016, pp. 1-18, DOI 10.1007/s12083-016-0532-6.
[15] S. K. Das, A. Kumar, B. Das, and A. Burnwal, "Ethics of E-Commerce in Information and Communications Technologies," *International Journal of Advanced Computer Research*, 2013, vol. 3, no. 1, pp. 122-124, doi=10.1.1.300.9397.
[16] S. K. Das, S. Tripathi, and A. Burnwal, "Fuzzy based energy efficient multicast routing for ad-hoc network," *in Computer, Communication, Control and Information Technology (C3IT), 2015 Third International Conference on, IEEE*, 2015, pp. 1-5, DOI: 10.1109/C3IT.2015.7060126.
[17] S. K. Das, A. Kumar, B. Das, and A. Burnwal, "Ethics of reducing power consumption in wireless sensor networks using soft computing techniques," *International Journal of Advanced Computer Research*, 2013, vol. 3, no. 1, pp. 301-304.
[18] S. K. Das and S. Tripathi, "Energy Efficient Routing Protocol for MANET Using Vague Set," *in Proceedings of Fifth International Conference on Soft Computing for Problem Solving*, Springer, 2016, pp. 235-245, DOI: 10.1007/978-981-10-0448-3_19.
[19] A. Kumar, A. Kumar and A. P. Burnwal, "Application of intelligent game theory approach in cognitive radio ad hoc networks", *International Journal of Indestructible Mathematics & Computing*, 2017, vol. 1, no. 1, pp. 35-40.
[20] S. K. Das and S. Tripathi, "Intelligent energy-aware efficient routing for MANET," *Wireless Networks*, 2016, pp. 1-21, DOI 10.1007/s11276-016-1388-7.
[21] S. K. Das, B. Das, and A. Burnwal, "Intelligent energy competency routing scheme for wireless sensor networks", *International Journal of Research in Computer Applications and Robotics*, 2014, vol. 2, no. 3, pp. 79–84.
[22] S. K. Das and S. Tripathi, "Energy efficient routing protocol for manet based on vague set measurement technique," *Procedia Computer Science*, 2015, vol. 58, pp. 348-355, doi:10.1016/j.procs.2015.08.030.
[23] B. K. Mishra, B. Yadav, S. Jha, and A. Burnwal, "Fuzzy set theory approach to model super abrasive grinding process using weighted compensatory operator," *International Journal of Research in Computer Applications and Robotics*, 2015, Vol. 3, no. 5, pp. 62-68.
[24] N. Kumari and A. P. Burnwal, "Interactive fuzzy programming model in multi-objective inventory control", *International Journal of Indestructible Mathematics & Computing*, 2017, vol. 1, no. 1, pp. 38-26.
[25] S. Murmu, S. Jha, A. Burnwal, and V. Kumar, "A proposed fuzzy logic based system for predicting surface roughness when turning hard faced components," *International Journal of Computer Applications*, 2015, vol. 125, no. 4.
[26] A. Burnwal, S. Mukherjee, and D. Singh, "An additive model of fuzzy geometric programming," *Mathematics Education India*, 2000, vol. 34, no. 1, pp. 25-29.
[27] H.Heijmans, Morphological Image Operators, *Academi Press*,1994.
[28] R. C. Gonzalez and R. E. Woods, Digital Image Processing, *Addison-Wesley*, 3rd ed. 1992.
[29] Joaquim De Mira Jr, Joceli Mayer, "Image Feature Extraction for application of Biometric Identification of Iris - A Morphological Approach". *proc IEEE Int'l Symp on Computer Graphics and Image processing*, SIBGRAPI'03
[30] A. Juels and M.Sudan, "A Fuzzy Vault Scheme", *proc.IEEE Int'l. Symp.Inf. Theory,A Lapidoth and E.Teletar,Eds*.,pp.408,2002.
[31] Umut Uludag, and Anil K.Jain, " Fuzzy Finger Print Vault", *Proc. Workshop: Biometrics: Challenges Arising from Theory to practice*, pp.13-16, 2004,W.H.Press
[32] S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, Numerical Recipes in C,2.Ed., *Cambridge University press*,1992.
[33] The Center of Biometrics and Security Research, CASIA Iris Image Database http://www.sinobiometrics.com.