Fingerprint liveness detection using deep learning

Zeynep İnel Özkiper, Zeynep Turgut, Tülin Atmaca, Muhammed Ali Aydin

Fingerprint Liveness Detection Using Deep Learning

1st Zeynep İnel Özkiper
Computer Programming
Halic University
Istanbul, Turkey
zeynepinel@halic.edu.tr

2nd Zeynep Turgut
Computer Engineering
Istanbul Medeniyet University
Istanbul, Turkey
zeynep.turgut@medeniyet.edu.tr

3rd Tulin Atmaca
Samovar Lab./IMT/Telecom SudParis
Institut Polytechnique de Paris
Evry, France
tulin.atmaca@telecom-sudparis.eu

4th Muhammed Ali Aydın
Computer Engineering
Istanbul University - Cerrahpasa
Istanbul, Turkey
aydinali@istanbul.edu.tr

***Abstract*— It has great importance to provide the highest accuracy from fingerprint identification and verification systems, which have a large number of biometric features. Fingerprint recognition systems are more widely utilized than other biometric feature recognition systems. For this reason, a fingerprint recognition system must be fast and reliable to realize the separation of the fake and live fingerprints and provide high accuracy. In this study fingerprint liveness detection system is presented using LivDet2015 dataset. SVM (Support Vector Machine), CNN (Convolutional Neural Network), CNN+SVM methods are used for classification and their performances are compared. Especially the classifying performance of CNN method is analyzed. Before the classification process is performed with SVM, edge enrichment, transformation and feature extraction steps are applied on images as preprocessing steps. The highest accuracy rate is obtained by using CNN - deep learning classifier.**

Keywords—liveness detection, deep learning, machine learning, fingerprint, cnn.

I. Introduction

Systems that identify people based on their physical or behavioral characteristics are called biometric systems. Biometric systems are widely used based on personal features such as fingerprints, face, iris, retina, hand geometry, signature and sound. In case of any crime, features such as hair, skin rash, saliva, blood traces and fingerprints or security cameras are used as evidence at the scene. Sometimes there may not be a security camera in the place where the crime is committed or a clear image cannot be obtained from the camera. Fingerprints are the most preferred features than DNA mappings because DNA mappings have high time requirements and cost more than fingerprint recognition systems. Fingerprint data, which has been used frequently since the 19th century in criminal identification systems, has been produced with different materials with technological developments. Data similar to fingerprints can be easily created using different items like gelatine, wood glue, etc. Making a distinction as to whether fingerprint data is real or fake will prevent frauds that can be made using fake fingerprints.

Motivation behind this study is to detect fake fingerprints by achieving high accuracy rates without analyzing natural properties of fingerprints. This study contributes to the literature utilizing detecting fake fingerprints by using a deep learning method: CNN (Convolutional Neural Network) and comparing its classification strength with SVM. Three different approaches are presented. In the first approach SVM technique is used. Before the classification process is performed with SVM, edge enrichment, transformation and feature extraction steps are applied on images as preprocess step. In the second approach, CNN method is used without applying any preprocessing step. In the third approach CNN + SVM hybrid method is utilized. In this approach SVM is implemented as a feature extractor, and CNN works as a classifier.

In Section II publications related to fingerprint liveness detection using various methods are briefly introduced. The theoretical background of the study is presented in Section III. In Section IV results are compared and discussed. Lastly conclusions of the study are given in Section V.

II. Related Work

Gao et al. [1] suggested using CNN (Convolutional Neural Network - Evolutionary Neural Network) for fingerprint recognition. They used original, simple and continuous time CNNs in their study. All images in their studies have 256 x 256 pixels. The algorithm which includes noise reduction and contrast enhancement, back enhancement, binarization and thinning preprocesses, reduces the high-frequency noise in an original gray level fingerprint, recovers the destroyed connection on the background and converts the original fingerprint image into a binary image. In the result, black lines contain all the features in the original image.

Bhattacharya and Mali [2] studied on the fingerprint recognition system with two types of matching methods: the identification that checks whether the fingerprint image belongs to a particular database and the verification that confirms that a particular person has the fingerprint. The recommended method does pixel-by-pixel mapping. According to this method, the image is cropped according to a certain point of the fingerprint image. They used the average gradient calculation to find the reference point, but they figured out that the gradient approach is not suitable for every fingerprint and needs other features for matching. They got the best result from the image with a block of 4x4 pixels. As a result, they emphasized that the reliability of the fingerprint recognition system depends on the sensitivity obtained in the detailing process.

Wang et al. [3] used autoencoder based on deep neural network for selecting fingerprint orientation area to classify fingerprint images. Fuzzy classifier based on Softmax regression model is used to increase the classification accuracy. They classified the NIST-DB4 database with three hidden layers and obtained 93.1% accuracy rate.

Darlow and Rosman [4] proposed the MENet network, which works with the method of extracting insignificant details using the deep convolutional neural network. The MENet consists of five convolutional layers have two fully connected layers with 1024 nodes and a softmax output layer. The Softmax normalization function is used to estimate the presence or absence of the detail point. ReLU activation function is used in all units except the output layer. MENet performed well, although not the best, with 14.2% loss compared to other commercial software compared (NIST, DP, SG, NT, GL). 80% of the FVC dataset is used for training and 20% for testing purposes. The authors explain the fingerprint recognition process, which includes fingerprint development, feature detection, and classification.

Yuan et al. [5] tried to distinguish real fingerprints from fake ones using the convolutional neural network (CNN). They use CNN because they are successful in pattern recognition, including deep learning-based feature extraction methods, self-learning ability, computer vision, and image classification. After using the convolution process for feature extraction, learned features based on CNN are fed with support vector machines (SVM) for classification. Principal component analysis (PCA) is applied to reduce the dimensions of the learned features between each convolution and pooling process. To measure the performance of the method, they used the LivDet 2011 dataset, which contains 16056 fingerprints in total, real and fake, and the LivDet 2013 data set consisting of 16853 fingerprints. The error rate of the method applied to the LivDet 2013 dataset yielded accuracy rates close to zero. But in the LivDet 2011 dataset, the classes with an error rate close to zero are less than livDet 2013.

Li et al. [6] proposed FingerNet, which uses deep convolutional neural network (CNN) as a fingerprint enhancement method. The coded part of FingerNet, which has three main parts, consists of the convolution part and the deconvolution part that performs the decoding and routes work that performs two decoding. The convolution part is used for removing fingerprint features. The deconvolution enhancement part is used to remove structured noise and improve fingerprints. Uses the multitasking learning strategy to guide the development process in the orientation part of the deconvolution. They used multitasking learning to improve performance. They tested FingerNet system with NIST SD27 database. Instead of using predefined image priorities, they used pixel-to-pixel direct learning with deep-learning end-to-end learning style.

Baştürk et al. [7] suggested using deep neural networks in fingerprint recognition. The structure of the deep neural network consists of two automatic encoders and one flexible thresholder classifier layers. They obtained the scales with the Gabor filter in the training of the network structure. They measured the test accuracy of the system as 98.31%. They performed the training on the graphic processor to shorten the duration.

Topcu and Erdoğan [8] offered GMM (Generalized Method of Moments) - SVM (Support Vector Machine) based solutions that can be used in secure fingerprint authentication systems. By transforming the property vector of GMM-SVM into a binary bit sequence, they accelerated fingerprint matching with distance calculation between binary vectors. In this study, they used the asymmetric locality sensitive hashing (ALSH) method that is sensitive to the asymmetric region. They evaluated the verification performance of the method used in the FVC2002 DB1A and FVC2002 DB2A databases and said that their approach to fingerprint authentication has a high accuracy and has advantages over existing fixed length detail representations.

Maheswari et al. [9] studied a convolutional neural network and dynamic differential annealing (CNN-DDA)-based spoofed fingerprint detection. In the related study CNN-DDA approach is proposed to analyze and evaluate the false or forged fingerprint concerning spoof forgery authentication system. Accuracy values are obtained from each datasets are 94.67%, 96.32% and 97.05%, respectively.

In this study, LivDet2015 dataset including live fingerprints collected from humans and fake fingerprints created with gelatin, latex, wood glue, ecoflex, body double and play dough is studied. By using support vector machines, deep learning - convolutional neural networks and a hybrid method: the convolutional neural network - support vector machine on the related dataset, fingerprint data -which are labeled as fake and live are classified so that a system that can prevent fingerprint fraud is created. The structure of the LivDet2015 dataset is examined and the machine learning methods most suitable for the data contained in the relevant dataset are selected; SVM and CNN methods are compared, and their performance analyzes realized. In this study, SVM technique and CNN technique are used to detect fake fingerprints. In order to perform the performance analysis of the CNN technique as a classifier, CNN and SVM techniques are also used in a hybrid form. SVM, CNN and CNN+SVM methods are used for detecting live fingerprints in LivDet2015 dataset which containes fake and real fingerprints.

III. THEORETICAL BACKGROUND

Since the quality of the image is important in the fingerprint recognition system, in order to improve the image, after image gathering, image preprocessing: image enhancement, transformation, feature extraction steps are applied on images respectively.

Fingerprints may classified using conventional classification algorithms [10]. Some stages are needed while using conventional classification algorithms. Related stages are seen in Fig.1. After gathering images for analyzing natural properities of the images, image preprocessing: image enhancement, transformation and feature extraction stages are used before classification while using SVM method.

Fig. 1: Image processing stages

In the study, the objective is to classify the fingerprints without analyzing the natural properties of the fingerprints during the preprocess stage.. CNN method is selected for achieving this goal. Image preprocessing steps are not realized while using CNN method.

SVM, CNN an a hybrid approach CNN + SVM are presented by combining SVM, CNN and both machine learning techniques to classify the fingerprint by using MATLAB. Hybrid approach is used for comparing the classifying performance of SVM and CNN. In hybrid approach CNN performs as a feature extractor, and CNN works as a classifier.

A. Image Gathering – LivDet2015

In this study, we aimed to distinguish fake fingerprints produced by fingerprints from living things. For this purpose, LivDet2015 dataset containing real and fake fingerprints was used. The related dataset was created in 2015 as a result of the competitions to create "Liveness Detection" datasets that were held at 2-year intervals. Competition for creating a dataset including fake and real fingerprints. Liveness detection refers determining real fingerprints in created datasets.

Liveness dataset is held at 2-year intervals [11] [12] [13] [14] [15]. In order to realize this study, LivDet2015, which is the newest dataset available for use, was preferred. In this study, training dataset in LivDet2015 dataset was used; training set is divided and some of the dataset is reserved for testing.70% of related dataset used for training and 30% of dataset used for testing.

LivDet2015 training set consists of two basic parts, real and fake fingerprints. Fake and real fingerprints are collected in four different categories, collected using four different devices: Green Bit, Biometrika, Digital Persona and Crossmatch. It refers to different fingerprint collection devices used in different categories. Ecoflex, body double, play dough, gelatine, latex and woodglue are used for fake fingerprints produced.

The fingerprint images in the LivDet2015 dataset were selected and edited before being classified in SVM, CNN and CNN + SVM algorithms. The dataset used in the study is included in Table 1 (Real Fingerprints: RF, Body Double: BD, Ecoflex: E, Play dough:P, Gelatine: G, WoodGlue: WG). Livdet2015 real and fake fingerprint image numbers are presented in Table 1. All classes except RF class, includes fake fingerprints which are generated using different materials. Hence Green Bit dataset includes 997 fake and 100 real fingerprints, Digital Persona includes 1000 fake and 1000 real fingerprins and Crossmatch includes 250 fake and 250 real fingerprints.

Table 1: Livdet2015 real and fake fingerprint image numbers.

Dataset	RF	BD	E	P	G	Latex	WG
Green Bit	997	-	250	-	250	250	250
Digital Persona	1000	-	250	-	250	250	250
Crossmatch	250	30	30	190	-	-	-

B. Image Enhancement – Canny Edge Detection Operator

The Canny edge detection operator was discovered in 1986 by John F. Canny. The Canny algorithm, which is used to detect various edges in the images, connects the strong and weak edges in the image. Comparing other edge detection methods, the algorithm bridging the strong and weak edges gives the best results in noisy images and is more successful [16].

In the Canny edge detection algorithm, firstly noise reduction is realized by using Gauss filter. Then, the sobel masks are applied to detect strong and weak edges, and the edge direction and gradient size of the pixels on the image are calculated. As a result of this edge detection algorithm, a binary image is obtained in which the white pixels are close to the real edges of the original image. The Canny operator creates continuity between adjacent pixels and creates a single pixel image. In Fig. 2 after applying the Canny algorithm of the fingerprint image, the edges of the image are determined.

Fig. 2: Fingerprint image after applying the canny algorithm

C. Transformation

Wavelet transform is a method which is used to analyze the data, performed by using wavelets with time-frequency analysis of a signal. The wavelet transform divides the signal into a set of functions as a standard in orthogonal modular spatial space with finite energy in the spatial space. Properties of the signal in the modular spatial domain are analyzed. Wavelet transform can analyze the function in modular spatial space and time domains with better local capacity of frequency and time. Results after transformation phase is seen in Fig.3 [17]. The image is reduced to four sub-pictures as approximate, horizontal, vertical and diagonal, respectively.

Fig. 3: Fingerprint transformation phase.

In the study, single level 2-D wavelet transform calculated and compression technique is used. Horizontal, vertical and diagonal matrices are calculated. The 2D wavelet transform function used is obtained by taking the tensor of one dimensional wavelet and scaling functions. With the proposed technique, the image is first divided into subbands, that is, divided into coefficients. These coefficients are then compared to a threshold value. The coefficients below the threshold are set to zero and the coefficients above the threshold value are compressed and coded.

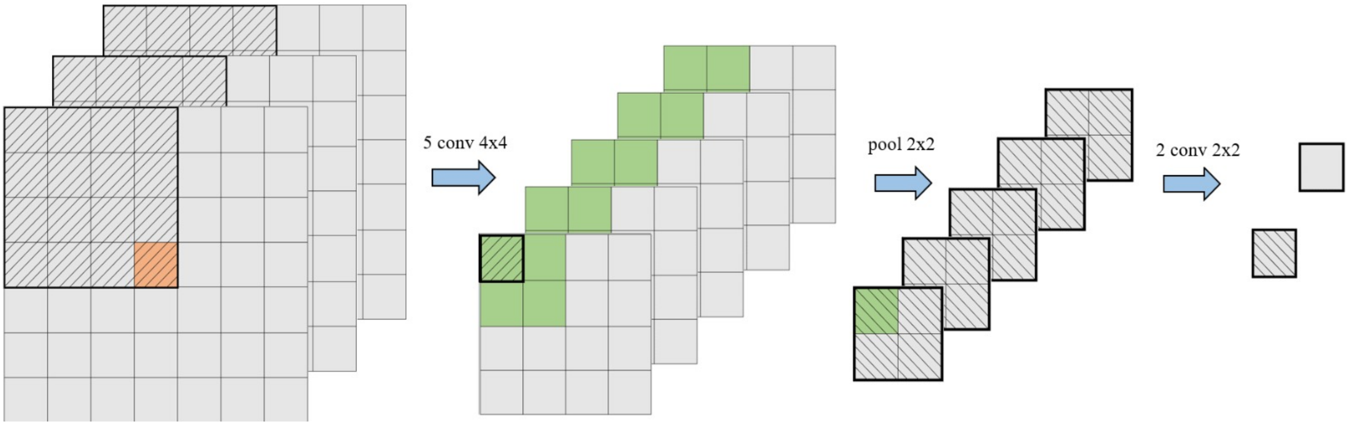

Fig 3. Convolutional network

D. Feature Extraction

In this study, entropy and variance calculations and feature extraction techniques are used to obtain distinctive features. Entropy specifies the grayscale image as a numerical sequence. Entropy is used when calculating the probability values of pixels in images. It is a statistical random measurement that can be used to characterize the input image, ie entropy is a quantitative measure of image information. If an image has more than two dimensions, it accepts the image as a multi-dimensional grayscale image. In this study, the probability of entropy and the distribution of the pixel values is calculated after the wavelet transform of the fingerprint image. The entropy filter can detect minor changes in the distribution of pixel values in the grayscale image.

In this methodology variance is a measure of how far a set of numbers spread. It is used to determine the edge position in image processing. Returns how far the numbers are from the calculated average and define the probability distribution of numbers. In fact, variance gives information about the propagation of pixel values. The variance image obtained is, an image of variances in the input or output images, which are squares of standard deviations. In this study, the variance of images are used as a quality measure of structural similarity between the two images.

E. Classification Step

Classification step includes comparing the fingerprint images according to the database. During the classification, two different techniques are used according to detail or pattern. In pattern matching, two images are compared and their similarities are examined. In the mapping based on detail, the location and direction of each point is checked. Detail based matching is more reliable against situations such as capturing the image of the fingerprint in different ways, changing skin condition. In this study, SVM technique, which requires qualification in the preprocess stage, and CNN machine learning technique, which performs quality extraction, are compared. In order to measure the classification performance of the SVM technique, the qualities obtained with the CNN classifier are also classified with SVM to examine the hybrid approach. Classification techniques are described below.

Support Vector Machines (SVM) is a supervised machine learning algorithm used for both classification and regression. SVM is generally used for classification determines how to divide points into two groups after displaying them in a coordinate plane in n dimensional space according to the characteristics of each item in the dataset. Binary SVM draws a boundary that best separates the two classes. Briefly, it is a plane that distinguishes between sets of objects with different class memberships. It is a method that classifies by creating hyperplanes in a multi-dimensional area that separates the states of different class labels. Accordingly, the classes are separated so as to allow an extreme plane to be formed between them. The equations for the classification process using the Support Vector Machine are included in Equation 1, Equation 2, and Equation 3. It shows n: data used for training purposes, c: number of classes to be matched, b: bias value, w: projection parameter in the related equations. Accordingly, the data in the class to be assigned is moved to positive values in order to assign any class, while other values are stacked to negative weight.

$$\min_{wj,bj} \quad \frac{1}{2}\left\|w_j\right\|_2^2 + C \sum_{i=1}^{n} \xi_i^j \qquad (1)$$

$$s.t. \quad w_j^T x_i + b_j \geq 1 - \xi_i^j, \; if \; y_i = j \qquad (2)$$

$$w_j^T x_i + b_j \le -1\,\xi_i^j,\ if\ y_i \ne j \quad (3)$$

$$\xi_i^{jk} \ge 0$$

Convolutional Neural Networks (CNNs) are like feed forward neural networks. They can model the nonlinear pooling layer and the fully connected layer. The outputs of each unit create 2-dimensional feature maps. Each feature map is created by applying a convolution (or pooling) filter to the entire image. A nonlinear activation function is always used after the pooling layer [17]. A simple convolutional neural network can be seen in Figure 4.11. In the picture provided, a series of convolution and pooling processes are carried out to classify the area shown in blue. Accordingly, the classification process is carried out by performing 5 4x4 convolution, 1 2x2 pooling and finally 1 2x2 convolution process. The structure of the convolutional network presented in Figure 3.

Convolution Layer: It consists of filters that can learn the parameters. Each filter is shifted across the width and height of the inlet volume, and each point is calculated by multiplying the value at the corresponding point in the filter. Each of the filters used in each convolution layer produces a 2-dimensional activation map. With this activation maps, depth is created and output volume is produced. Equation 4 shows m kernel width and height, h convolution output, x input, w convolution kernel [18].

$$h_{i,j} = \sum_{k=1}^{m} \sum_{l=1}^{m} w_{k,l} x_{i+k-1,j+l-1} \quad (4)$$

Pooling Layer: Also called sub-sampling layer. It is the same size as the filter used and subtracts the maximum number in each region where the filter applied to the input volume travels. This layer is greatly reduced by changing the spatial size, i.e. depth, of the input volume. Thus, the cost is reduced by reducing the amount of parameters or weights. Its mathematical formula is given in Equation 5 (Ganegedana [18]). Let be x input, h convolution output:

$$h_{i,j} = \{x_{i+k-1,j+l-1} \forall 1 \le k \le m \; and \; 1 \le l \le m \quad (5)$$

Fully Linked Layer: This layer takes the input and creates a vector with a class number dimension. The probability of the input for the different classes is calculated by looking at the high-level properties that are most strongly connected to a particular class and have specific weights.

It is often used in image recognition because CNN makes accurate predictions on images. Although CNN has a small and inexpensive architecture compared to standard feed forward neural networks, it requires a lot of computation and large labeled data set in its education.

The CNN structure used in the study consists of 3x3 convolution layers and 8x8, 16x16, 32x32 filters are used respectively. The ReLu (Rectified Linear Unit) activation function was used after each convolution layer. ReLu layer makes negative values in input data zero. It is expressed mathematically in Equation 6. The maximum pooling layer is 2x2 in size and the range is 2.

relationship between input and output data. Convolutional Neural Networks is an improved version of artificial neural networks and they especially work on images. Its layers have three-dimensional neurons, width, height and depth. Three main layers are used in the convolutional neural networks architecture. These layers are; the convolution layer, the

$$f(x) = \begin{cases} 0, x < 0 \\ x, x \ge 0 \end{cases} \quad (6)$$

In this study, false fingerprints were detected from fingerprint images by using two controlled classification techniques, CNN and SVM. While performing the convolutional neural network classification task, it also performs the feature extraction. In this hybrid model, CNN works as a trainable feature extractor and works as a SVM recognizable classifier. It is an important success factor in feature extraction recognition systems. The output value of the CNN network is considered a property for the SVM classifier. The CNN network is trained for several periods, and then the SVM classifier replaces the output layer. SVM takes the output layer of the CNN network as the feature vector and performs the classification process. The purpose of the CNN classifier here is to automatically extract the distinctive features of the input image.

F. Performance Metrics

The performance analysis of the machine learning classifiers used was evaluated by analyzing the metrics in the confusion matrix. In Table 2, the figure explaining the confusion matrix is given.

Table 2: Confusion matrix

Predicted \ Actual	Positive	Negative
Positive	**TP**	**FP**
Negative	**FN**	**TN**

For a biometric identification system based on detection fake fingerprints:

- True Positive (TP): The case where the fake fingerprint is classified as fake.
- False Positive (FP): The case where the live fingerprint is classified as fake.
- True Negative (TN): The case where live fingerprints are classified as live.
- False Negative (FN): The case where fake fingerprints are classified as live.

Using metrics in confusion matrix, precision, recall (sensitivity), accuracy, specificity, F1 score, Matthews correlation coeffient of SVM, CNN and hybrid model CNN and SVM) and kappa values are calculated. Related values:

- Precision: It enables to measure what percentage of the data detected as false fingerprints is false fingerprints. Precision calculation formula is given in Equation 7.

$$Precision = \frac{TP}{TP + FP} \tag{7}$$

- Sensitivity: It is the criterion that enables to find the rate of successful detections performed as false fingerprints. Recall calculation formula is given in Equation 8.

$$Recall - \ Sensitivity = \frac{TP}{TP + FN} \tag{8}$$

- Accuracy: Indicates how many percent of all values are classified according to the class to which they belong. The equation calculation formula is given in Equation 9.

$$Precision = \frac{TP + TN}{TP + TN + FP + FN} \tag{9}$$

- Specificity: It is the criterion that shows what percentage of the values stated to belong to the wrong class are classified as wrong. The specificity calculation formula is given in Equation 10.

$$Specificity = \frac{TN}{TN + FP} \tag{10}$$

- F1 Score : It is the harmonic average of precision and sensitivity. F1 score calculation formula is given in Equation 11.

$$F1\ Score = \frac{2\ (Precision+Sensitivity)}{(Precision+Sensitivity)} \tag{11}$$

- Matthews Correlation Coefficient (MCC): Used as a measure of the quality of binary classifications in machine learning. MCC returns values between -1 and +1. The result means that the forecast is good as you get closer to +1. MCC calculation formula is given in Equation 12.

$$MCC = \frac{TP * TN - FP * FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \tag{12}$$

- Cohen's Kappa: Cohen's Kappa model was first used in social sciences, biology and medical sciences. Its main purpose is to measure the degree of agreement or disagreement of two or more people who observe the same event. Then, expert systems started to be used in the fields of machine learning and data mining. It measures the degree of agreement between the predictions and reality of the model used [19]. It is a measure that determines the accuracy and reality of the result obtained from the confusion matrix. Cohen's Kappa model predicts the degree of agreement between the two models. Cohen's Kappa coefficient takes a value between [-1, 1]. The higher the Kappa value, the better the accuracy means. The equation calculation formula is given in Equation 13.

$$CKappa = \frac{\frac{(TP + TN)}{(TP + TN + FP + FN)} - \left[\frac{(TN + FP)(TN + FN) + (FN + TP)(FP + TP)}{(TP + TN + FP + FN)^2}\right]}{1 - \left[\frac{(TN + FP)(TN + FN) + (FN + TP)(FP + TP)}{(TP + TN + FP + FN)^2}\right]} \tag{13}$$

IV. RESULTS

The results obtained by using SVM method for classifying fingerprints by classifying fingerprints are presented in Table 3. When the accuracy value is taken into consideration, it is seen that the highest accuracy rate is reached on the Crossmatch dataset with 51.45%. Accuracy rates obtained in three data sets are released in the range of 48% - 51% when using the SVM classifier. It is seen that SVM classifier does not show a strong distinction in the classification process.

Table 3: Results obtained by using SVM

Dataset	Accuracy((%)(%)	Precision(%)	Recal (%)	Specificity (%)	F1 Score (%)	Matthews (%)	Kappa (%)
Green Bit	49.35	49.31	46.45	52.25	47.84	01.30	01.28
Digital Persona	47.58	47.78	52.20	42.95	49.90	04.87	04.62
Crossmatch	**51.45**	51.02	72.31	30.59	59.83	03.19	02.90

The results obtained using the CNN method for classifying fingerprints by classifying the fingerprints are included in Table 4. Considering the obtained accuracy value, it is seen that the highest accuracy rate was reached on the Green Bit dataset with 98.16%. When the CNN method is used for qualification and classification, it is seen that the accuracy rates range between 86% and 98% in three data sets. It is seen that CNN classifier shows a strong and acceptable classification performance compared to SVM classifier.

Table 4: Results obtained by using CNN

Dataset	Accuracy (%)	Precision(%)	Recal (%)	Specificity (%)	F1 Score (%)	Matthews (%)	Kappa (%)
Green Bit	**98.16**	99.32	97.00	99.33	98.15	96.35	96.33
Digital Persona	**85.67**	85.43	86.00	85.33	85.71	71.33	71.33
Crossmatch	**90.00**	91.67	88.00	92.00	89.80	80.06	80.00

The results obtained by using CNN + SVM method for classifying fingerprints by classifying fingerprints are included in Table 5. When the accuracy value is taken into consideration, it is seen that the highest accuracy rate is reached on the Crossmatch dataset with 85.33%. When the results of the classification methods are compared it is seen that CNN+SVM approach does not present the highest accuracy rate. As a classifier, the CNN method obtained the highest accuracy rate due to its adaptive learning ability.

Table 5: Results obtained by using CNN+SVM

Dataset	Accuracy (%)	Precision(%)	Recal (%)	Specificity (%)	F1 Score (%)	Matthews (%)	Kappa (%)
Green Bit	61.00	92.28	24.00	97.99	38.09	32.70	21.99
Digital Persona	84.50	85.81	82.67	86.33	84.21	69.05	69.00
Crossmatch	**85.33**	88.41	81.33	89.33	84.72	70.89	70.67

V. CONCLUSION

In the study, we aimed to evalute classification performance of CNN method on fingerprint liveness detection. For this purpose the results obtained using CNN method is compared with SVM and CNN+SVM approaches. Classification are realized on LivDet2015 dataset containing real and fake fingerprints. In the classification process performed with SVM, preprocess stage is realized. In CNN+SVM approach CNN is used as a feature extractor and SVM is used as a classifier. The CNN method achieved the highest accuracy in all aspects. CNN method provides 98.16% accuracy rate in GreenBit, 85.67% accuracy rate in Digital Persona, and 90.00% accuracy rate in Crossmatch dataset.In future studies, the CNN technique and classification ability will be compared with other machine learning and deep learning methods.

REFERENCES

[1] Gao, Q., Forster, P., Mobus, K. R., & Moschytz, G. S. (2001, May). Fingerprint recognition using CNNs: Fingerprint preprocessing. In ISCAS 2001. The 2001 IEEE International Symposium on Circuits and Systems (Cat. No. 01CH37196) (Vol. 3, pp. 433-436).

[2] Bhattacharya, S., & Mali, K. (2011). Fingerprint recognition using minutiae extraction method. Proc. of International Conferance on Emerging Technologies (ICET-2011): International Journal of Electrical Engineering and Embedded Systems, 0975-4830.

[3] Wang, R., Han, C., Wu, Y., & Guo, T. , 2014, Fingerprint classification based on depth neural network. arXiv preprint arXiv:1409.5188.

[4] Darlow, L. N., & Rosman, B. 2017, October. Fingerprint minutiae extraction using deep learning. In 2017 IEEE International Joint Conference on Biometrics (IJCB) (pp. 22-30).

[5] Yuan, C., Li, X., Wu, Q. J., Li, J., & Sun, X. 2017 . Fingerprint liveness detection from different fingerprint materials using convolutional neural network and principal component analysis. Computers, Materials & Continua,voli 53(3),pp. 357-371.

[6] Li, J., Feng, J., & Kuo, C. C. J. 2018. Deep convolutional neural network for latent fingerprint enhancement. Signal Processing: Image Communication, vol. 60 pp., 52-63.

[7] A. Baştürk, N. Sarikaya Baştürk, and O. Qurbanov, "Fingerprint recognition by deep neural networks and fingercodes," in 26th IEEE Signal Processing and Communications Applications Conference, SIU 2018, Jul. 2018, pp. 1–4, doi: 10.1109/SIU.2018.8404577.

[8] B. Topcu and H. Erdogan, "Fixed-length asymmetric binary hashing for fingerprint verification through GMM-SVM based representations," Pattern Recognit., vol. 88, pp. 409–420, Apr. 2019, doi: 10.1016/j.patcog.2018.11.029.

[9] Maheswari, B. Uma, M. P. Rajakumar, and J. Ramya. "Dynamic differential annealing-based anti-spoofing model for fingerprint detection using CNN." Neural Computing and Applications 34.11 (2022): 8617-8633.

[10] P. G. Patil, "A Survey on Fingerprint Identification Techniques," SJ Impact Factor 6, vol. 887, 2018, doi: 10.22214/ijraset.2018.1267.

[11] P. Foggia, C. Sansone, and M. Vento, "First International Fingerprint Liveness Detection Competition-LivDet 2009 *," 2009. Accessed: Jun. 28, 2020. [Online]. Available: http://prag.diee.unica.it/.

[12] D. Yambay, L. Ghiani, P. Denti, G. L. Marcialis, F. Roli, and S. Schuckers, "LivDet 2011 - Fingerprint liveness detection competition 2011," in Proceedings - 2012 5th IAPR International Conference on Biometrics, ICB 2012, pp. 208–215, doi: 10.1109/ICB.2012.6199810.

[13] Ghiani, L., Yambay, D., Mura, V., Tocco, S., Marcialis, G. L., Roli, F., & Schuckcrs, S. (2013, June). Livdet 2013 fingerprint liveness detection competition 2013. In 2013 IEEE international conference on biometrics (ICB) (pp. 1-6).

[14] Ghiani, L., Yambay, D. A., Mura, V., Marcialis, G. L., Roli, F., & Schuckers, S. A. (2017). Review of the fingerprint liveness detection (LivDet) competition series: 2009 to 2015. Image and Vision Computing, vol 58, pp. 110-128.

[15] V. Mura, L. Ghiani, G. L. Marcialis, F. Roli, D. A. Yambay and S. A. Schuckers, "LivDet 2015 fingerprint liveness detection competition 2015," 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2015, pp. 1-6, doi: 10.1109/BTAS.2015.7358776.

[16] A. Jagadeesan and K. Duraiswamy, "Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris." Accessed: Jun. 28, 2020. [Online]. Available: http://sites.google.com/site/ijcsis/.

[17] Pinheiro, P., & Collobert, R. (2014, January). Recurrent convolutional neural networks for scene labeling. In International conference on machine learning (pp. 82-90). PMLR.

[18] "Intuitive Guide to Convolution Neural Networks - Towards Data Science." https://towardsdatascience.com/light-on-math-machine-learning-intuitive-guide-to-convolution-neural-networks-e3f054dd5daa (accessed Jun. 28, 2020).

[19] A. Ben-David, "Comparison of classification accuracy using Cohen's Weighted Kappa," Expert Syst. Appl., vol. 34, no. 2, pp. 825–8