ISSN: 0976-9102 (ONLINE)
DOI: 10.21917/ijivp.2020.0317

CMBA - A CANDID MULTI-PURPOSE BIOMETRIC APPROACH

Sehrish Saleem[1], Shahzad Ashraf[2] and Muhammad K. Basit[3]
[1,3]Department of Computer Science, Muhammad Nawaz Sharif University of Engineering and Technology, Pakistan
[2]College of Internet of Things Engineering, Hohai University, Changzhou Campus, China

Abstract

All humans are born with unique physically identified body characteristics to other persons which remains unchanged throughout life. These characteristics are taken into account by the emerging technology to get recognized from person to person. The technology used by the traditional human identification system sometimes becomes inefficient when data or images received are not up to the acceptable quality mark or when a person has a face covered with mask-like during epidemic virus fistula. In order to overcome the human recognition challenges, a Candid Multi-purpose Biometric Approach (CMBA) has been proposed which can make human identification easier and approachable. The CMBA human recognition approach uses two uniquely identified modalities such as foot and iris. This approach shrewdly identifies and makes the bodacious recognition among humans and suggests the sagacious result which is foremost better than the traditional biometric system. The CMBA is offering opportunity to take more than two biometric features, by combining them to overcome unimodal biometric system limitations and to achieve optimal results. Using sagacious edge detector and Hough transformation technique, the Iris and foot part are segmented into easy and quick extraction voting system which produce succulent output. In fact, this technique is new in biometric identification era.

Keywords:

Biometric System, Face Recognition, Modalities, Face Mask

1. INTRODUCTION

From a physiological and behavioral point of view, the biometric method is becoming common for the recognition and authentication of individuals. When the conclusion is the correct, the evaluation screen fits with images already stored-in and the visualization is checked thereafter [1]. In order to locate the test picture in the stored database, the user is marked or does not know if it is just one of several mapping schemes. With the abundance of data and confidential details stored in personal electronic devices, it is important to secure them from unauthorized access. Deficiencies in protection may contribute to theft of identification or details. Theft of identity is the manipulation of identity while copying the secure data is obtained from the information theft. There are three level of human security, out of which number third level implements greater difficulty of the user's personal property in an authentication scheme [2]. It uses the features of the individual's physiological or mental, called biometrics. With the assistance of fully or semi-automatic systems it provides a potential solution for identity management. Many of the advantages of biometric systems relative to other authentication method relying on token and information are given below.

- *Unique*: It is assumed that biometric properties are special. Having special to an entity and define a person's unique characteristic.
- *Convenient*: The use of biometrics is easy because the customer does not need a key or hidden information to be processed. The customer often has physiological or behavioural characteristics that cannot be incorrectly put, misplaced or overlooked.
- *Hard to Forge*: Difficult to forge biometric characteristics. An attacker may use a spoofing technique to strike him, however the simultaneous usage of more than one biometric attribute greatly reduces the risk of forgery.
- *Requires Physical Presence*: After verification a biometric program collects live biometric samples. The physical appearance of the consumer is also necessary. It instills a sense of belonging with the benefit of non-repudiation; that is, the individual cannot refuse his involvement in authentication at a later point in time.

Some in practice biometric identification technique has been described in Table.1. Usually, all biometric results are being taken in two steps; either through training process or by testing process. The brief discussion is given as:

Training process: The process of training is given here: 1) Camera captures or acquires input image. 2) Preprocessed picture requires file re-dimensioning, reformatting. 3) Extraction function is carried out and 4) Built-in data corpus.

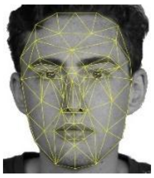
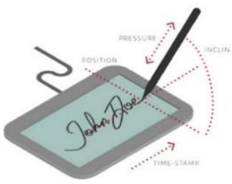
Testing Process: It is closer but balanced at the planning point [3]. The preparation and assessment procedures are illustrated in Fig.1. There are numerous challenges hindering the traditional and in practice biometric system.

There are numerous challenges faced by the uni-biometric system such as: Noise, Intra-class variations, Non-universality and Spoof attacks.

The CMBA Multi-purpose biometric approach-purpose biometric approach provide incentives to carry in more than two biometric functions, integrate them to address unimodal shortcomings of the biometric method and obtain optimum performance [4]. For a CMBA biometric interface, we used two modalities such as, foot and iris. Sprints are being developed whereas, iris is unique and not altered as a transparent layer structure during a person's life.

The rest of the article is arranged as, related work is addressed in section 2. Section 3 presents the proposed methodology Section 4 demonstrates the performance obtained through results while concluding remarks are given in section 5.

Table.1. In-practice biometric techniques, comparison and challenges

Biometric technique		**Process**	**Challenges**
	Finger print thumb impression	Indeed, it is a most appropriate and common method of human identification an individual over the last decade. The system uses a magnetic ink to get the print on paper with finger or thumb. It’s a pattern with ridges and valleys on the finger skin layer. Certain patterns emerge during the formation of the fetus and remain constant throughout the course of life.	It needs a sufficient number of characteristics (minutia), true characteristics and their consistency. It also demands the consumer to collaborate strongly, to spoof and to decrease the consistency of the sample obtained.
	Face recognition	The facial or face recognition is a technology in which an individual is recognized and instantly checked via digital picture. This non-invasive data processing is one of the key benefits of the face over other techniques. The Facial Recognition Method has two key parts: (i) the position of the face in the picture and (ii) the identification of the object. Holistic facial recognition methods utilize anatomical differences between facial traits such as pupils, nose, mouth and eyebrows as attributes.	Non-cooperative behaviour of users, changes in background lighting, illumination, exposure, expressions, occlusions, ageing, etc.
	Ear biometry	Ear biometry utilizes attributes or traits of the ear for matching. It is secure and does not shift with age. This has long been seen in the investigative area as a form of individual identification. The ear form is constant and does not shift with time. With time. This has no expression as compared to face. The light pattern is always standardized.	Hair or some other international object such as the earring, hat, earphones etc. are the biggest annoyance of the ear. Ear is significantly influenced by the changes of positions, although from the front photo it is not noticeable. Small heads have less features
	Hand geometry	It includes the calculation and study of the form of the hand of the consumer. This is a fairly quick, easy to use and cost-effective method. It can be easily integrated with other devices or system even if it requires special hardware to be used. Factors such as dry skin have little impact on the system’s efficiency.	Jewellery or agility can present a problem in proper geometry extraction. Some of the main drawbacks is the poor differential potential of hand geometry.
	Palmprint	It contains folds, key lines, shape, ridges, delta points, local minutiae points, etc. It is important to use all such details for acknowledgment. Even in monozygous twins, the palmprint patterns are found to be unique, but the stability of palmprint features is not yet critically studied. The camera used to get the picture by hand is low cost and user friendly.	The scanners used to obtain the palmprint are bulkier and due to the wide capture region it requires more computing capacity. The amount of features in a palmprint image is lower, so it is challenging to remove due to rough palm surface.
	Voice recognition	Every individual person possessed specific tone, pitch, and speaking style under the behavioral characteristics of voice biometric system therefore it’s a speedy method of identification which requires no specific tool or system. The voice character requires properties including fundamental pitch, nasal sound, cadence, inflection, etc.	Voice can be captured quickly, and unauthorized access is likely. The speaker can alter a person’s speech and may find speech identification challenging, such as noise, sickness, gender, mental and physical conditions.
	Signature identification	Handwritten signatures in other fields, such as banking and legal documents, are also used for offline device authentication. Wide signature database availability renders it one of the most-needed automated authentication schemes.	One of the biggest challenges of this technology is poor permanence characteristics due to high levels of variability in handwriting with time. An impostor can reproduce a signature easily. Since not everyone can sign, lack of universality is a prime factor as well.

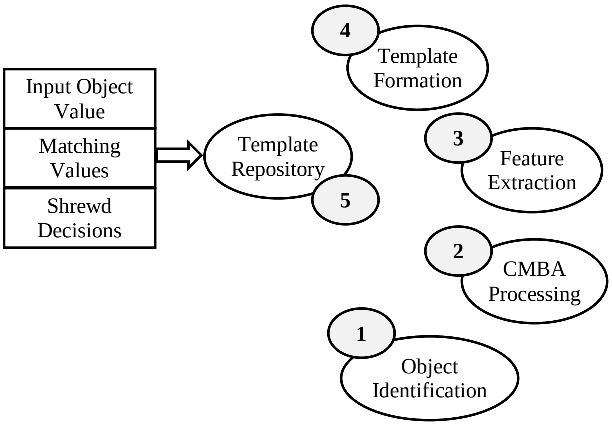


Fig.1. Information training flow process

2. RELATED WORKS

Many researchers have made significant contributions reported [5], that the biometrics is becoming more commonly used in several places through different biometric device such as bank, institute and airports. Multi-purpose biometric is preferred in authentication-based image processing applications. There also exist a multi modal systems working on physiological and demography information for identification of person.

Author links open overlay panel Michail et al. [7], introduced a biometric system for person recognition that shown the improvement accuracy of the recognition system. Another research work on face and ear-based hybrid system has been presented by [8]. This system is used Iterated Function concept in which images are compression and indexed. Sarfraz et al. [9], designed a multi-biometric system that combines face modalities and foot modalities using PCA [10], classifier for face and wavelet transformer for foot and concatenated after normalization process to obtain a matching score and take a decision. Another author Davrondzhon [11], proposed a system for multimodalities biometric that combines face, ear and iris using PCA, Eigen image [12], and hamming travers [13], classifier for feature extraction, sum rule method is used for fusion to calculate matching score. They introduced recognizing person utilize multiple biometric traits and their advantages such as high accuracy and robustness, that increased recognition performance. Herbadji et al. [14], developed a Multi-biometric system, which combined face and foot modalities at decision level using PCA classifier for face and wavelet transformer for foot and concatenated after normalization process to obtain matching score [15].

3. METHODOLOGY

The body parts can be paired with the other body elements in several potential ways, leading to very diverse machine architectures. Particularly in parallel or in cascade, the Iris footprint can be combined and therefore further findings are arranged as:

3.1 IRIS BIOMETRICS

Iris recognition work on the colored part of eye that is isometrics surrounds by pupil known as iris. Iris image is captured using high quality camera every person has a unique iris. Process of calculating patterns are very complex it stored in bit format [7]. Hamming traverse method is used for calculating the distance between test image and stored template if the distance is zero that indicate the test image and training image is same otherwise, we can say both images are different.

4. FOOTPRINT BIOMETRICS

Identification of peoples by fingerprint is becoming a wonderful success. Measurement such features are not a complicated process some transformation such as furrier, Haar are available [16]. Each parson has completely different footprint and it is easy to capturing without any special requirement both leg images can be used for recognition. Captured foot image needs some additional approach such as cropping and resizing. The Fig.2 displays the picture captured by high quality camera than the RGB image converted into gray scale after that resize them for preparing the database [17].

(a) (b)

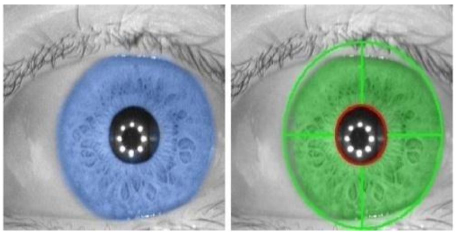
Fig.2. Information retrieval process from foot segments

4.1 HAMMING DISTANCE METHOD FOR IRIS

Hamming distance approach is applied for a matching iris templates incorporate noise masking. The distance between two iris templates is calculated in bits format and distance calculated between two iris templates if the distance is minimum that indicate the iris are same otherwise iris are not matched which confirms, hamming distance is a reliable and accurate for iris recognition [18]. The iris recognition process completed in three stages:

- *Segmentation*: Located the iris region
- *Normalization*: Created a consistency of data iris region
- *Feature Encoding*: Produced templates as set of discriminated features of the iris.

The process of segmentation and normalization is illustrated in Fig.3.



110011001111111
100010001001011
110011111001011
000010001001111
110110011001101
110011101001101

Fig.3. Bits formation from extracted iris segment

4.2 SEQUENTIAL MODIFIED HAAR TRANSFORM TECHNIQUE

The sequential modified Haar wavelet [19], is based on the mapping technique in which integer-valued signals are mapped using the reconstruction of image technique. Wavelet coefficients represented by decimal numbers and each decimal value needed eight bytes for storing the Haar value [4].

4.3 CMBA APPROACH

The sample of eye images are being consider as input to the system and thereby iris templates are generated as output. The discrete bits formation of the image has been obtained illustrated in Fig.4, showing segmentation and normalization stages. The system proposed produces n number of iris codes out of n number of eyes tests performed at various time periods from the same person. Using majority voting scheme, a unique iris code *x* is built from the n number of iris code. The suggested framework operates on *x* and generates codewords, known as Error Corrected Iris Code (ECIC). These ECICs are composed of iris coding and parity regulation *p*. The hash h is also created from code x. Eventually, parity regulates *p* of the ECIC, matrix *h* of parity and hash-*h* render code that are embedded in digital images by transformation of the integrated wavelet and incorporation processing threshold.

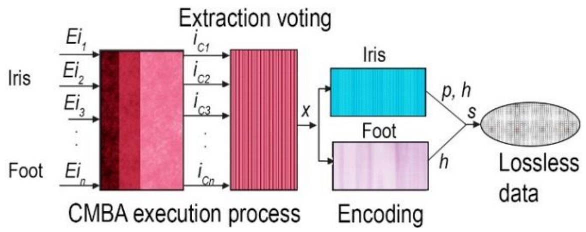


Fig.4. Proposed CMBA Multi-purpose biometric recognition process

The new and unique feature of the CMBA is the speed and precise segmentation of irises the iris image being captured to reduce identifying errors, producing a vector with distinguishing texture characteristics and a proper dimension to improve the detection and computational efficiency [22]. The sagacious edge detection and circular Hough transforms are used for the segmentation process. The segmented iris is normalized and phase data is extracted by applying Log-Gabor filter [23], and encoded shrewdly to produce the refined vector feature through phase quantization method [24]. The iris from real eye object has been extracted after undergoing segmentation, normalization and quantization process as. Unless the iris area has been effectively segmented from the eye object, the next step is to turn the iris region in such a manner that it has set measurements to enable comparisons [25]. Dimensional incoherence between eye images are mainly because of the iris stretching caused by the dilation of pupils from different luminance levels. Other sources of inconsistency include varying imaging distance, camera rotation, head tilt and eye rotation within the socket of the eye. Construction outcomes of individual iris code *x* from *n* number of iris code are achieved using a specific procedure named extraction vote. The Fig.5 explains the fabrication of these unique iris *x* from three sample iris codes. The sparse parity test matrix is used to describe CMBA codes. This small matrix is often generated at random, depending on the sparsity limitations. The valid message bits are processed by the multi-purpose phase when satisfy the condition thereby extraction voting occurs. After creating a specific iris code *x*, each column in iris code *x* is considered to be a message in CMBA encoding and encoded to render ECIC with the aid of generator values. The special iris code *x* is converted into hash *h*, often referred to as cancellable iris code. The Table.2 shows factual score, imposter score and threshold value for object 1 and 2 respectively.

The iris and foot biometrics were tested individually and Table.3 show False accept rate (FAR) [26], and false reject rate (FRR) [27], of Iris and foot. The weight of all individual iris and foot modalities was calculated, shown in Table.3. Iris recognition and foot recognition algorithms produced dissimilarity scores [28]. The Min-Max normalization is used to convert all dissimilar data into similar data shown in Table.3. The Table.3 shows the weight value of iris and foot after the fusion of two traits. Matching score [6], was calculated for two modalities using their weight. The Table.4 shows the matching score for combination of two traits iris and foot.

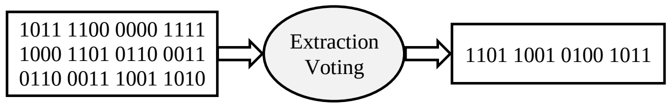


Fig.5. Extracting Voting Mechanism

Table.2 The iris and foot score

Traits	Genuine Score	Imposter Score	Threshold Value
Iris	1.7121E+04	1.9082E+04	1.7330E+04
Foot	2.2277E+04	2.6613E+04	2.2325E+04

Table.3. Iris and foot related FAR and FRR parameters

Traits	FAR	FRR	Weight	Normalized Score
Iris	1.1010E+00	9.8793E-01	0.89	0.05
Foot	1.1921E+00	9.9785E-01	0.83	0.07

Table.4. Cumulative matching score

Traits	Score
Iris + Foot	0.292

5. PERFORMANCE AND RESULTS

For getting performance results, near about 100 sampling objects (eye and foot) among 500 images were considered. For each iris object, the four samples were taken for multi-purpose biometric process. The remainder of the iris representation in the repository is linked to the other iris in the authentication process [20]. A total number of (500×499)/2 = 124,750 comparisons are made, out of which 345 intra-group matches were found and another 116,602 inter-group matches were recorded. The Fig.8, exhibits a total intra-group and inter-group distribution. It has been observed that travers between intra-group and Inter-group is exorbitant and the portion occurring between the intra-class and the inter-class is quite trivial, thereby nearly 100% of the right identification levels are obtained. In-order to determine the error correction capacity of CMBA, Reed Solomon (RS) [21], and code is being applied which eventually generate the results as illustrated in Fig.9. The selected RS and CMBA curves overlaid on top of the real and impostor normalized HD distributions. RS correction curves are also notably lower than the CMBA curves. It can be seen also. In comparison, the RS encoding is often less granular than the CMBA. It leads in efficiency loss, with the False Rejection Rate (FRR) and the False Acceptance Rate (FAR) levels.

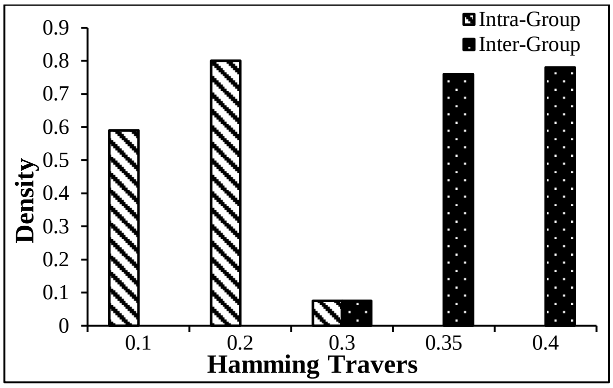


Fig.7. Distribution record during Intra and Inter-group

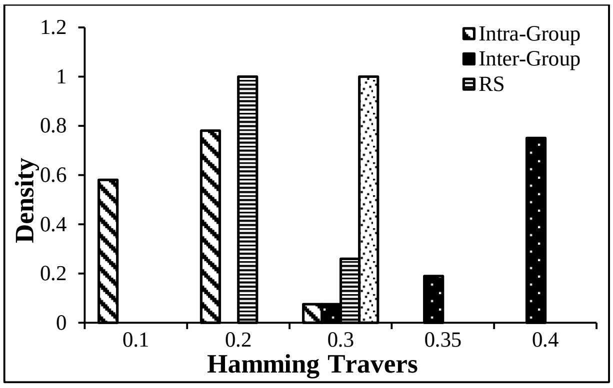


Fig.8. Proposed error correction determination

6. CONCLUSION

The CMBA system employed biometric features of iris and foot. For hamming archways and sequential modified classifier approaches of Haar transformation, weight was calculated of each biometric element. After normalization, the knowledge was combined. The Iris is divided into an easy and quick technique, based on the Sagacious edge detector and Hough transformation. For other approaches, the actual FRR and FAR are 2% and 0.38%, while the FRR and FAR suggested by CMBA are 1.87% and 0.365%. The framework uses CMBA codes for lower FRR and FAR. As a conclusion, it can be claimed that, compared to other reported technologies, the proposed system has superior performance in terms of reliability, accuracy and continuity.

REFERENCES

[1] A. Melamed, "2018 Biometric Predictions: Advanced Biometric Technologies Take Off", Available at: https://www.biometricupdate.com/201801/2018-biometric-predictions-advanced-biometric-technologies-take-off, Accessed at 2018.

[2] M2SYS, "False Rejection Rate," Available at: https://www.m2sys.com/blog/important-biometric-terms-to-know/false-rejection-rate-what-does-it-mean-and-why-should-i-care/, Accessed at 2018.

[3] S. Ashraf, S. Saleem and T. Ahmed, "Sagacious Communication Link Selection Mechanism for Underwater Wireless Sensors Network", *International Journal of Wireless and Microwave Technologies*, Vol. 10, No. 4, pp. 22-33, 2020.

[4] S. Ashraf, M. Gao, Z. Chen, S. Kamran and Z. Raza, "Efficient Node Monitoring Mechanism in WSN using Contikimac Protocol", *International Journal of Advanced Computer Science and Applications*, Vol. 8, No. 11, pp. 1-13, 2017.

[5] MSU Today, "Unlocking New Possibilities for Biometrics", Available at: http://msutoday.msu.edu/feature/2018/unlocking-new-possibilities-for-biometrics, Accessed at 2020.

[6] S. Ashraf, S. Saleem and T. Ahmed, "Sagacious Communication Link Selection Mechanism for Underwater Wireless Sensors Network", *International Journal of Wireless and Microwave Technologies*, Vol. 10, No. 2, pp. 12-25, 2020.

[7] M.N. Giannakos, K. Sharma, I.O. Pappas, V. Kostakos and E. Velloso, "Multimodal Data as a Means to Understand the Learning Experience", *International Journal of Information Management*, Vol. 48, No. 2, pp. 108-119, 2019.

[8] J. Pandya, "Hacking Our Identity: The Emerging Threats from Biometric Technology", Available at: https://www.forbes.com/sites/cognitiveworld/2019/03/09/hacking-our-identity-the-emerging-threats-from-biometric-technology, Accessed on 2020.

[9] N. Sarfraz, "Adermatoglyphia: Barriers to Biometric Identification and the Need for a Standardized Alternative", *Cureus*, Vol. 11, No. 2, pp. 1-9, 2020.

[10] F.G. Mohameed and Morooj K. Luaibi, "Facial Recognition Based on DWT-HOG-PCA Features with MLP Classifier", *Journal of Southwest Jiaotong University*, Vol. 54, No. 6, pp. 1-14, 2019.

[11] D. Gafurov, "*Emerging Biometric Modalities: Challenges and Opportunities*", Springer, 2020.

[12] R. Singh, "The essence of eigenvalues and eigenvectors in Machine Learning", Available at: https://towardsdatascience.com/the-essence-of-eigenvalues-and-eigenvectors-in-machine-learning-f28c4727f56f, Accessed at 2019.

[13] J.F. Doriguello and A. Montanaro, "Quantum Sketching Protocols for Hamming Distance and Beyond", *Physical Review A*, Vol. 99, pp. 1-13, 2019.

[14] A. Herbadji, Z. Akhtar, K. Siddique and M. Cheniti, "Combining Multiple Biometric Traits Using Asymmetric Aggregation Operators for Improved Person Recognition", *Symmetry*, Vol. 12, No. 3, pp. 1-19, 2020.

[15] S. Ashraf, Z.A. Arfeen, M.A. Khan and T. Ahmed, "SLM-OJ: Surrogate Learning Mechanism during Outbreak Juncture", *International Journal for Modern Trends in Science and Technology*, Vol. 6, No. 5, pp. 162-167, 2020.

[16] S. Ashraf, A. Raza, Z. Aslam, H. Naeem and T. Ahmed, "Underwater Resurrection Routing Synergy using Astucious Energy Pods", *Journal of Robotics and Control*, Vol. 1, No. 5, pp. 1-12, 2020.

[17] B. Ammour, L. Boubchir, T. Bouden and M. Ramdani, "Face-Iris Multimodal Biometric Identification System", *Electronics*, Vol. 9, No. 1, pp. 85-94, 2020.

[18] S. Ashraf, M. Gao, Z. Mingchen, T. Ahmed, A. Raza and H. Naeem, "USPF: Underwater Shrewd Packet Flooding Mechanism through Surrogate Holding Time", *Wireless Communications and Mobile Computing*, Vol. 2020, pp. 1-12, 2020.

[19] A. Mohammadi, N. Aghazadeh and S Rezapour, "Haar Wavelet Collocation Method for Solving Singular and Nonlinear Fractional Time-Dependent Emden-Fowler Equations with Initial and Boundary Conditions", *Mathematical Sciences*, Vol. 13, pp. 255-265, 2019.

[20] S. Ashraf, A. Ahmad, A. Yahya and T. Ahmed, "Underwater Routing Protocols: Analysis of Link Selection Challenges", *AIMS Electronics and Electronics Engineering*, Vol. 4, No. 2, pp. 200-215, 2020.

[21] I.S. Reed and X. Chen, "*Reed-Solomon Codes*", Error Control Coding for Data Networks, Springer, pp. 233-284, 1999.

[22] S. Ashraf and T. Ahmed, "Underwater Routing Protocols Analysis of Intrepid Link Selection Mechanism, Challenges and Strategies", *International Journal of Scientific Research in Computer Sciences and Engineering*, Vol. 8, No. 2, pp. 1-9, 2020.

[23] Log Gabor Filter, "Log Gabor Filter", Available: https://en.wikipedia.org/w/index.php?title=Log_Gabor_filter&oldid=959860559, Accessed at 2020.

[24] P. Kapoor, D. Lee, B. Kim and S. Lee, "Computation-Efficient Quantization Method for Deep Neural Networks", *Proceedings of International Conference on Learning Representations*, pp. 1-8, 2018.

[25] S. Ashraf, T. Ahmed, A. Raza and H. Naeem, "Design of Shrewd Underwater Routing Synergy Using Porous Energy Shells", *Smart Cities*, Vol. 3, No. 1, pp. 74-92, 2020.

[26] Bayometeric, "False Acceptance Rate and False Recognition Rate", Available at: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr, Accessed at 2020.

[27] False Rejection, "What is false rejection rate (FRR)? Webopedia Definition." Available at: https://www.webopedia.com/TERM/F/false_rejection.html, Accessed at 2020.

[28] S. Ashraf, T. Ahmed, S. Saleem and Z. Aslam, "Diverging Mysterious in Green Supply Chain Management", *Oriental Journal of Computer Science and Technology*, Vol. 13, No. 1, pp. 22-28, 2020.