# PlexNet: An Ensemble of Deep Neural Networks for Biometric Template Protection

Ashutosh Singh[1]
Institute of Engineering and Technology, Dr. A.P.J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow, India

Ranjeet Srivastva[2]
Babu Banarasi Das Northern India Institute of Technology, Dr. A.P.J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow, India

Yogendra Narain Singh[3]
Institute of Engineering and Technology, Dr. A.P.J. Abdul Kalam Technical University, Uttar Pradesh, Lucknow, India

***Abstract*—The security of biometric systems, especially protecting the templates stored in the gallery database, is a primary concern for researchers. This paper presents a novel framework using an ensemble of deep neural networks to protect biometric features stored as a template. The proposed ensemble chooses two state-of-the-art CNN architectures i.e., ResNet and DenseNet as base models for training. While training, the pre-trained weights enable the learning algorithm to converge faster. The weights obtained through the base model is further used to train other compatible models, generating a fine-tuned model. Thus, four fine-tuned models are prepared, and their learning are fused to form an ensemble named as PlexNet. To analyze biometric templates' security, the rigorous learning of ensemble is collected using a smart box *i.e.,* application programming interface (API). The API is robust and correctly identifies the query image without referring to a template database. Thus, the proposed framework excludes the templates from database and performed predictions based on learning that is irrevocable.**

***Keywords*—Biometrics; template protection; deep learning; transfer learning; ensemble**

## I. Introduction

Identity theft is one of the major epidemics of current century. In the absence of a reliable identity proofing system, data and information thefts have plagued the applications such as online transactions and social welfare schemes [1]. Traditional security systems such as ID cards and passwords cannot protect from digital impersonation thus, obsolete due to their lost and stolen possibilities [2]. To overcome the problems of lost and deliberate sharing of identity markers, biometric recognition has introduced and gradually became the prime tool for individual authentication. Biometrics uses the physiological or behavioural traits of an individual for identification. Commonly used physiological traits include face, fingerprint, palmprint and hand geometry, while signatures, gait, voice are used as behavioural traits. These biometric traits are proved to be personal, reliable, accessible and universal [3].

Although, the biometric systems are reliable in comparison to traditional identification systems, they are vulnerable to several exploits. The biometric system vulnerabilities can be broadly categorized as faults, failures and attacks [4]. Faults are mistakes made by human or system such as data corruption, software aging and storage space fragmentation [5]. A failure is the consequence of one or more faults. It may be service failures, development failures or security failures. Unexpected service, wrong prediction of complexity or unaccounted situations and imbalance thresholds are some examples of service, development and security failures, respectively.

The faults and failures may lead to fraudulent attacks on machine (*i.e.*, hardware and software) as well as at the administrative level [2]. These attacks can be broadly classified as the sensor level, feature extraction level, matcher level and database level attacks. At sensor level, covertly acquired fake samples such as digital face images, synthetic fingerprints or recorded voice can be presented. The replay of raw biometric trait or injection of false data before pre-processing or feature extraction are common feature extractor level attacks. The attacks on communication channel between feature extraction and matcher module is considered as matcher level attack. For example, infested bug to the algorithm or alteration of match score are some matcher level attacks [6].

The attacks on database consists of templates, are possibly the most prominent fraudulent attacks on a biometric system. The template includes biometric characteristics of an individual that may be compromised, if attacked. Storage of templates in diverse applications create a serious threat to the user's privacy [27]. Thus, a robust mechanism is required to secure the templates stored in the database. An ideal mechanism of template protection should meet the following requirements [8]-[10], [29].

- *Cancelability*: The compromised template must be revoked by reissuing a unique template from the same biometric features.
- *Diversity*: It defends user privacy by ensuring that same template is not being used across databases.
- *Security*: The recovery of original template from the compromised ones must be computationally harder. It avoids the fabrication of a physical spoof from the compromised template.
- *Performance*: The template protection mechanism should not affect the recognition performance of the biometric system.

Despite several template protection schemes, the protection of biometric templates while preserving it's discriminability is still a challenge [8]-[9], [12]-[28], [30], [16]-[17]. In this paper, a novel framework is designed to collectively meet all

the requirements of a robust biometric template method. It achieves high performance through rigorous learning of ensemble that forms the basis for exclusion of template from the database. The absence of a template ensures the cancelability and security requirements, whereas immovable learning avoids it's use in diverse applications.

The proposed ensemble is named 'PlexNet' due to it's resemblance to the plexus such as network of nerves in the nervous system [7]. It is a network of pre-trained and fine-tuned architectures of the variants of deep networks *i.e.*, ResNet and DensNet thus, creating four network paths as shown in Fig. 1. Initially at each path, one of the architectures from ResNet or DenseNet is used as base model trained on biometric sample *e.g.*, facial images with weights of ImageNet database. The weights obtained from base model are further fine-tuned with a compatible architecture. The combination of fine-tuned weights from all network paths results an ensemble the 'PlexNet'.

The contribution of the paper is for the protection of biometric templates using ensemble learning. The plexnet is prepared using ensemble of transfer learning. As transfer learning is a well-established method for converging to the desired goal faster and more accurate, hence we are implementing transfer learning as a tool. Also, the existing ensemble methods generally use majority voting or averaging mechanism that made predictions based on the individual training of the models. Whereas, the proposed ensemble method combines the learning by fine stacking all the fine-tuned models and then retrains on the target dataset. Therefore, the training of ensemble takes the advantage of the weights gathered by each of the fine-tuned model and converges faster with better accuracy than the traditional ensemble models.

The learning of the PlexNet is conducted in an application programming interface (API). The API acts as an smart box to predict the class label for the presented biometric template *i.e.*, facial image as shown in Fig. 2. The learning at API is done so vigorous that it correctly identifies the input image without referring to a template. Thus, the prepared API eliminates the requirement of nurturing a template database. Further, it follows the requirements of a robust template protection method. For example, cancelability *i.e.*, there is no chance to compromise the templates. The learning of the model can not be directly transferred to other models, thus, diversity is ensured. It matches security paradigms, as the recovery of original image is almost impossible. The high performance reported by our proposed PlexNet framework forms the basis for exclusion of the template database. Briefly, the substantial contributions of this work are as follows:

1. A novel ensemble of deep neural networks is designed for biometric template security, as called 'PlexNet' due to it's resemblance to the plexus in the nervous system.
2. An innovative learning procedure is adopted using pre-trained models that results in faster training and testing, that further solves the problem of class imbalance.
3. Primally, application program interface (API) is constructed that predicts the output based on rigorous learning without referring to a template database.
4. The efficacy of proposed framework is evaluated on challenging databases of face biometrics e.g., VGGFace2 and MegaFace. PlexNet outperforms other methods and supports presented method of template exclusion thus, making it impregnable.

The rest of the paper is organized as follows. The literature survey of the biometric template protection is presented in Section II. The proposed ensemble framework with a detail description of architectures used and the requirement of transfer learning, ensemble learning and data augmentation are discussed in Section III. The experimentation process that includes database description, experimental setup, results along with security analysis are presented in Section IV. Finally, the conclusions are drawn in Section V.

## II. Literature Survey at a Glance

The rapid growth in technology and sensing have increased the demand of deployment of the biometric recognition system *e.g.*, at residences, offices, portable devices and other public access checkpoints. Though, this easiness has brought numerous challenges of biometric vulnerabilities that effects the system may be exploited by an adversary. Thus, an efficient and robust mechanism for biometric template protection is essential. The information captured by the sensor may differ for the same biometric trait. So, the conventional method of password protection using cryptographic hash functions can not be directly applied to a biometric system. Normal encryption is not a sustainable solution, as the saved template must be decrypted every time to make the comparison with the query template. Several biometric template protection techniques have been developed [8], [9], [12]-[28], [30], [16]-[17]. Various biometric template protection techniques are classified as follows,

1. *Biometric Cryptosystems:* Biometric cryptosystem was originally developed to protect keys either using biometric features or generating a cryptographic key [8], [9]. Later, it evolved as a technique for template protection. In a biometric cryptosystem, public information known as helper data is stored in the database instead of original biometric template [10]. This helper data is independent of biometric template and do not reveal the biometric features. It just helps to recover the key used for encryption. Hence, matching is performed between the key extracted from the query template and the stored template key. Biometric cryptosystems can be classified into key binding and key generation approaches [48]. These algorithms differ in the way they generate the helper data.
   (a) *Key binding approach:* In the key binding approach, the helper data is obtained by associating a key with the biometric template. The helper data is stored as a template in the database. Since the key is independent of the biometric data, it is really hard to recover the original template or the binding key for the helper data. The stored template is used for key recovery at the time of matching with query template. Thus, the authentication is performed with matching of query and stored keys. This approach is primarily used for key protection. The utilization of these approaches for template protection may not fulfil the criteria of cancelability. Here, the

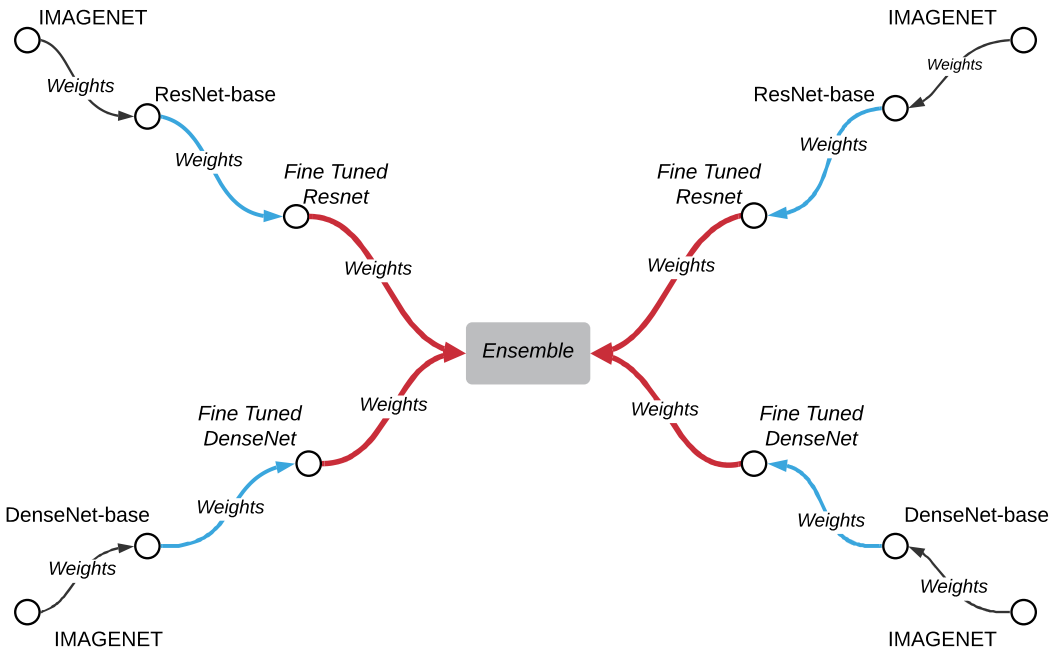


Fig. 1. Proposed PlexNet Architecture.

matching is based on error correcting code that may produce incorrect results. Further, if the key is leaked, the original template can easily be acquired.

Fuzzy vault and fuzzy commitment are cryptographic based protection techniques [20], [12]-[13]. A fuzzy vault scheme where a key $k$ is locked using an unordered set $A$ is proposed by Juels and sudan [20]. During the enrollment phase, a polynomial $p$ comprising of the biometric features is used to encode key $k$ resulting in $p(k)$. The unordered set $A$ is projected on $p$ and some false points are added to secure the location of $p$. During authentication, if the query template overlaps the genuine location of $p$, key is reconstructed. Further, the idea was extended by Uludag *et al.*, securing fingerprints [21]. Nandakumar *et al.*, proposed the idea of using password for further strengthening fuzzy vault [22]. Though a robust technique in the past, this scheme fails to provide revocability and protection from matching across biometric systems.

Another key binding approach *i.e.*, fuzzy commitment is developed combining two approaches of cryptography and error correcting code. Here, during enrollment phase, a random key is encoded using error-correcting codes. The resultant is a codeword $c$. A hash value of $c$ is also computed. The XOR operation is performed between generated codeword $c$ and the biometric features, resulting in an encrypted template. This encrypted template known as helper data, is stored along with the hash value of $c$. During authentication, the features from query template are decoded and XOR operation with helper data is performed to obtain codeword $c'$. If hash $c$ matches the hash $c'$, the user is accepted as genuine. Further, this scheme is extended using helper data with face biometric [15].The limitation of the fuzzy commitment scheme lies in the use of the template as helper data. If the biometric data is non-uniform, helper data may leak information on the secret key as well as about the template itself [14].

(b) *Key generation approach:* In this approach, the helper data is generated using biometric template. The key is generated from the helper data and query template. The basic principle of key generation technique is the quantization of helper data that produces the cryptographic keys [24], [26]. The biometric feature vector is divided into several intervals of feature elements. These intervals are selected from multiple biometric instances and encoded to store as helper data. During authentication, a similar approach is applied to the query template. A correct mapping between the intervals results in a key. The key generation algorithm with a quantization approach, can extract same keys from several instances of biometric data provides high stability. However, making it vulnerable to security attacks due to record multiplicity [19]. Moreover, if separate keys are generated for several instances of biometric data, the system suffers from increased entropy and reduced stability resulting in a high rejection rate.

The concept of secure sketch and fuzzy extractor

was introduced by Dodis *et al.* [25]. A secure sketch is obtained when a biometric template is encoded with a special algorithm. The query template and the secure sketch is required to decode the template, generating the near matching original template. Fuzzy extractors take input biometric identifiers as noisy data and generates a key as well as a helper data. During authentication, it requires both the helper data and the noisy data (query biometric) and generates the matching key.

2. *Template Transformation Approaches:* Here, a transformation function $(f)$ is applied to the original biometric template $(t)$ and only the transformed template $[f(t)]$ is stored in the database. The transformation function can be derived from any random key or password-based approach. During matching, the same function $(f)$ is applied to the query template $(t')$ and is compared against the original transformed template $[f(t)]$. The template transformation can be further categorized into invertible *i.e.*, salting and non-invertible transformations [8], [49].
(a) *Salting technique:* In salting, the biometric features are transformed using an invertible transformation function. Since a key is used for transformation, it should be secured and only be available for authentication. Due to a fixed key used for transformation, system achieves low false acceptance rate (FAR). Connie *et al.*, used pseudo random keys for hashing palmprint templates [30]. A salting technique for face templates is proposed by Teoh and Ngo [31]. They also introduced a biophasor technique based on salting [28]. The transformed template can be inverted into the original if the transformation function is known. Thus, the salting technique suffers from the problem of invertibility making it susceptible to adversary attacks. Random projection is another example of salting technique, where the original biometric template is projected to another domain by a matrix with zero mean and unit variance. The problem with random projection is that the original matrix can be recovered if the projection matrix is known to the adversary. Zhe *et al.*, proposed a ranking based hashing that demonstrated two notions, one sued random projection while the other used random permutation-based hashing schemes. Hence, generating invertible as well as non-invertible transformations [32].
(b) *Non-Invertible transformation:* On the contrary, a key is used as a transformation function in the non-invertible transformations making it a one-way transform. So, even if the transformation function is known, the inversion is computationally harder to achieve. A non-invertible transformation function for fingerprint is used by Ratha *et al.* [34]. In another work, they proposed Cartesian, polar and functional transforms that are non-invertible [11]. These functions transform the fingerprint minutiae *e.g.*, the Cartesian transformation divides the minutiae space into a grid and each cell is rearranged to a new position according to the key. The query template is transformed similarly and matched to the original transform for authentication. The use of robust hash function provides better cancelability and security than salting, but the performance may decrease. One of the reasons for low performance of these biometric systems are that they do matching in transformed domain that results in high FRR. Further, if the transformation function is compromised, the system loses non-invertability. Thus, it is difficult to achieve a balance between discriminability and non-invertability.

3. *Hybrid Approaches:* Hybrid approaches were also introduced to take the advantages of both biometric cryptosystem and transformation. Feng *et al.*, proposed an approach, where the extracted template is randomly projected to a subspace generating a cancelable template [33]. The discriminability is increased during the transformation and finally fuzzy commitment is used to protect the generated cancelable template. A hybid method based on revocable biotokens for face biometrics is proposed by Boult [35]. Liu *et al.*, combined fuzzy vault technique with multi-space random projection to improve the security of palmprints [36]. The fingerprint and palmprint features are combined to build a hybrid system [37]. Further, neural network was introduced in combination with secure sketch [38]. This combination provides high tolerance against noisy data as well as revocability and non-invertibility. Sardar *et al.*, proposed a hybrid solution by combining the non-invertibility with a biocode encryption. This helped in enhancing security levels along with better accuracy [39]. Talreja *et al.* proposed a multibiometric template protection using binarization and hashing that uses a key for each individual during identification, hence the use had to have they key during the recognition process [40].

## III. Proposed Ensemble Framework

The machine learning techniques simulate the learning process of the human brain and automatically create significant feature vectors. The major issue of these techniques is their limited generalization capability. For example, if the unseen patterns are to be tested, these methods usually results in unconvinced predictions. To improve generalizability, deep neural networks, particularly convolutional neural networks (CNN's) have evolved. The CNN's are proved to be very effective in several image processing and computer vision applications [44]. The capabilities of CNN's are yet to be explored for biometric template protection. The performance and generalizability of CNNs motivated us to utilize it for securing biometric templates. Two state-of-the-art CNN architectures *i.e.*, ResNet and DenseNet are used in order to form an ensemble.

### A. CNN Architectures

The CNN is designed stacking three types of layers *i.e.*, convolution, pooling and a dense or fully connected layer. The convolution layer containing filters with numeric weights is responsible for feature extraction. The input image is convoluted with filters generating feature map. It contains the dominant features while preserving the relationship between the neighbouring pixels. More formally, let the input image be denoted as $x$, the filter be $f$ and the rows and columns of the

convoluted matrix are denoted as $a$ and $b$, respectively. Then, the convolution operation is defined as,

$$Conv[a,b] = (x*f)[a,b] = \Sigma_i \Sigma_j (f[i,j]\, x[a-i, b-j]) \quad (1)$$

Two CNN architectures *i.e.*, ResNet and DenseNet are chosen for making an ensemble [41], [42]. The selection of these architectures is based on their performances on VGGFace2 and MegaFace databases. In addition, these two architectures have several variants and proved to be complimentary to each other.

*1) ResNet Architecture:* The main idea behind ResNet is the skipping of one or more layers. The convolutional, relu, pooling and batch normalization layers are added in a redundant manner to form a residual network. The initial block consists of two $3 \times 3$ convolutional layers where each convolutional layers comprise 64 filters of size $3 \times 3$. The rectified linear activation (ReLU) is the default activation followed by a batch normalization to maintain the mean activation as zero and the standard deviation closer to 1. The size of the second convolutional layer is reduced using max-pooling of size $2 \times 2$. After each convolutional layer a dropout is applied to avoid over-fitting [50]. The strength of ResNet lies in its identity short-cut connection that flows the gradient by skipping one or more layers. It solves the vanishing gradient problem where the back-propagated gradient becomes infinitely small due to repeated multiplication. Thus, the identity short-cut connection provides the way to feed-forward the output of a ResNet block directly to the other block in the next layer.

More formally, let $\Theta_l(.)$ be a non-linear composite transformation function of convolution, ReLU, pooling and batch normalization. The output of a ResNet block at layer $l$ taken as $\Upsilon_l$, is [41],

$$\Upsilon_l = \Theta_l(\Upsilon_{l-1}) + \Upsilon_{l-1} \quad (2)$$

where $\Upsilon_{l-1}$, represents the input to a ResNet block at layer $l$. It means output of a ResNet block is depends on input from previous layer and it's non-linear transformation with function $\Theta_l(.)$. Several such blocks are stacked that create a short-cut path for the gradient that optimizes the back-propagation. Due to stacking, ResNet may results in generating redundant layers.

*2) DenseNet Architecture:* Huang *et al.*, proposed another solution to vanishing gradient problem using DenseNet [42]. DenseNet comprises of several blocks that are densely connected. The features generated by one block is input to the next dense block. In larger CNN models, there may be feature loss before it reaches to the output layer. DenseNet overcomes this issue with the use of repeated blocks. Further, the DenseNet requires fewer parameters in comparison to the other models such as ResNets, [43].

DenseNet architecture consists of dense block and transition layers. The dense block is a collection of different type of layers connected to similar previous layers. The feature maps are generated using $3 \times 3$ convolutional layer within a block. The generated feature maps are scaled with a batch normalization layer. The feature maps generated by each layer are concatenated together. Thus, the output of a layer $l$ in a DenseNet unit can be represented as:

$$\Upsilon_l = \Theta_l([\Upsilon_0, \Upsilon_1, .....\Upsilon_{l-1}]) \quad (3)$$

Here, the transition between two dense layers is achieved through a transition layer that controls the number of connections. The ResNet and DenseNet architectures are found to be complementary to each other due to the fact that both provide solution to vanishing gradient. The ResNet handles it with large number of parameters that is compensated by feature reuse in DensNet.

### B. Transfer Learning

In order to overcome the issue of under-fitting in smaller databases, the concept of transfer learning is introduced [51]. The weights of a pre-trained model are utilized while training a new model on a different database. Thus, the learning starts from an elevated point that avoids data insufficiency. Moreover, the identical distribution of training and test data is not required while using transfer learning.

Formally, let, $\zeta_1$ be the learning curve of a model pre-trained on database $\chi_1$. The goal is to improve the learning curve, $\zeta_2$ for a new model with a new database $\chi_2$. The learnt behaviour of the model pre-trained on, $\chi_1$ is transferred to the predictive function, $\phi$. The function $\phi$ in turn, improves the learning curve, $\zeta_2$ on database $\chi_2$. Several state-of-the-art image classification methods are based on transfer learning [53]. Different model are pre-trained on ImageNet that contains millions of images of over 1000 categories [18]. The upper layers of these pre-trained models can be fine tuned to match the current model working on the new database.

### C. Ensemble Learning

The pre-trained models perform better than a model that starts learning from the scratch. However, sometimes a single pre-trained model may not be enough to establish a robust learning for a given database due to class imbalance or concept drift [52]. To overcome this issue, ensemble of learning algorithms is used for many classification problems [54]. It performs learning by combining different learning models to a single predictive model.

An ensemble network can be built using different classifier architectures, initial weights and training databases. Although, the use of different classifier architecture may be a good choice, it requires compatible architectures. For example, ResNet-152 architecture may accept the initial information from a ResNet-101 or ResNet-50, but can not accept the initial weights from other architectures such as DenseNet or VGG [41], [42].

The proposed ensemble framework *i.e.*, PlexNet is prepared using two pre-trained architectures *i.e.*, ResNet and DenseNet. These architectures are chosen over other architectures such as VGG, MobileNet, ResNetV2 and InceptionResNetV2, due to the following reasons,

- The ResNet and DensNet architectures have several variants that are compatible to each other. Thus, an ensemble with different classifier architectures is achieved.
- Secondly, these architectures have achieved better accuracies than other pre-trained architectures as shown in Table I.

The initial training starts with pre-trained models on ImageNet database [45]. These initial models are presented as the endpoint of the framework as shown in Fig. 1. The weights obtain after training the initial models on the query database are saved. These weights are then fed to the next level of compatible architectures present at the axons of the PlexNet architecture. Thus, the axon models are fine-tuned and achieve higher accuracy with faster convergence than their predecessors. Finally, these fine-tuned models are combined in an integrated stacking model to prepare a meta-learner *i.e.*, Now, feature level fusion is performed that fuses features from each fine-tuned model using concatenation. The result of fusion is a feature vector representing weights from each class. Further, the features are passed to a fully connected neural network of ensemble model that map the features to their corresponding classes based on expected likelihood.

The robust learning of PlexNet that ensures lower false prediction is collected and saved in a smart box *i.e.*, known to be an API as shown in Fig. 2. The query image does not expose features but maps to the appropriate class while processed with API. The model resembles the learning of a human brain to recognise a person using facial images. Learning with faces, again and again, created patterns in the brain that are to be known. If a similar pattern occurs then, there is no need to seek any reference but the brain matches the description with the learning did in the past and identify the person. Similarly, the API predicts the appropriate class of a query image referencing it's learning. Therefore, our model of template protection need not store templates in database for making predictions. Thus, the requirement of nurturing a template database is eliminated, hence making it impregnable against fraudulent attacks.

### D. Data Augmentation

To reduce the over-fitting due to class imbalance or rather unavailability of sufficient data, augmentation of images is performed for accommodating the intraclass variations [46]. Various transformation techniques are applied on the available set of images, such as geometric (*e.g.*, reflection, scaling, rotation, shear, translation) and photometric (*e.g.*, brightness, noise reduction, hue adjustments, edge enhancements).

In order to maintain the heterogeneity of generated images and space-time complexities to be minimum, online data augmentation is introduced. We use the image 'Datagenerator' function available in Keras that apply different transformations in each epoch [47]. For example, the images are flipped in one epoch, whereas zooming is applied in another epoch. As the number of epochs increases, so the number of transformation on the random images per class. Thus, each model learns with a different set of images per class at the axon level.

## IV. Experimental Results

### A. Databases

Two publicly available databases *i.e.*, VGGFace2 and MegaFace are used for training and testing all the architectures. The VGGFace2 database comprises of more than 9000 subjects spanning over different accents, ages and ethnicities [55]. There are more than 350 facial images per subject that are further subjected to augmentation. The size of the images varies from 50 pixels to more than 300 pixels, which are averaged to 225 pixels for the experimentation limitations. The facial images of this database are acquired in an unconstrained environment. It means the images have pose and style variations, front or side views and may contain torso part, hence putting more challenges to a face recognition system [56].

TABLE I. Testing Accuracies of base Models using Face Databases

| | *Accuracy (%)* | | | |
|---|---|---|---|---|
| | VGGFace2 | | MegaFace | |
| *Architecture* | 80:20 | 90:10 | 80:20 | 90:10 |
| ResNet | 93.14 | 90.93 | 96.46 | 94.65 |
| DenseNet | 92.52 | 89.12 | 97.21 | 95.74 |
| MobileNet | 88.71 | 85.41 | 95.39 | 94.18 |
| VGG | 89.25 | 87.34 | 96.29 | 95.96 |
| ResNetV2 | 90.69 | 88.32 | 95.76 | 92.77 |
| InceptionResNetV2 | 89.26 | 86.91 | 95.93 | 93.34 |

The MegaFace database contains millions of facial images belonging to hundred of classes [57]. The images are compressed using JPEG formats. The three channel colored images are available with a dimension range from $250 \times 226$ to $300 \times 312$. These are also changed from their original size to $225 \times 225$. The classes have an unbalanced distribution of images ranging from 500 to 700. In MegaFace database, images are taken in a constrained environment *i.e.*, the faces are cropped and only the front view is included.

### B. Validation Metrics

Let, $Pred = (Pred_1, Pred_2, Pred_3 \ldots . Pred_n)$ be the predicted classes by the classification algorithm, and $Act = (Act_1, Act_2, Act_3 \ldots . Act_n)$ be the actual $n$ classes. The proposed method is evaluated using following validation metrics,

- *True Positives (TP):* is the representation of a correct prediction of a positive class by the model *i.e.*, ($Pred_i = Act_i$), where $i$ represents class labels.
- *True Negatives (TN):* similar to that of true positives, true negatives are the correct identification of the negative class by the model *i.e.*, $(Pred_i \in (1 - Act))$.
- *False Positives (FP):* If the model predicts the negative class as the positive class it is termed as false positives *i.e.*, ($Pred_i = Act_j$), where i, j represents class labels from predictions and actual class sets, respectively and $i \neq j$.
- *False Negatives (FN):* If there is an incorrect prediction of a negative class it's a false negative *i.e.*, $((1 - Pred_i) \in (Act))$.
- *Confusion Matrix:* From the above predicted and actual labels, confusion matrix $C$ can be derived for the classes where $C_{i,i}$, determines the correct predictions for the $i^{th}$ class whereas $C_{i,j}$ determines the $i^th$ classes that were misclassified as $j^th$ class.
- *Precision & Recall:* With the calculation of number of TPs, FPs and FNs, the precision and recall are calculated as,

$$Precision = \frac{TP}{TP + FP} \tag{4}$$

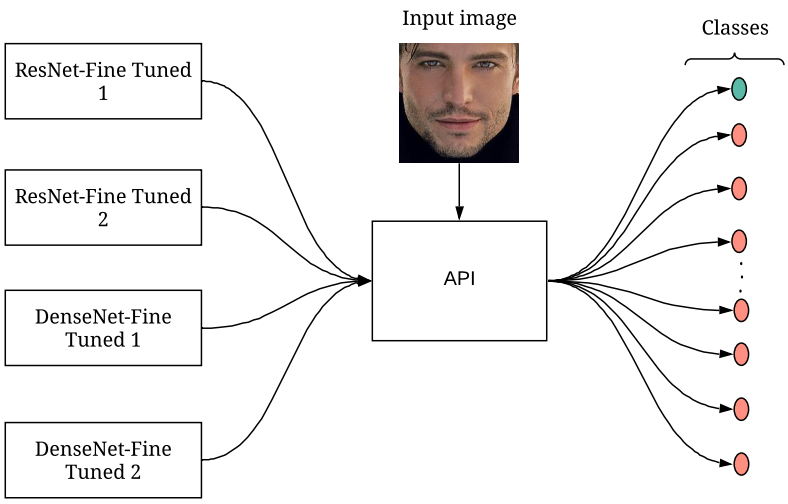


Fig. 2. API Generation using Score Fusion and Classification.

$$Recall = \frac{TP}{TP + FN} \tag{5}$$

- *F1-Score:* is the harmonic mean that represents a single measure for both precision and recall.

$$F1\,Score = \frac{2 \times Precision \times Recall}{Precision + Recall} \tag{6}$$

### C. Results

The selection of pre-trained models in PlexNet is based on the accuracy achieved on VGGFace2 and MegaFace databases, as shown in Table I. The accuracies of different architectures are evaluated at two different training and testing database ratio *i.e.*, 80:20 and 90:10. The accuracies at the 80:20 split ratio are found better than the accuracy at split ratio of 90:10 on both databases. So, all the experiments are performed on the training and testing database ratio of 80:20. On VGGFace2 database, the accuracy of ResNet base model is found to be the highest *i.e.*, 93.14% at the training and testing database ratio of 80:20. Similarly, the DenseNet achieves the best accuracy of 92.52% at the base model. The accuracies of all other tested architectures are found lower in comparison to these models. Similarly, on MegaFace database these two architectures achieve better accuracies. For example, the ResNet and DenseNet architectures achieve the accuracies of 96.46% and 97.21%, respectively. Beside the accuracies, ResNet and DenseNet complement each other, hence chosen as base models.

The PlexNet is prepared through the integrated stacking model using pre-trained architectures. The information gathered using all the pre-trained weights helps the ensemble to attain the best accuracies as shown in Fig. 3. The base models chosen for both the databases achieve lower accuracies. On VGGFace2 database, the ResNet base model achieves the accuracies of 88.54%, 93.45% and 93.14% at epochs 1, 5 and 10, respectively as shown in Fig. 3a. Similarly, the DenseNet base model at epochs 1, 5 and 10, reports the accuracies 73.24%, 90.12% and 92.52%, respectively. The fine-tuned model perform better using the learning weights of base models. For example, the accuracies of ResNet and DenseNet fine-tuned models are found to be 94.91% and 93.95%, respectively at 10 epochs. Finally, the fusion of fine-tuned models results in PlexNet that reports the accuracy of 96.48% on the VGGFace2 database.

The proposed method performs better on MegaFace database. The testing accuracies on MegaFace database is shown in Fig. 3b. Here, the testing accuracies of ResNet base model are 82.66%, 94.56% and 96.44% at 1, 5 and 10 epocs, respectively. The DenseNet base model performs better than ResNet base model. It reports the accuracies of 81.65%, 95.12% and 97.21% at 1, 5 and 10 epocs, respectively. Since, the MegaFace database contains facial images acquired in a constrained environment, it may results in lower intraclass variations, hence better accuracies are achieved using all the models. Here, the ResNet and DenseNet fine-tuned models reported the highest accuracies of 97.57% and 98.16% at 10 epochs, respectively. The overall accuracy of proposed PlexNet on MegaFace database outperforms all other existing methods and found to be 99.61%.

The values for precision, recall and F1-score on MegaFace database found to be better than VGGFace2 database and reported to 0.9948, 0.9946 and 0.9947, respectively. The higher values reported for these metrics on both databases further show the robustness of PlexNet. The values for these metrics demonstrate that VGGFace2 is a challenging database, as it contains images in unconstrained environment with large variations in pose, illumination and ethnicity.

The effectiveness of a biometric system is evaluated in terms of true acceptance rate (TAR). In order to achieve better visualization of the accuracy of the PlexNet, a receiver operating characteristic (ROC) curve is drawn as shown in Fig. 4. The ROC curve plots false acceptance rate (FAR) on x-axis and TAR on y-axis. Thus, a relationship is established between FAR and TAR that can be utilized while deciding a

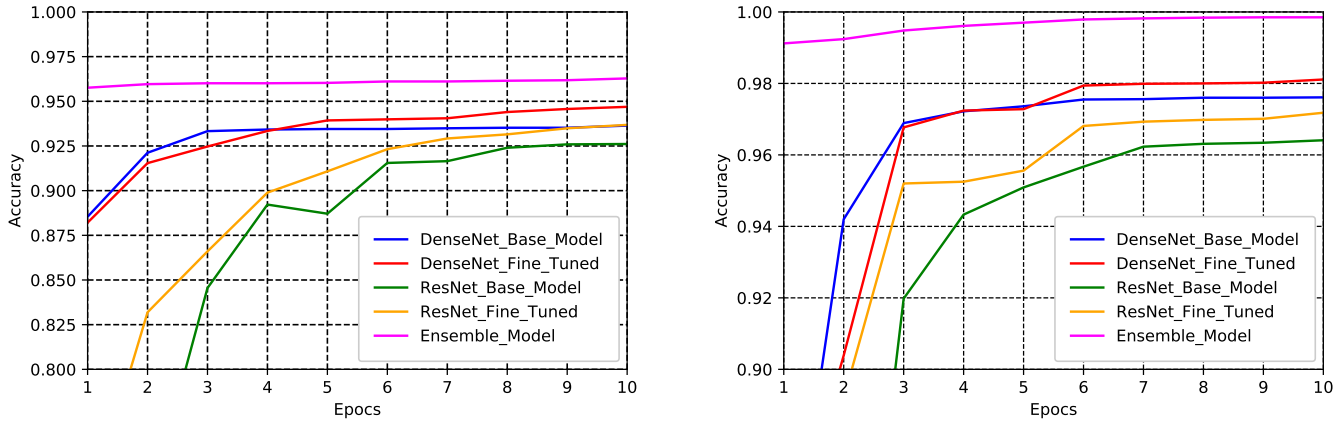


Fig. 3. Visualization of Testing Accuracies using a) VGGFace2 and b) MegaFace Databases.

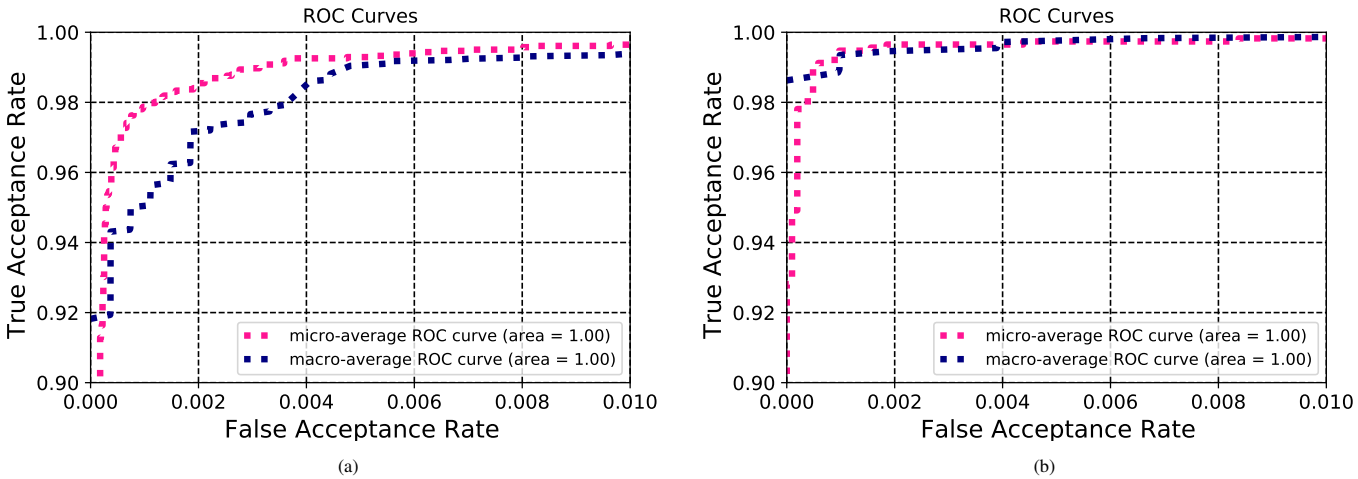


Fig. 4. Receiver Operating Characteristic Curves for a) VGGFace2 and b) MegaFace Databases.

threshold for FAR to attain optimal TAR. The PlexNet achieves 98% and 99% TAR at 0.2% and 1% FAR, respectively on the VGGFace2 database. It shows the effectiveness of PlexNet even on databases acquired in an unconstrained environment. The PlexNet performs better on the MegaFace database and reports a higher TAR of 99.6% just at 0.2% FAR. The TAR reaches to 100% at the FAR value of only 0.8%.

### D. Comparative Analysis

The performance of proposed template protection method is compared with existing methods on various biometric databases as shown in Table II. The template protection methods using fingerprint biometrics reported the GAR of 97% and 94% at 0.1% and 0% FAR, respectively [62], [58]. The discriminability of iris features proved to be better as the method of Talreja *et al.* reported 99.1% GAR at 0% FAR [40]. However, the iris patterns are taken obtrusively and are inconvenient for users. Therefore, the recognition performance of iris biometrics may deteriorate for real-time databases as in case of Kumar *et al.*, who reported 91% GAR at 0% FAR [63]. Most of the template protection methods tested on face biometrics use Multi-PIE database that is taken

TABLE II. PERFORMANCE COMPARISON WITH EXISTING METHODS OF TEMPLATE PROTECTION

| *Method* | *Dataset* | *GAR%@FAR%* |
|---|---|---|
| Nagar et al. [62] | FVC 2002 | 97.0@0.1 |
| Kumar et al. [63] | IITD iris | 91.0@0.0 |
| Talreja et al. [40] | WVU iris | 99.1@0.0 |
| Hybrid Approach [59] | Multi-PIE | 90.61@1.0 |
| BDA [60] | Multi-PIE | 96.38@1.0 |
| DeepCNN [61] | Multi-PIE | 96.53@0.0 |
| Wang & Hu [58] | FVC 2002 | 94.0@0.0 |
| **Our Method** | **VGGFace2** | **92.0@0.0** |
| **Our Method** | **MegaFace** | **98.5@0.0** |

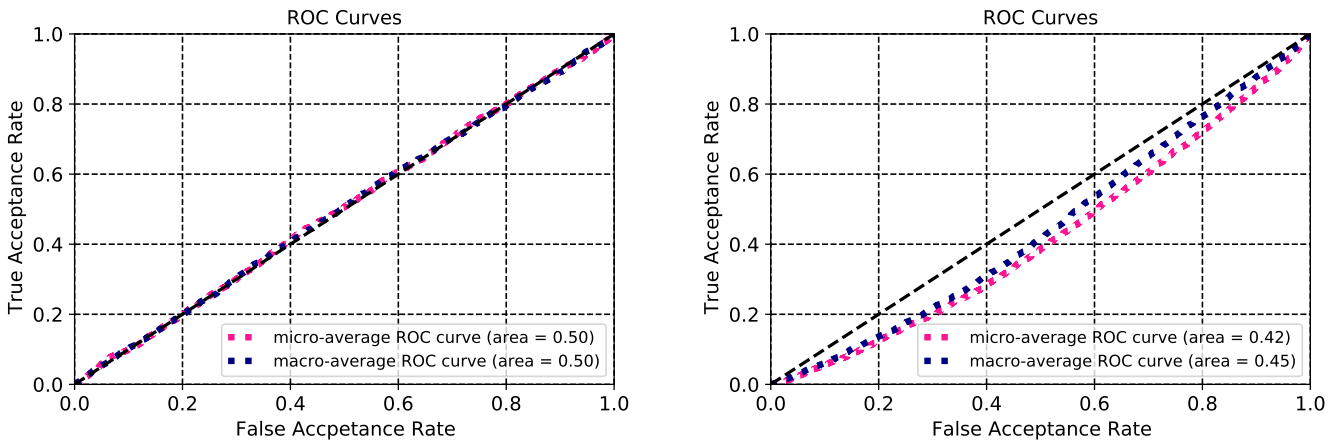


Fig. 5. ROC Curve for Birthday Attack on a) VGG and b) MegaFace Databases.

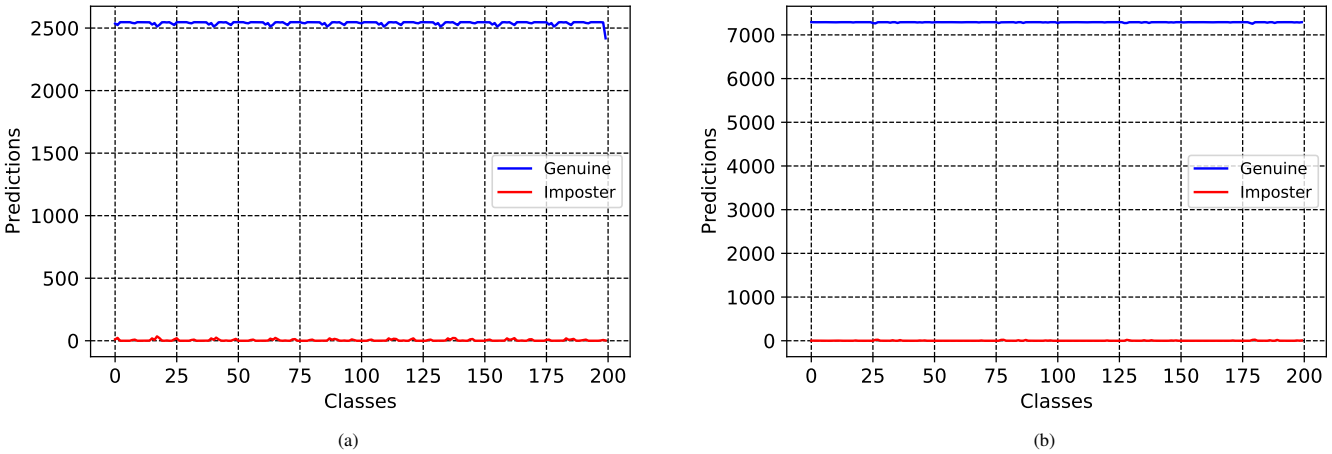


Fig. 6. Genuine Imposter Distribution for Birthday Attack on a) VGG and b) MegaFace Databases.

in constrained environment. The performance of proposed method is evaluated on both constrained and unconstrained databases. The proposed method reports 92% GAR at 0% FAR on VGGFace2 database that is taken in unconstrained environment. The performance of proposed method improves on MegaFace database. In comparison to other constrained environment databases, our method reports highest GAR of 98.5% at 0% FAR. Thus, the proposed method outperforms other existing methods on both constrained and unconstrained databases.

### *E. Security Analysis*

The security paradigm of the proposed ensemble of biometric template security is analyzed to avoid possible fraudulent attacks on the biometric system. We can consider following parameters to evaluate the robustness of the proposed template protection method.

- *User Impersonation:* The attacker may try to impersonate as a genuine user. The experimental results show that higher TAR is achieved at marginal FAR on both databases. For example, on the VGG2Face database 99% TAR is achieved at lower FAR of 1%. It can be further reduced without much loss in TAR. The false acceptance is further minimized while using the MegaFace database, as 100% TAR is achieved at 0.8% FAR. The proposed biometric system is to be set as to not allow any false acceptance *i.e.*, FAR of 0%, while maintaining the TAR of 93% and 97% on VGGFace2 and MegaFace database, respectively. Hence, there is less chance of template impersonation while using the unconstrained database. Finally, the false biometric attempts made by an intruder to breach the security of the system can be negligible.

- *Denial to Attackers:* Generally, in a biometric system the features of a query image are matched with the

templates stored in the database. An attacker may gain access to the templates of the gallery in such cases. In the proposed framework of PlexNet the gallery database is removed. The learning of PlexNet is enough to make a correct prediction without maintaining the template database. Therefore, there is hardly any possibility of attacks on the template database. The proposed method predicts the class label for a query image using a smart box *i.e.*, API. The API may be compromised by an attacker. It consists of weights and biases from different pre-trained models having millions of parameters per model. The access of image information from these parameters is almost impossible. Hence, the proposed ensemble ensures the security of biometric templates that are completely irrevocable.

To further strengthen our claims, we performed birthday attack to check the vulnerability of the prepared model against cross-referencing of the database. To achieve this, both the databases were cross referenced against each other. For example, the API prepared using VGG face dataset was fed the MegaFaceDataset and vice-versa. The result of this attack is shown in Fig. 5 and Fig. 6. The ROC curve is considered most accurate if it is close to the top left of the corner and then moves horizontally. Likewise, if the plot is closer to the diagonal, as shown in Fig. 5a and 5b, it shows that the probability of false identification is very low. The birthday attack is further analyzed using positive and negative predictions. In both the cases, the positive predictions tend to be near 0 or exact 0 while negative predictions were closer to 1, as shown in Fig. 6a and 6b. This further strengthens the claim that the proposed model has negligible false acceptance during an adversary attack.

## V. Conclusion and Future Scope

The deep neural networks have achieved tremendous performance in computer vision, pattern recognition and image analysis. These networks learn intrinsic patterns of data automatically without being programmed. The advantages of using deep neural networks such as CNNs are yet to be explored for the application of biometric template protection. The application of CNNs in biometric recognition has motivated us to utilize the potential for biometric template protection. It has shown that a single learning model may not perform better on complex databases due to class imbalance or data insufficiency. The class imbalance and data insufficiency may results in the problem of over-fitting and under-fitting, respectively. To overcome these issues, an ensemble has proved to be efficient in several state-of-the-art methods of biometric authentication. This paper has presented a detailed study on biometric template protection. It has been achieved through exclusion of templates from the database by exploiting the learning of deep neural networks. The exclusion of the template database requires a high performing network architecture, so an ensemble has designed.

The ensemble called 'PlexNet' is designed using deep neural networks. Two state-of-the-art CNN architectures *i.e.*, ResNet and DenseNet are chosen to form the PlexNet. The selection of these architectures is based on experimentation on a database of millions of images and their complementarity. The selected base models are trained separately using their pre-trained weights from ImageNet. The performance of PlexNet for biometric template protection has evaluated on two publicly available databases *i.e.*, VGGFace2 and MegaFace. It has achieved outstanding recognition results that outperform other state-of-the-art template protection mechanism using face biometrics [56].

The proposed PlexNet model laid the foundation for biometric template protection. An API has prepared that learnt base and fine-tuned models together. The API is acted as a smart box for the query image that has predicted the correct class without exposing the biometric features during training. The proposed template protection framework did not store templates in the gallery for any possible predictions by intruders. Therefore, proposed framework has made possible the exclusion of templates from gallery and performed predictions based on learning that is irrevocable.

## References

[1] A. Singh, R. Srivastva, Y. N. Singh, "Prevention of Payment Card Frauds using Biometrics", International Journal of Recent Technology and Engineering (IJRTE), 8 (3S), pp. 516-525, 2019.

[2] A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, 14 (1), pp. 4-20, 2004.

[3] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security", IEEE Transactions on Information Forensics and Security, 1 (2), pp. 125-143, 2006.

[4] Y. N. Singh and S. K. Singh, "A Taxonomy of Biometric System Vulnerabilities and Defenses", International Journal of Biometrics, 5 (2), pp. 137-159, 2013.

[5] Grottke M., Matias R. and Trivedi K.S., "The fundamentals of software aging", IEEE International Symposium on Software Reliability Engineering, pp.1-6, 2008.

[6] A. K. Jain, R. Bolle, and S. Pankanti, Eds., "Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers, Dordrecht, The Netherlands, 1999.

[7] R. Srivastva, A. Singh, Y. N. Singh, "PlexNet: A fast and robust ECG biometric system for human recognition", Information Sciences, 558, pp. 208-228, 2021.

[8] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges", Proc. of the IEEE, 92 (6), pp. 948-960, 2004.

[9] A. Cavoukian and A. Stoianov, "Biometric encryption: a positive-sum technology that achieves strong authentication, security and privacy", Tech. Rep., Office of the Information and Privacy Commissioner of Ontario, Toronto, Ontario, Canada, March 2007.

[10] A. Vetro and N. Memon, "Biometric system security", in Proc. of the 2nd International Conference on Biometrics, Seoul, South Korea, August 2007.

[11] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates", IEEE Transactions on pattern analysis and machine intelligence, 29 (4), pp. 561-572, 2007.

[12] A. Juels and M. Wattenberg. "A fuzzy commitment scheme", Proceedings of the 6th ACM conference on Computer and communications security, pp. 28-36. ACM, 1999.

[13] H. Lu, K. Martin, F. Bui, K. N. Plataniotis and D. Hatzinakos, "Face recognition with biometric encryption for privacy-enhancing self-exclusion", 2009 16th International Conference on Digital Signal Processing, Santorini-Hellas, pp. 1-8, 2009.

[14] P. Tuyls and J. Goseling, "Capacity and examples of template-protecting biometric authentication systems", In: Maltoni D., Jain A.K. (eds) Biometric Authentication. BioAW 2004. Lecture Notes in Computer Science, vol 3087. Springer, Berlin, Heidelberg, pp. 158-170, 2004.

[15] M. VanderVeen, T. Kevenaar, G. J. Schrijen, T. H. Akkermans, F. Zuo, "Face biometrics with renewable templates", in Proc. of SPIE: Security, Steganography, and Watermarking of Multimedia Contents, vol. 6072, 2006.

[16] K. Nandakumar, A. Jain, "Biometric template protection: bridging the performance gap between theory and practice", IEEE Signal Processing Magazine, 32 (5), 88-100, 2015.

[17] Y. Sutcu, Q. Li, N. Memon, "Protecting biometric templates with sketch: theory and practice", IEEE Transactions on Information Forensics and Security, 2 (3), pp. 503-512, 2007.

[18] Alex Krizhevsky,Ilya Sutskever,G E Hinton, "Imagenet Classificiation with Deep convolutional neural network", Communications of the ACM, 60 (6), May 2017.

[19] C. Rathgeb, A. Uhl and P. Wild, "Iris-biometrics: from segmentation to template security", S. Jajodia (ed.), Advances in Information Security, Springer, 2013.

[20] A. Juels and M. Sudan, "A fuzzy vault scheme. Designs, Codes and Cryptography", 38 (2), pp. 237-257, 2006.

[21] U. Uludag, S. Pankanti, A. K. Jain, "Fuzzy vault for fingerprints", in Proc. of 5th International Conference on Audio- and Video-Based Biometric Person Authentication, AVBPA 2005, Hilton Rye Town, NY, USA, 20-22, July 2005.

[22] K. Nandakumar, A. Jain, S. Pankanti, "Fingerprint-based fuzzy vault: implementation and performance", IEEE Transactions on Information Forensics and Security 2 (4), pp. 744-757, 2007.

[23] Dang, T. K., V. Q. P. Huynh, and Q. H. Truong, "A Hybrid Template Protection Approach using Secure Sketch and ANN for Strong Biometric Key Generation with Revocability Guarantee". The International Arab Journal of Information Technology (IAJIT), 15 (2), pp. 331-340, 2018.

[24] Y.-J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation", in Proc. of the IEEE International Conference on Multimedia and Expo (ICME '04), vol. 3, pp. 2203-2206, Taipei, Taiwan, June 2004.

[25] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data", Tech. Rep. 235, Cryptology ePrint Archive, February 2006.

[26] C. Vielhauer, R. Steinmetz, and A. Mayerhofer, "Biometric hash based on statistical features of online signatures", in Proc. of the International Conference on Pattern Recognition, vol. 1, pp. 123-126, Quebec, QC, Canada, August 2002.

[27] D. C. L. Ngo, A. B. J. Teoh, J. Hu, "Biometric Security", Cambridge Scholars Publishing, Newcastle upon Tyne, 2015.

[28] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs", IEEE Transactions on Pattern Analysis and Machine Intelligence, 28 (12), pp. 1892-1901, 2006.

[29] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition", Springer, Berlin, Germany, 2003.

[30] T. Connie, A. Teoh, M. Goh, D. Ngo, "Palmhashing: a novel approach for cancelable biometrics", Information Processing Letters, 93 (1), 1-5, 2005.

[31] A. Teoh, D. Ngo, "Biophasor: token supplemented cancellable biometrics", in 9th International Conference on Control, Automation, Robotics and Vision (ICARCV), pp. 1-5, 2006.

[32] Z. Jin, J. Y. Hwang, Y. Lai, S. Kim and A. B. J. Teoh, "Ranking-Based Locality Sensitive Hashing-Enabled Cancelable Biometrics: Index-of-Max Hashing," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 2, pp. 393-407, Feb. 2018.

[33] F. Y. Cheng, Y. P. Chi, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template", IEEE Transactions on Information Forensics and Security, 5 (1), pp. 103-117, 2010.

[34] N. K. Ratha, J. H. Connell, R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, 40 (3), pp. 614-634, 2001.

[35] T. Boult, "Robust distance measures for face-recognition supporting revocable biometric tokens", in 7th International Conference on Automatic Face and Gesture Recognition (FGR), pp. 560-566, 2006.

[36] H. Liu, D. Sun, K. Xiong, Z. Qiu, "A hybrid approach to protect palmprint templates". Scientific World Journal 2014, pp. 686-754, 2014.

[37] Y. Chin, T. Ong, A. Teoh, K. Goh, "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion". Information Fusion 18, pp. 161-174, 2014.

[38] Dang, T. K., V. Q. P. Huynh, and Q. H. Truong, "A Hybrid Template Protection Approach using Secure Sketch and ANN for Strong Biometric Key Generation with Revocability Guarantee", The International Arab Journal of Information Technology (IAJIT), 15 (2), pp. 331-340, 2018.

[39] A. Sardar, S. Umer, C. Pero and M. Nappi, "A Novel Cancelable FaceHashing Technique Based on Non-Invertible Transformation With Encryption and Decryption Template," in IEEE Access, vol. 8, pp. 105263-105277, 2020.

[40] V. Talreja, M. C. Valenti and N. M. Nasrabadi, "Deep Hashing for Secure Multimodal Biometrics," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1306-1321, 2021.

[41] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition", 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Las Vegas, NV, 2016.

[42] G. Huang, Z. Liu, L. van der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks", 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, pp. 2261-2269, 2017.

[43] Y. M. Glaser, "Densely Connected Convolutional Neural Networks for Natural Language Processing", Honors Theses 36, University of North Georgia, 2018.

[44] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition", 3rd International Conference on Learning Representations, ICLR 2015, San Diego, CA, USA, pp. 1-14, 2015.

[45] J. Deng, W. Dong, R. Socher, L.-J. Li, K. Li, and L. Fei-Fei, "ImageNet: A Large-Scale Hierarchical Image Database", in 2009 IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, pp. 248-255, 2009.

[46] L. Perez and J. Wang, "The Effectiveness of Data Augmentation in Image Classification using Deep Learning", ArXiv e-prints, 2017.

[47] Keras Applications, "https://keras.io/applications/", accessed 15th July 2020.

[48] Cavoukian A., Stoianov A, "Biometric Encryption", In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security". Springer, Boston, MA, 2011.

[49] A. Nagar and A. K. Jain, "On the security of non-invertible fingerprint template transforms", 2009 First IEEE International Workshop on Information Forensics and Security (WIFS), London, pp. 81-85, 2009.

[50] Caruana, Rich & Lawrence, Steve & Giles, C, "Overfitting in Neural Nets: Backpropagation, Conjugate Gradient, and Early Stopping", Advances in Neural Information Processing Systems. 13. pp. 402-408, 2000.

[51] Lin, Jianzhe & Wang, Qi & Ward, Rabab & Wang, Z.. (2018). "DT-LET: Deep Transfer Learning by Exploring where to Transfer". Neurocomputing, Vol 390, pp. 99-107, 2020.

[52] Ghaemi, R., Sulaiman, M. N., Ibrahim, H., & Mustapha, N., "A survey: Clustering ensembles techniques", World Academy of Science, Engineering and Technology, 50, pp. 636-645, 2009.

[53] Tan, Chuanqi & Sun, Fuchun & Kong, Tao & Zhang, Wenchang & Yang, Chao & Liu, Chunfang, "Survey on Deep Transfer Learning", 27th International Conference on Artificial Neural Networks, Rhodes, Proceedings, Part III., 2018.

[54] Yuan X, Xie L, Abouelenien M., "A regularized ensemble framework of deep learning for cancer detection from multi-class, imbalanced training data", Pattern Recognition, 77, pp. 160-172, 2018.

[55] Cao, Q. and Shen, L. and Xie, W. and Parkhi, O. M. and Zisserman,1. A., "VGGFace2: A dataset for recognising faces across pose and age", International Conference on Automatic Face and Gesture Recognition, 2018.

[56] R. Shyam and Y. N. Singh, "Recognizing Individuals from Unconstrained Facial Images", Intelligent Systems Technologies and Applications, Advances in Intelligent Systems and Computing, Springer, vol. 384, pp 383-392, 2015.

[57] Kemelmacher-Shlizerman, Ira and Seitz, Steven M and Miller, Daniel and Brossard, Evan, "The MegaFace benchmark: 1 million faces for recognition at scale", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 4873-4882, 2016.

[58] Song Wang, Jiankun Hu, "A blind system identification approach to cancelable fingerprint templates", Pattern Recognition, Vol. 54, pp. 14-22, 2016.

[59] Feng, Y. C., Yuen, P. C. and Jain A. K., "A hybrid approach for generating secure and discriminating face template", IEEE transactions on information forensics and security, 5(1), pp.103-117, 2010.

[60] Feng Y. C. and Yuen, P. C. "Binary discriminant analysis for generating binary face template", IEEE Transactions on Information Forensics and Security, 7(2): pp. 613-624, 2012.

[61] Jindal, A. K., Chalamala, S., and Jami, S. K., "Face Template Protection Using Deep Convolutional Neural Network", IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Salt Lake City, UT, USA, pp. 575-5758, 2018.

[62] A. Nagar, K. Nandakumar, A.K. Jain, "A hybrid biometric cryptosystem for securing fingerprint minutiae templates", Pattern Recogn. Lett. 31(8), 733–741 (2010)

[63] A. Kumar, A. Kumar, "A cell-array based multibiometric cryptosystem". IEEE Access 4, pp. 15–25 2016