# Optimized Variational Bayesian Extreme Learning Machine Algorithm for Multimodal Biometric Recognition

**Sandhya Tarar, Vyomika Singh, Vibhash Yadav, Shekhar Singh, Hemant Gupta**

***Abstract:*** ***In the thriving field of secure biometric systems, numerous advancements have been created and the need of the hour is Variational Bayesian Extreme Learning Machine (VBELM) which has an advantage in terms of time efficiency, speed, security and accuracy over traditional Extreme Learning Machine method (ELM). After observing the experimental results of Variational Bayesian Extreme Learning Machine (VBELM) we observe that testing accuracy, over fitting problem and recognition models are the issues and in order to address them, we curate an Optimized VBELM (OVBELM) which has opened doors for an exceptional performance in terms of improved statistical testing accuracy, improved recognition rates, execution time, reduced error rates and improved average fusion time.In this paper, optimized Variational Bayesian Extreme Learning Machine (VBELM) is based on local feature fusion of three modalities- Face, Fingerprint and Iris where appending iris as a third modality makes the system robust and secure. The optimized biometric recognition system which is trained on an artificial neural network (ANN) exhibits exceptional results after applying on 240 face images (40 people with 6 images for each individual) from FERET Face database (Facial Recognition Database), 240 fingerprint images( 40 people with 6 images for each individual) from FVC2002 fingerprint database and 240 iris images (40 people with 6 images for each individual) from UBIRIS database and result analysis depicts that the optimized VBELM (OVBELM) is having an edge over VBELM and traditional ELM duly reflected with improved execution time , testing accuracy, average fusion time and reduced error rates.***

***Index Terms:*** ***Artificial Neural Network (ANN),Extreme Learning Machine (ELM), Feature based fusion, Multimodal biometrics system, Optimizedm Varia-tional Bayesian Extreme Learning Machine (OVBELM);Variational Bayesian Extreme Learning Machine (VBELM)***

## I. INTRODUCTION

Enough case studies, real life implementations and continuous research in biometrics has been studied, observed and thoroughly researched since a long time. But the main objective of such technology like any other booming technology is the security concerns and time complexities that come with it. Biometric security and threats related to it is the topic of discussion and research these days. No doubt, this is the present day and upcoming future technology and is also stated to be highly secure, but security and system reliability is one of the increasing issues related to this invention which changed the way people looked and implemented information technology. Variational Bayesian Extreme Learning Machine is a step up in the feature based fusion and subsequent advancement in the field.

It is aptly said that if somehow a biometric is comprised, it is comprised forever and the loss can't be retrieved back again[1]. This statement clearly highlights the necessity of pivotal and mandatory security in biometric systems. Anil Jain, et al. did a tremendously impressive work jotting down the major factors that determines the mandatory requirements in a good biometric system as – Universality, Uniqueness, Permanence, Measurability, Performance, Acceptability and Circumvention [2]. These factors led to a widespread increase in development and quality up gradation of biometric systems. Using single trait in a biometric system is called unimodal biometrics, while using more than one trait to improve the recognition rate is called multimodal biometrics[3][4].Unimodal biometrics though has the capability that changed the domain of security forever but as said a password is private but biometrics is public in nature and we need an effective system for a better security aspect. There are certain disadvantages that unimodal biometrics possess such as noisy sensor data, low security rate, non-universality, unacceptable error rates, spoof attacks and overall less resistance to attacks. Inter-class attacks also happen especially in traits such as facial recognition, in cases of twins, etc. To improve this situation one can combine more than one trait in a system resulting in a multimodal biometric system. Multimodal biometrics, on the other hand provides a more helping hand in improving the security many folds. Multimodal biometrics enhances the security, has higher tolerance, is more stable and has more reliability. The overall recognition rate also improves. But multimodal biometrics has certain pitfalls too. The system should be curated very carefully as complexity increases with increasing traits.

Information fusion in biometrics is mostly of two types – Fusion done before matching and fusion done after matching. The fusion can be done at sensor level, feature level, decision level and many more [5].

**Revised Manuscript Received on December 22, 2018.**

**Sandhya Tarar**, School of Information and Communication Technology, Gautam Buddha University

**Vyomika Singh,** School of Information and Communication Technology, Gautam Buddha University

**Vibhash Yadav,** Information Technology Deptt, Rajkiya Engineering College, Banda, UP, 210201, India

**Shekhar Singh,** Computer Science and Engineering Deptt, Shri Venketeshwara University, Gajraula, Uttar Pradesh, 244236, India

**Hemant Gupta,** Computer Science and Engineering Deptt, Carleton University, Canada

Fusing multiple traits fuses spatial information lowering the overall system error rates [6]. In this research paper, we go for fusion at the feature level.The need of the hour is to make multimodal biometric systems more secure and threat-proof and the subsequent solution to all this is using the technique of feature fusion properly, which fuses two or more features by different techniques. The concentration is on Variational Bayesian extreme learning machine and subsequently on improving and optimizing the algorithm using multiple measurements Bayesian learning and training them on a neural network. A stable algorithm, fast learning and efficient feature extraction opens doors to a clean and stable biometric system. Performance parameters are analysed and the system is made secure and fast. Hence the main motive remains that a multimodal biometric system has improved algorithm, a better functioning strategy and efficient feature extraction enabling more insight to detail and improving the security of such systems.

Incorporating Artificial Neural Network (ANN) technique in this process to train data is the future of biometric generation. Reliability and accuracy is manifold increased. Statistical patterns are identified in the process. Experimental results exhibit a big deal of accuracy improvement in terms of time elapsed, error rate and even more. A cross between these two scientific techniques have resulted in better verification, flexible and accurate working. Also, an ANN is favourable for searching an identity in a big database. The feature fusion enables enhanced security, so that breaching is practically impossible. The network allows the system to combine key biometric traits in a very flexible environment.

The remaining paper is structured as follows: the second section initiates the background research work done in the field of VBELM and feature fusion techniques. The third section explains the proposed work; the fourth section demonstrates the enhancement in the existing algorithm. The fifth section shows system design and modelling, sixth part has the simulation and experimental results, the seventh sectionhas a proper in –depth discussion of the proposed work, and the eighth section wraps up the research into a conclusion while the last section provides acknowledgement and references involved in the research methodology

## II. RELATED WORK

Major findings lie in the fact that whenever errors are tried to be overcome by varying the threshold, the other error rate increases automatically. Therefore there is a need for balance, with a decision threshold that can be specified to either minimize the risk of FAR, or to minimize the risk of FRR. Factors such as noisy data, spoofing, intra-class variation and intra-class similarity are some of the challenges already being faced [8]. Peter Waggett, IBM, et al. (2016), talks about the increasing attacks on biometric systems, especially spoofing even in 3d technology which clearly shows security remains the top concern till date [9].Sandhya Tarar discussed extensively about finger mosaicking in her work in which quality of the fingerprint was improved substantially by comparing

comparing FRR and FAR [10]. A lot about clustering algorithms like K-mean clustering is also seen in this work by Ruchikumari et al where in DWT was interconnected with the proposed algorithm for improvement in quality of feature extraction [11]. The quality of fingerprint image was also enhanced in another work by SubiyaZaidi and et al. wherein Peak signal to Noise Ratio (PSNR) and Mean square error (MSE) were calculated and distortion, blurring were removed and improved [12]. Sandhya Tarar, et al proposed fingerprint quality enhancement by using the technique of Iterative Fast Fourier Transform (IFFT) where a higher level of efficiency is calculated by reconstruction of the quality by subsequent analysis[13]. ELM is an algorithm based approach using feature vector set for pattern classification [14]. ELM posed disadvantages such as unstable parameters, hidden nodes and over fitting problem, because of which it was aptly replaced by VBELM[7][15]. VBELM is basically Extreme Learning Machine combined with Bayesian probalistic model so that it appends added features. The probabilities used are prior and posterior. The problem posed by ELM caused the advent of VBELM which gave solutions to hidden nodes problem and over fitting. Over fitting leads to making the system very complex by introducing many parameters. Generalization power is lost, leading to poor performance in new data. This Bayesian method is highly constructive in comparison to ELM. In VBELM, a multimodal framework is curated with fusion of two modalities whose local visual features are extracted such as – Gabor filter feature, LBP (Local binary pattern) feature and Zernike Moment feature, which are further fused. [7]. This procedure not only has a better reliability and accuracy than ELM, a comparative study shows that VBELM is solving all the disadvantages the ELM technique exhibited.

Visual features from different traits can be fused together to create a robust and secure system.Features of face and iris are combined using wavelet features in a research work authored by Jun-Ying Gan et al. who fused the features using Kernel Fischer Determination Analysis (KFDA) technique [16]. Data face fusion was a new concept adopted in a research paper authored by Mohammad Hanif, et al who proposed an optimized system which was developed by fusing visual and thermal images. Gabor filter was used to extract the features and the proposed system worked well in different conditions and lighting [17]. Yibing Wang et al. illustrated one such more research technique for face recognition using Kernel technique as well as Support Vector Machines (SVM)[18] .Though image illumination helped in clarity but had this system been multimodal, the security would have been further increased. Mina Farmanbar et al. studied the fusion of palm print and face biometrics, using the technique of match score level fusion [19]. Maryam Eskandari et al. used a relatively advanced approach in face-iris fusion in a multimodal biometric system. Experimental results prove that the system is more vigorous [20].OmidSharifi et al. designed an iterative evolutionary algorithm for the fusion of features of face and iris.

Fusion was score level as well as feature level [21]. Sandhya Tarar, et al curated a research for protection of data especially multimedia in nature can be done by watermark extraction and validation using hybrid techniques IWT-SVD scheme which can be improved even further [22]. One can incorporate a lot in this field. On the basis of RECENT research, brain scans are the next modality which is not only completely un-breachable but also very strongly non-cancellable. Accuracy of 97% was reached [23].After surveying the literature and related research, one point was crystal clear that there is a need of an even more optimal, modified algorithm which appends all the features.

Also introducing a new modality (which is something that was not much prevalent in earlier researches) could be an upgrade. Addition of one more modality in an already multimodal system will increase the security threshold. A resampling technique may estimate model accuracy. K-fold cross validation and some other techniques may also enhance the system. The entire process should be efficiently engineered so that elapsed time is lesser and recognition rate is more.

## III. System Design and Modelling

The proposed work not only improves theexisting VBELM algorithm for effective results and calculative analysis but also imbibes descriptive feature extraction of every image before fusing and after fusion, the fused final image is not only feature rich but practically impossible to be breached in and it is also tough to create a fake image like this, unlike other spoof attacks on single modalities. Also problems such as over fitting leads to complex models with unstable variables. The proposed algorithm makes the system more efficient and major factors like time and speed were not compromised by fusing a third modality in the system. Over fitting issue was also solved.

Block based feature matrices are created after extraction of interesting and useful features. Sizing should be kept in mind while using the fusion technique so as to avoid overlapping complexities. Sufficient light is thrown over this matter. In the previous work, face and fingerprint were fused after image enhancement and geometric normalization. The proposed work enhances the system security by adding one more threshold or modality – Iris. The reason to choose iris as the third modality in our research is simple and crystal clear – Performance of iris as a single trait is substantially impressive and combined with more traits (Here face and fingerprint) increases the overall accuracy and performance factor.

Bayesian statistical techniques were investigated. Over fitting problem can be avoided by sizeable portions. Already existing VBELM is significantly improved in terms of optimization; time elapsed in the complete process by adding one more modality and decreasing the time complexity. The algorithm that works on neural network is understandable, reliable, and highly responsive and exhibits high performance. The features are taken as data inputs and trained on different parameters.

From normalized matrices, coefficient rules are extracted. Artificial neural network has the ability to derive useful features from complicated data, exhibits real time operation, has fault tolerance and is deeply organized. Iris as a modality is added which has very high accuracy rate as a biometric modality. There are really less chances of iris to be mirrored as the Hodge centre remains nearly the same. In a crux, one can say that the proposed work is time-efficient, appends security by increasing a modality and exhibits stupendous results.

## IV. Algorithm

The working of our system is basically an improvised VBELM, with data being trained on Neural Network inclusive of three modalities – Face, Fingerprint and Iris.The basic objective of this algorithm is that it should be time-efficient, precise, and unique, with less time execution and increased accuracy and recognition rate. The algorithm is curated with great precision paying attention to minute details like accurate feature extractions and image enhancement with techniques like noise removal with filters, unsharp mask filtering and deblurring .

The steps were designed as follows:

STEP 1: Input

Input standard images of Fingerprint, Face and Iris.

STEP 2: Image pre-processing

Image acquisition, segmentation, normalisation and illumination.

First stage of any vision system is image acquisition.

STEP 3: Features are extracted (Features are numerical description of an image), pre-processing of images are done.

Face: Illumination and geometric normalization.

Fingerprint: Image enhancement, segmentation, normalisation. (Remove blur)

Iris: Remove irrelevant information, localization and normalization of the iris image.

STEP 4: Extraction of features.

Features are extracted and region of interests (ROI) are taken out for face and fingerprint. We go for Gabor filter feature (GFF), Zernike Moment feature (ZMF) and Local Binary Pattern feature.(LBP)

STEP 5: Assign input weights (From any random interval from R to Rn) and calculate output weights w ,where w =( ΦTΦ)-1ΦT (Moor Penrose Pseudo Inverse of matrix Φ) [7]

STEP 6: Fusion of face and fingerprint images.

MoorePenrose pseudo inverse is applied and weights are assigned. [7]

Gabor filter, LBP filter and Zernike moment calculation is done.

Gabor filters: Used for time frequency analysis of image. [7]

Zernike moment: Zernike moment descriptor extracts the Zernike moments.

LBP Filter: Robust the image and makes it clearer. A uniform pattern with a fixed size extracts this feature.

Therefore features can be summed up as :

Local features of face: Fib = [FiG ,FiH , FiL], i = 1, … , K.

Local features of fingerprint images: FtiB = [FtiG, FtiH,FtiL]

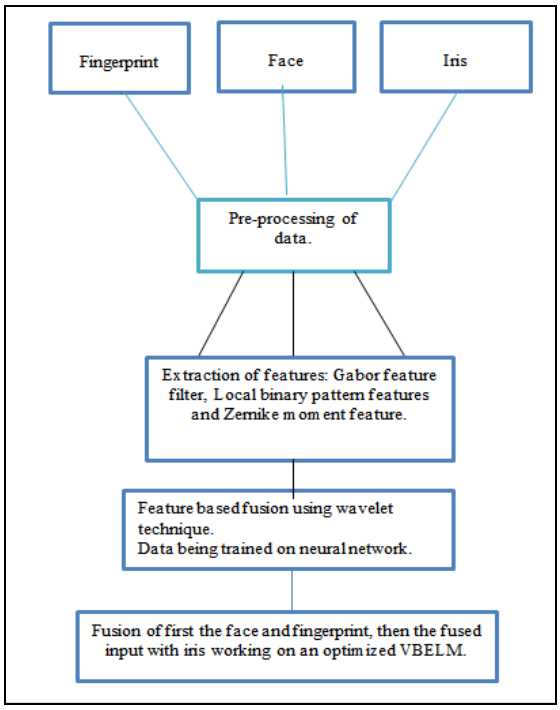


Figure 1: OVBELM Methodology

STEP 7: Iris's features are extracted.

Image partitioning is done. Visibility, spatial frequency, energy of gradient, variance and edge information is studied.

STEP 8: Data is collected in form of feature matrix and trained.

STEP 9: Proposed block based feature level algorithm integrates wavelet transform with neural network by incorporating Iris and fusing it with already fused image (Face and fingerprint) is re-fused and a new final image is curated. [24]

STEP 10: Second level discrete wavelet transform is applied.

Partition LL2 components of images and extract features.

STEP 11: NEURAL NETWORK

An index vector is constructed which will be used as an input for neural network with adequate number of layers and neurons.Take put three features from iris and fused image respectively and fuse them.Train the neural network for two conditions:

Targeti = { 1 , if features are clear

0, if they are not. }

STEP 12: PERFORM TESTING

perform testing of the trained neural network on all image block pairs.

STEP 13: Verify the fusion result in terms of time elapsed and the complexity factor and analyze the experimental results.

Compare results with the normal algorithm

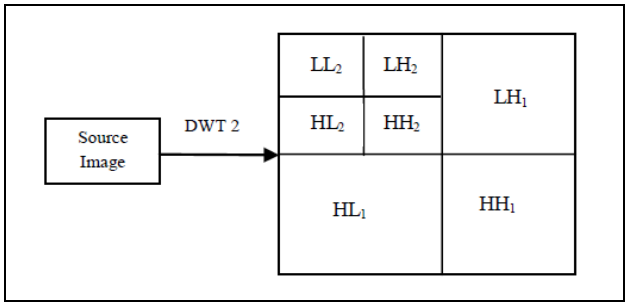


Figure 2: DWT Wavelet Transform[24]

## V. System Functioning

After substantial research, our problem statement would be to curate a working system which addresses all the existing problems in research papers and scholarly articles. Need of the hour is an algorithm which is actually effective and efficient and time-effort optimization is present with wider application. Image fusion is basically summation of important features into a single informative figure.

Adding one more modality in a multimodal system which uses feature fusion via VBELM is a challenge. The most accurate modality will end in a more accurate result. We ended up choosing Iris as the third modality along with face and fingerprint. As per a survey conducted by M2SYS (a biometric solution provider), 58% people chose iris as the most accurate modality. The small template size (speedy matching), strong acceptance rate, accuracy and unique pattern were some of the characteristics on which this modality was finalised. Medically, the structure of the iris remains the same with a 1 in 1078 chance of two irises actually matching. [25] Not to confuse retina and iris, as retina involves scanning of veins while iris recognition all depends on iris size and structure. [26]Hence the system designing was such that the biometric system hence created has fault-tolerance, quick speed and effective results.

## VI. Experimental Results

### A. Experimental Results

The functioning is based on the algorithm mentioned in section 4.

Features are extracted and region of interest (ROI) areas are chosen. The background image of fingerprint and the face were fused resulting in a new fused image which was further fused with iris on an improved VBELM algorithm trained on an artificial neural network. Also the features were extracted and images were improved. The results are not only spastically sound but also biometrically feasible. We run a trial of over 250 runs and the best trials were taken for a result analysis. The functioning of this algorithm exhibited some results and processing data which is attached in this section. Screenshots of trials are attached at the end of this section. After summing up the trials, average results were taken and jotted down which are as follows.


Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

**Table 1: Complete average values of 250 trials**

| Characteristics | VBELM | Proposed VBELM |
|---|---|---|
| Time taken | 84.6183 sec | 32.7283sec |
| Mean square percentage | 16.25% | 0.95% |
| AVE time | 94.3665 sec | 26.3738 sec |

**Figure 3:** 16 different face values for facial recognition[27]

**Figure 4:** Test data for face recognition[28]

**Figure 5:** Variations in the same person, taken from FERET database

**Figure 6:** Variations in the same person [29]

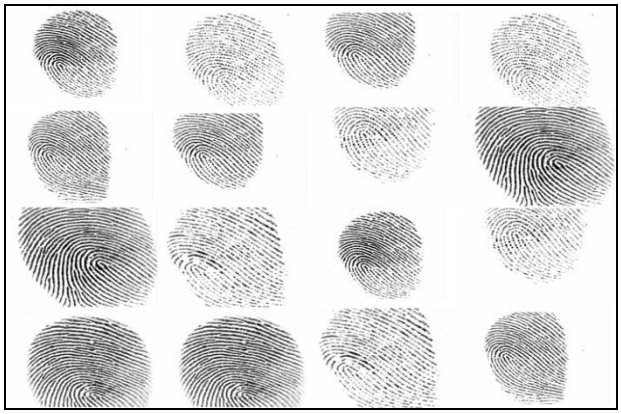

**Figure 7:** Fingerprints taken from FVC2002 database [30]

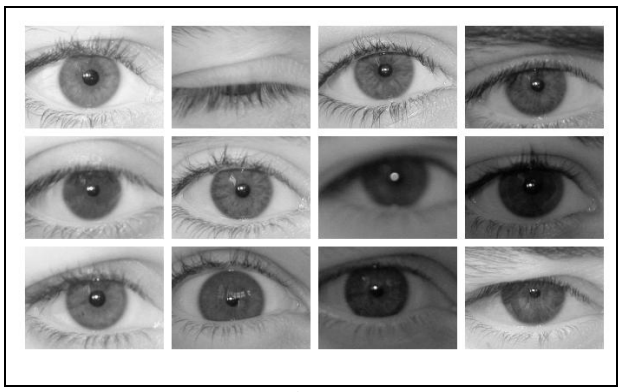

**Figure 8:** Iris samples from UBIRIS Database[31]

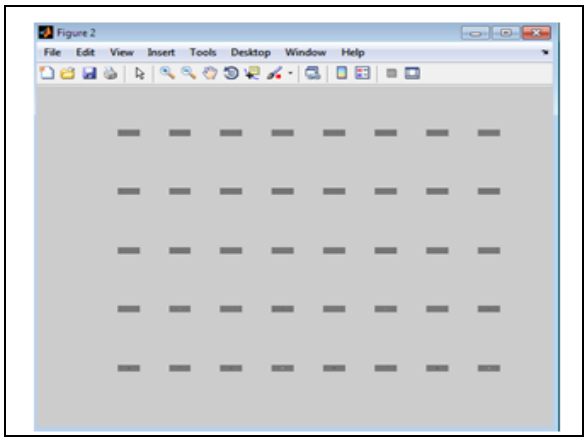


**Figure 9:** Gabor Filter Feature


Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication


**Figure 10:** An example of Fingerprint extracted Features

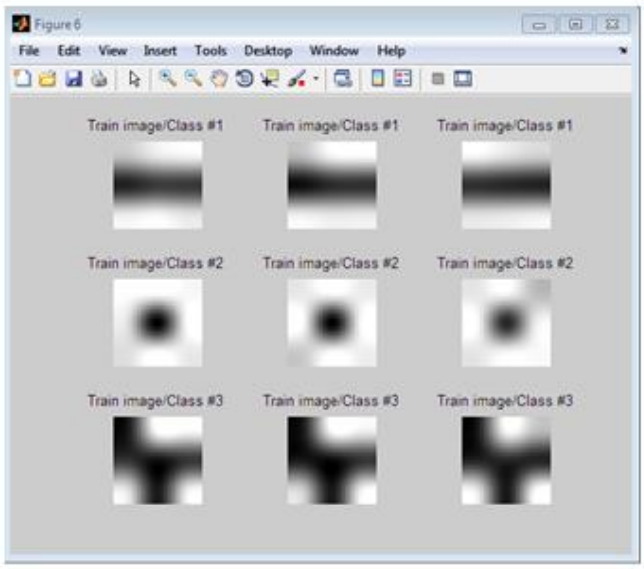


**Figure 11:** Train Images

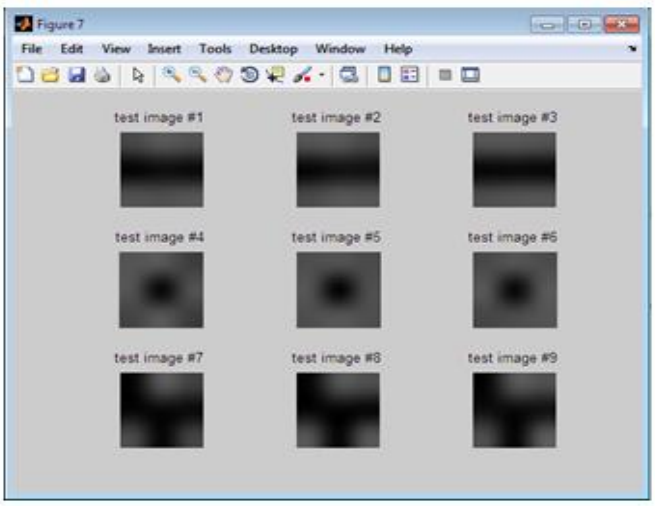


**Figure 12:** Test Images

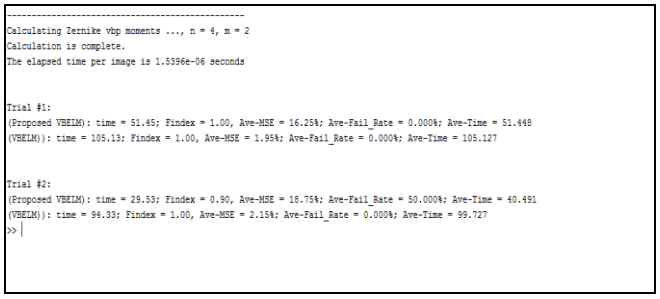


**Figure 13:** Trial 1

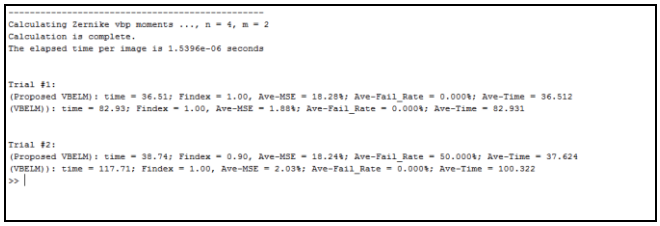


**Figure 14:** Trial 2

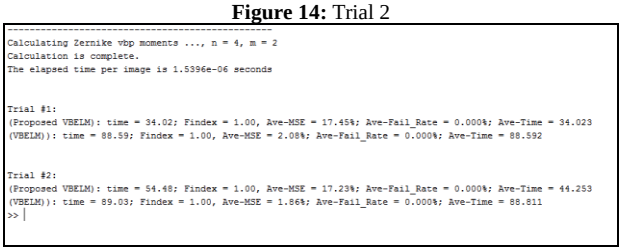


**Figure 15:** Trial 3

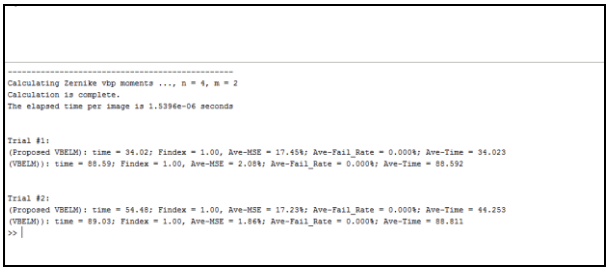


**Figure 16**: Trial 4

*B.* Result Discussion

Database plays an integral part in any system. We took three databases.

- Face images = FERET Database [27]
- Fingerprint images = FVC2002 Database [30]
- Iris images: UBIRIS Database [31]

In this section of result discussion we highlight the findings and analysis of the research we have proposed in this paper .While fusing the sample images we took care that certain factors were kept in mind which were not fulfilled in earlier research. The work was curated such that certain factors created a comparison between Variational Bayesian Extreme Learning Machine (VBELM) and Optimized Variational Bayesian Extreme Learning Machine (OVBELM). The comparison is as follows:

**Table 2:** VBELM VS OVBELM

| Comparison Factors | VBELM | OVBELM |
|---|---|---|
| Execution Time | 95.82seconds | 40.78 seconds |
| Average Fusion Time | 17.88seconds | 2 seconds |

**Table 3:** Metrics Comparison between VBELM VS OVBELM

| Metric | VBELM | OVBELM |
|---|---|---|
| Testing accuracy | - | Increased |
| Error Rates | - | Increased |
| Fusion Parameters | Same | Same |

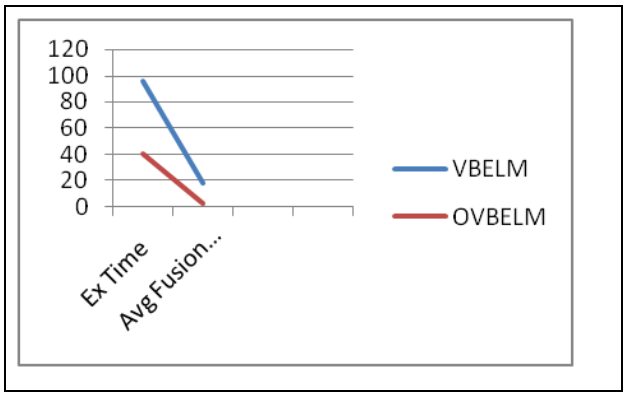


**Figure 17:** Comparison between VBELM and OVBELM

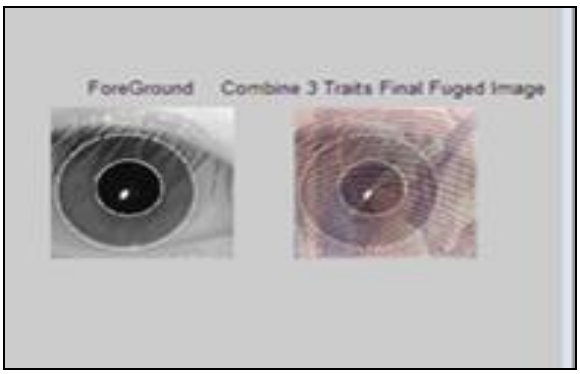


**Figure 18:** Sample Fusion.

## VII. Conclusion and Future Work

This research paper designs a stable, efficient, and accurate multimodal biometric system based on local features which are fused to give a new fused image which is not only feature rich but also makes the system impossible to breach. With this approach of optimizing VBELM, not only has time decreased, security has further more increased with the advent of increased feature fusion with three modalities. The system is secure, stable and incorporates a cleaner biometric system in comparison to the earlier system. The feature fusion of face, fingerprint and iris was done to append the necessary features and the resultant fusion image has a strong hold, is threat proof and doesn't even decrease the time complexity because of image pre-processing and image enhancement. Several upcoming avenues of research in this field can make a drastic difference in the field of biometrics and image processing. Experimental results have proved that error rate has substantially decreased and time complexity and system complexity has decreased as well. New additions can be done to make this system more worthy and effective. One can even add more performance parameters than testing parameters and weight combinations can be differed. In terms of future work, one can vision more areas of fusion and maybe more modalities like veins and brain prints.And this could be the potential future of the biometric security in the coming years. As a substantial research method, brain scans will be the ultimate password which would be unique to every individual resulting in a highly processed and scientific approach. Therefore a set of modalities can be replaced by either veins or brain prints being scanned on a deeper neural network.

## REFERENCES

1. AkankshaAggarwal, Manoj K. Verma, "Enhancing Performance of multimodal biometric system using gabor feature and similarity index" June 2016, International Journal of Engineering Trends and Technology (IJETT).
2. Peter Waggett, IBM (2016), "Risk-based Authentication: Biometrics brave new world".
3. Sandhaya Tarar, Ela Kumar, "Fingerprint Mosaicking Algorithm to Improve the Performance of Fingerprint Matching System", 2014, Computer Science and Information Technology .
4. RuchiKumari, Sandhya Tarar," An Efficient High Dimensional Indexing Method For Content Based Image Retrieval (CBIR)", International Journal of Engineering and Techniques - Volume 2 Issue 3, May – June 2016
5. SubiyaZaidi, Sandhya Tarar, Shrish Kumar Singh, "To evaluate the performance of fingerprint enhancement techniques",2015 Annual IEEE India Conference (INDICON).
6. Sandhya Tarar, ElaKumar,"Fingerprint Image Enhancement: Iterative Fast Fourier Transform Algorithm and Performance Evaluation",2013, International Journal of Hybrid Information Technology, Volume 6, No.4, July 2013.
7. Guang-Bin Huang, Qin-Yu Zhu, Chee-KheongSiew,,"Extreme Learning Machine: Theory and applications", Volume 70, Issues 1-3, December 2006, Pages 489-501.
8. Hai-Jun Rong, Yew-Soon Ong, ,"A fast pruned extreme learning machine for classification problem", December 2008, Volume-72, Issues 1-3, Pages 359-366, Neurocomputing, Elsevier.
9. Jun-Ying Gan, Jun-Feng Liu, "Fusion and recognition of face and iris feature based on wavelet feature and KFDA", 2009 International Conference on Wavelet Analysis and Pattern Recognition, IEEE.
10. Mohammad Hanif, Usman Ali," Optimized Visual and Thermal Image Fusion for Efficient Face Recognition", 2007, 9th International Conference on Information Fusion, IEEE.
11. Yibing Wang, BangjunHu , "A More Efficient Face Recognition Framework Based on Illumination Compensation, Kernel PCA and SVM", 2014 Seventh International Symposium on Computational Intelligence and Design, IEEE.
12. Mina Farmanbar, OnsenToygar ," A Hybrid Approach for Person Identification Using Palmprint and Face Biometrics", June 2015, International Journal of Pattern Recognition and Artificial Intelligence 29(6):1556009.
13. Maryam Eskandari, OnsenToygar ," A new approach for face-iris multimodal biometric recognition using score fusion.", May 2013, International Journal of Pattern Recognition and Artificial Intelligence, Volume 27, Issue 03.

14. OmidSharifi, MaryanEksandari ," Optimal Face-Iris Multimodal Fusion Scheme", June 2016, Symmetry 8(6):48.
15. Chhaya Verma, Dr. Sandhya Tarar, "Watermark extraction and validation in images using hybrid techniques"(2016), International journal of computer science trends and technology(IJCST), Volume 4, Issue 1.
16. Maria V. Ruiz, Zhanpeng Jin, Sarah Laszlo," CEREBRE: A Novel Method for Very High Accuracy Event-Related Potential Biometric Identification.", July 2016,IEEE Transactions on Information Forensics and Security ( Volume: 11, Issue: 7, )
17. C.M Sheela Rani, V. Vijaya Kumar, et al , "An Efficient Block based Feature Level Image Fusion Technique using Wavelet Transform and Neural Network.", August 2012, International Journal of Computer Applications (0975 – 8887) Volume 52– No.12.
18. Secure ID News, Online source: https://www.secureidnews.com/news-item/iris-vs-retina-biometrics-yes-they-really-are-different/
19. M2SYS Blog on biometric technology, Online source : http://www.m2sys.com/blog/biometric-hardware/reliable-biometric-modality/
20. Feretdatabase : http://www.itl.nist.gov/iad/humanid/feret/feret_master.html
21. "Euclidean & Geodesic Distance between a Facial Feature Points in Two-Dimensional Face Recognition System", Dec 2016, RachidAhdid, KhaddoujTaifi.
22. Shouyi Yin *, Xu Dai, PengOuyang, Leibo Liu and Shaojun Wei, "A Multi-Modal Face Recognition Method Using Complete Local Derivative Patterns and Depth Maps", Sensors , 2014, 14(10), 19561-19581.
23. Online Source: http://bias.csr.unibo.it/fvc2002/
24. Online Source :https://utiris.wordpress.com/2014/03/04 /university- of-tehran-iris-image-repository/