6-2021

Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities

Ahmed Sedik

Lo'ai A. Tawalbeh

Mohamed Hammad

Ahmed A. Abd El-Latif

Ghada M. El-Banby

See next page for additional authors

Authors

Ahmed Sedik, Lo'ai A. Tawalbeh, Mohamed Hammad, Ahmed A. Abd El-Latif, Ghada M. El-Banby, Ashref A.M. Khalaf, Fathi E. Abd El-Samie, and Abdullah M. Iliyasu

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 23, 2021, accepted June 5, 2021, date of publication June 10, 2021, date of current version July 12, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3088341

Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities

AHMED SEDIK[1], LO'AI TAWALBEH[2], (Senior Member, IEEE), MOHAMED HAMMAD[3], AHMED A. ABD EL-LATIF[4], (Senior Member, IEEE), GHADA M. EL-BANBY[5], ASHRAF A. M. KHALAF[6], FATHI E. ABD EL-SAMIE[7,8], AND ABDULLAH M. ILIYASU[9], (Senior Member, IEEE)

[1]Department of the Robotics and Intelligent Machines, Faculty of Artificial Intelligence, Kafrelsheikh University, Kafr El-Sheikh 12345, Egypt
[2]Cyber Security Research Centre, Department of Computing and Cybersecurity, Texas A&M University at San Antonio, San Antonio, TX 78224, USA
[3]Faculty of Computers and Information, Menoufia University, Shebin El-Kom 32511, Egypt
[4]Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Kom 32511, Egypt
[5]Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[6]Department of Electrical Engineering, Faculty of Engineering, Minia University, Minya 61111, Egypt
[7]Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt
[8]Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh 21974, Saudi Arabia
[9]Electrical Engineering Department, College of Engineering, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia

Corresponding authors: Lóai Tawalbeh (ltawalbeh@tamusa.edu) and Abdullah M. Iliyasu (ailiyasu@psau.edu.sa)

This work was supported in part by the Texas A&M System Chancellor Research Initiative (CRI) Grant awarded to Texas A&M University-San Antonio, TX, USA, and in part by the Prince Sattam Bin Abdulaziz University, Saudi Arabia, through the Deanship for Scientific Research funding for the Advanced Computational Intelligence and Intelligent Systems Engineering (ACIISE) Research Group, under Project 2020/01/12173.

ABSTRACT Smart cities and their applications have become attractive research fields birthing numerous technologies. Fifth generation (5G) networks are important components of smart cities, where intelligent access control is deployed for identity authentication, online banking, and cyber security. To assure secure transactions and to protect user's identities against cybersecurity threats, strong authentication techniques should be used. The prevalence of biometrics, such as fingerprints, in authentication and identification makes the need to safeguard them important across different areas of smart applications. Our study presents a system to detect alterations to biometric modalities to discriminate pristine, adulterated, and fake biometrics in 5G-based smart cities. Specifically, we use deep learning models based on convolutional neural networks (CNN) and a hybrid model that combines CNN with convolutional long-short term memory (ConvLSTM) to compute a three-tier probability that a biometric has been tempered. Simulation-based experiments indicate that the alteration detection accuracy matches those recorded in advanced methods with superior performance in terms of detecting central rotation alteration to fingerprints. This makes the proposed system a veritable solution for different biometric authentication applications in secure smart cities.

INDEX TERMS Deep learning, cyber threats, biometric alteration detection, cybersecurity, 5G network, smart city, authentication.

I. INTRODUCTION

Use of human biometrics in identity authentication is an area of interest for researchers from different backgrounds. Moreover, the identity of a person can be authenticated via different biometrics such as finger vein, face, fingerprint, and iris. Human identification is deployed in several applications such as access control, cyber security, and blockchains. Furthermore, owing to their uniqueness and animateness, more recently, the human biometrics are replacing passwords in several applications. For example, smart phones use the iris and fingerprint to be the password to access the device. Additionally, some financial organisations like Paneer have provided mobile applications for money transfer via the use

The associate editor coordinating the review of this manuscript and approving it for publication was Zahid Akhtar.

of fingerprints for the client authentication. Furthermore, the advent of online banking and its pervasiveness have led to increases in attempts to hack bank accounts via password spoofing as well as efforts to alter the biometric of the person. As the most common biometric used in person identification, verification and other cyber security applications, fingerprints are frequently targeted by criminals. Consequently, it is important to determine whether the integrity of such biometric data has been impugned.

In this regard, various studies for authentication detection prior to recognition of biometrics have been undertaken. Among them, Gad *et al.* [1] proposed a unimodal recognition methodology based on iris as well as multi-biometric scenarios. They proposed new modalities in both segmentation and feature extraction phases. In the segmentation phase, they proposed a masking technique for localisation and two modalities, (delta mean, and multi-algorithm mean) which they validated using CASIA v.1, CASIA v.4 and UBIRIS v.1. In [2], Wang *et al.* proposed an iris recognition technique based on Navier-Stokes (NS) equation with 1D Gabor filter used to construct the feature vector. They reported implementing their proposed technique using iris images exposed to varying levels of noise. Their experiments validated the techniques capability to accomplish person recognition despite the iris biometric being exposed to different noise conditions.

Other areas of use of iris recognition are in person authentication and identity verification. For example, in [3], Gad *et al.* replaced the traditional use of username and password with the iris as a unimodal biometric trait. The feature extraction stage of their proposed scheme utilises the Delta Mean (DM) and Multi-Algorithm Mean (MAM) that is followed by a feature reduction process to guarantee good performance. The scheme also has a classification stage that is undertaken using a Euclidian Distance (ED) classifier.

Similarly, authentication and identification suing finger vein have also been proposed. In [4], Peng *et al.* proposed a finger vein recognition method using a combination of Gabor wavelet and Local Binary Patterns (LBPs) with a Block-based Linear Discriminant Analysis (BLDA) for the task of feature reduction. Another finger vein recognition approach based on image quality enhancement was proposed by Peng *et al.* [5]. They used a Region of Interest (ROI) methodology for finger vein segmentation. Furthermore, the finger vein method was deployed for authentication in [6]. Specifically, Gabor filter was used to select parameters in eight orientations of the finger vein network, whose patterns are extracted using two distinct orientations. For their contribution in [7], Peng et al proposed a multi-biometric authentication system based on variations of fingerprints including finger knuckle, shape, vein as well as the original fingerprint of a certain person. A score-level fusion modality based on triangular norm on these fingerprints is then used to generate a single image representing the person's identity. Finally, they validated their system on a merged dataset.

Face biometric is involved in the face recognition process in several applications. In one such application in [8], a fusion process is performed using Multiscale Complex Fusion for Gabor Jet Descriptor (MCFGJD). The main idea of this work is to extract the features from the images using the Gabor descriptors generated from some block-wise statistics of the image including mean and standard deviation, which are generated from the magnitude, phase, real and imaginary parts of Gabor coefficients. After that, a feature reduction process is carried out on the extracted features using Linear Discriminant Analysis (LDA) algorithm. Finally, both thermal and visual images are fused.

Another research trend in biometric-based human identification involves a combination of two or more biometrics to improve security and authorisation. For example, the work in [9] presented a human identification system based on both thermal and visible face images as well as iris. This work depends on 1D Log-Gabor filter to generate a single feature vector from the dual iris codes. In addition, complex Gabor Jet descriptors are extracted from the thermal and visible face images to enhance the representation of their features. Furthermore, an image fusion technique is used to combine all biometrics. In [9], an Aczel-Alsina triangular norm (AA t-norm) technique was used for image fusion. In this way, the system can be used in both identification and authentication applications.

Meanwhile, the potency of Deep Learning Models (DLMs) has led to its deployment in a wide range of applications comprising medical image diagnosis [10]–[12], forgery detection [13], etc. Our proposed system uses a convolutional neural network (CNN) and a hybrid structure that combines CNN with convolutional long-short term memory (ConvLSTM) as DLMs for the detection of different levels of alteration in biometrics that are employed for person identification.

The remainder of this study is organised as follows. The outlines of our proposed system are presented in the next section (i.e., Section II), and the foundations of the proposed DLMs are discussed in latter parts of the same section. Experimental validation of our system as an effective platform for detection of alterations in biometric data is reported with discussions in Section III and IV, respectively.

II. PROPOSED FRAMEWORK AND DEEP LEARNING MODELS (DLMS)

We envision the deployment of our system as part of applications in a typical smart city, such as online banking platforms that are important for financial inclusion like electronic wallets. Like many of the emerging technologies, our system seeks to replace traditional username and password credentials with unique biometric traits of individuals. Despite enhancing secure access and authentication of users, biometrics are susceptible to the unrelenting efforts of criminals, such as spoofing to alter the biometrics. Therefore, it is necessary to discriminate between pristine (i.e., original) and altered biometrics such as fingerprints.

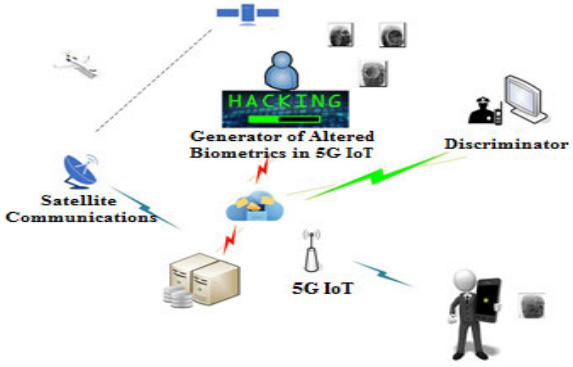

FIGURE 1. Conceptual framework in 5G smart city scenario.

Figure 1 presents an overview of the conceptual platform we envisage for our proposed framework. Its implementation presupposes a client using his mobile device for online banking applications, where the client's fingerprint biometric is used for authentication and verification in financial transactions. In their illicit effort to violate such systems, criminals alter the biometric data which could be deemed at one of three levels (easy, medium, and hard).

This makes efforts to discriminate pristine and altered biometric modalities crucial for financial transactions in smart cities and Internet-of-Things (IoT) platforms. Developing a deep learning framework to accomplish this task is the main objective of our study. Details of our proposed system are presented in the remainder of this section.

Deep Learning Models (DLMs) depend on multiple layers to progressively extract higher-level features from unstructured data. Its use in our proposed biometric alteration detecting system is accomplished via three stages as illustrated in Figure 2. In the first stage, a pre-processing procedure is performed on the input images to unify their sizes and convert them into tensors suitable for DLM processing. In the second (i.e., extraction) stage, the features from the images are transformed using a hierarchy of convolutional (CNV), Convolutional Long Short-Term Memory (ConvLSTM), pooling, Global Average Pooling (GAP) and decision making (dense) layers. Additionally, activation functions, such as the Rectifier Linear Unit (ReLU) and SoftMax functions are used to evaluate the output of each layer.

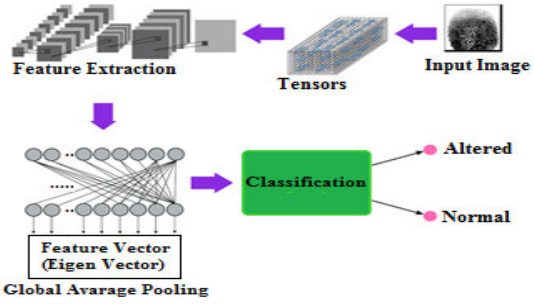

FIGURE 2. Proposed framework stages.

This study presents two DLMs. The first model is based a CNN consisting of three CNV layers followed by three pooling layers. This sequence of convolutional and pooling layers is required to extract the features from the input image tensors. Furthermore, the extracted feature map of each layer serves as input to an activation function to obtain the output of this layer. The activation function of each convolutional layer is the ReLU activation function, whose positive values are obtained with the same values, while the negative values are set to be zero at the output of the activation function as defined in Equation (1).

$$f(x) = \max(0, x) \tag{1}$$

Another feature extraction process tailored towards feature reduction is carried out by pooling layers. In this regard, there are two main types of pooling process. The first type, the Max pooling, is required to extract the maximum value of each block, whereas the second type, i.e., the average pooling, extracts the average value of each block in the feature map as depicted in Figure 3.

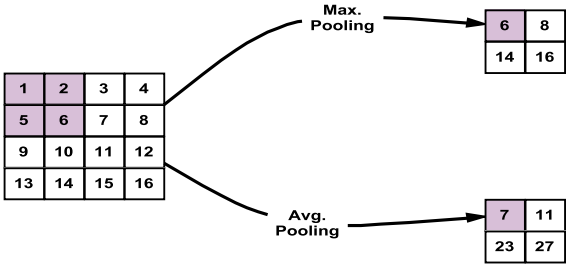

FIGURE 3. Illustration of Max and Avg. pooling (figure adapted from [12]).

The architecture of the CNN DLM in Figure 4 outlines a data flow, where input layers are unified into a $224 \times 224 \times 3$-dimensional input. The number and type of filters used determine the dimensions of the output feature map. For example, a model whose first convolutional layer has 16 filters and a stride of 2 would produce a $222 \times 222 \times 16$ output feature map. The second model utilised in our study consists of a ConvLSTM layer followed by two convolutional layers each of which is followed by a pooling layer for feature reduction. The architecture and data flow of this model is presented in Figure 5. Additionally, as depicted in Figure 4, the shape of the output feature map of the pooling layer is reduced in two dimensions only.

The Long Short-Term Memory (LSTM) is a special case of the artificial Recurrent Neural Networks (RNNs), which like the standard RNN, is stable and reliable for long-range dependencies [12]. Despite this, the LSTM is impeded by redundancy of spatial data. The ConvLSTM augment this shortcoming by replacing fully-connected layers in the LSTM with convolutional layers [12]. In this structure, ConvLSTM evaluates the same functionality of LSTM in 2D images [13]. Like LSTM, in ConvLSTM, the current state depends on all previous states as depicted in Figure 5 [12] and formulated in Equations (2) to (6).

Consequently, it can be inferred that if states are viewed as they would in the hidden representations of moving objects,

then the larger transitional kernel of a ConvLSTM should be capable of capturing faster motions [12]–[18]. Furthermore, ConvLSTM has the ability to encode the spatio-temporal information in its memory cells. To ensure that the states have the same dimensions as the inputs, padding is needed before applying the convolution operation. Furthermore, all states are initialised to zero before the first input, which corresponds to the so-called total ignorance of the future [12].

III. SIMULATION EXPERIMENTS AND RESULTS

This section presents outcomes of extensive simulation-based experiments undertaken to prove the efficiency of our proposed system in detecting alterations to fingerprint biometrics employed across different applications for person identification and verification.

We begin with an overview of the dataset used in the experiments; definitions of metrics employed for our quantitative validation of the proposed system as basis for comparisons with state-of-the-art techniques obtained from similar studies.

$$i_t = \sigma(W_{xi} * X_t + W_{hi} H_{t-1} + W_{ci} \circ C_{t-1} + b_i) \quad (2)$$

$$f_t = \sigma(W_{xf} * X_t + W_{hf} H_{t-1} + W_{cf} \circ C_{t-1} + b_f) \quad (3)$$

$$C_t = f_t \circ C_{t-1} + i_t \circ \tanh(W_{xc} * X_t + W_{hc} H_{t-1} + b_c) \quad (4)$$

$$O_t = \sigma(W_{xo} * X_t + W_{ho} H_{t-1} + W_{co} \circ C_t + b_o) \quad (5)$$

$$H_t = O_t \circ \tanh(C_t) \quad (6)$$

where:

i_t: The input gate.
C_{t-1}: The status at the previous cell (it is hidden).
f_t: The forget gate.
H_t: The final state of the latest state.
O_t: The output gate.

A. DATASET DESCRIPTION

The simulation experiments are carried using the Sokoto Coventry Fingerprint (SOCOFing) dataset [18]. SOCOFing dataset includes 6,000 fingerprint images from 600 persons, i.e., 10 fingerprints for each person. In addition, SOCOFing dataset includes three different alteration methodologies: obliteration, central rotation, and z-cut. Each alteration method consists of 15,000 altered images. Therefore, SOCOFing dataset consists of 50,000 images for both pristine and altered fingerprint images. Figure 6 shows samples of the fingerprints for a certain person.

B. EVALUATION METRICS

Our proposed system is evaluated using standard metrics as employed in recent and established studies. The equation matrix [12] in Figure 7 summarises definitions for specificity, accuracy, Positive Predictive Value (PPV), Negative Predictive Value (NPV), F1 score and Mathew's Correlation Coefficient (MCC).

Based on standard definitions, True Positive (TP) is the number of tampered images that were truly detected as tampered images, True Negative (TN) is the number of original images that were truly detected as original images, False Positive (FP) is the number of original images that were falsely detected as tampered images, and False Negative (FN) is the number of tampered images that were falsely detected as original images.

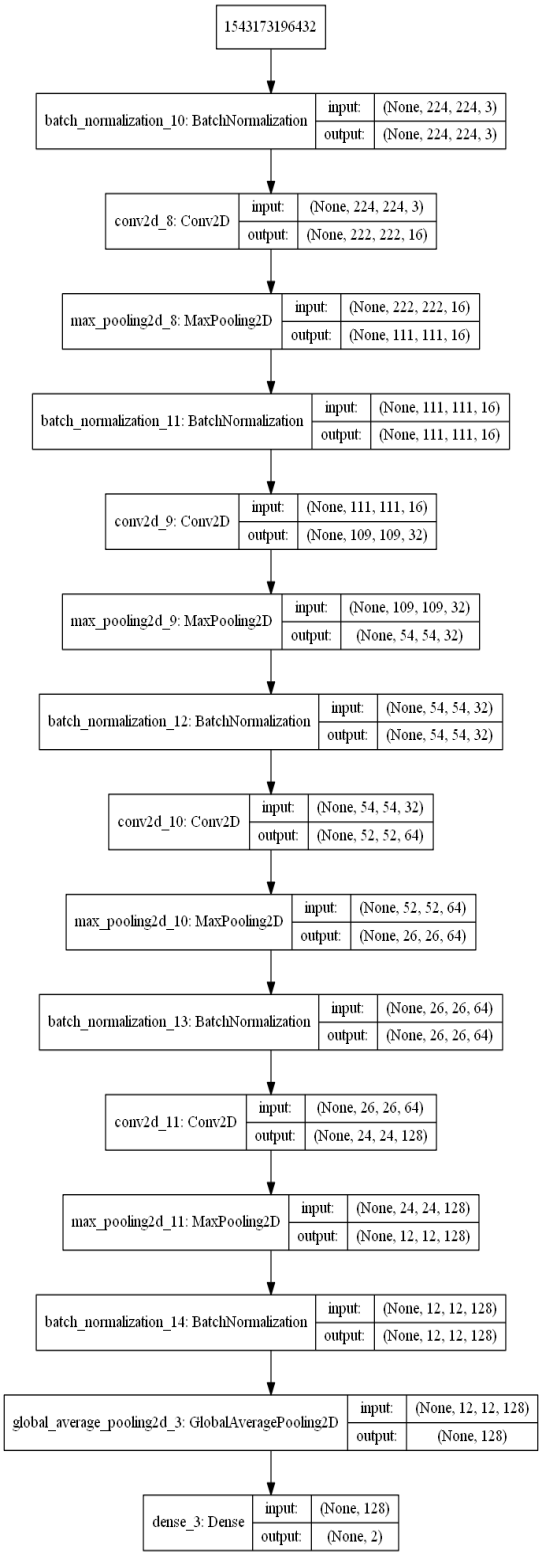

FIGURE 4. Data flow for CNN model.

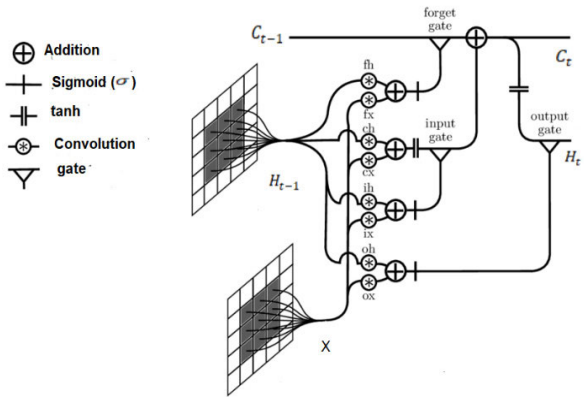

FIGURE 5. ConvLSTM workflow (figure adapted from [12]).

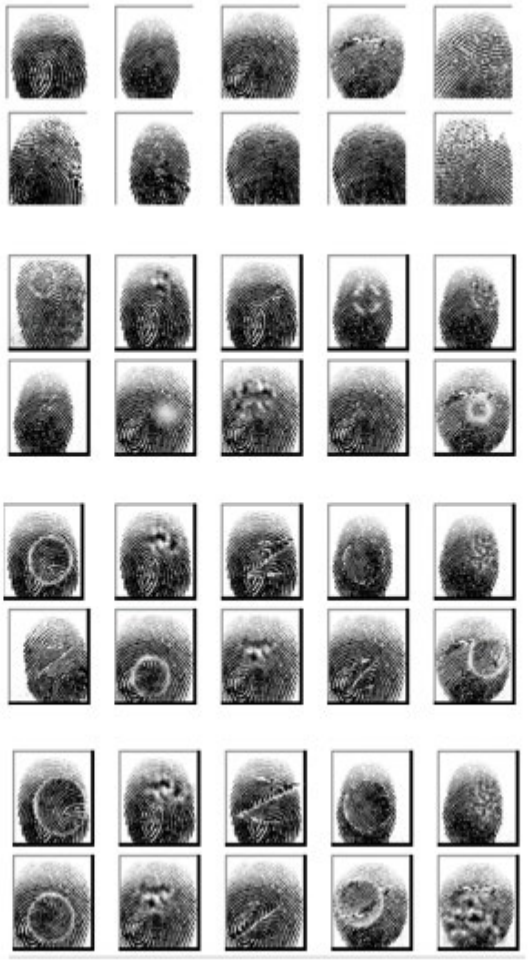

FIGURE 6. Samples of the fingerprints for a certain person of SOCOFing dataset.

C. SIMULATION RESULTS

The experiments reported in this section were simulated on an Intel core i7 8th edition CPU workstation with NVIDIA 4GB DDR5 GPU and 16GB RAM DDR5.

The objective of experiments is to ensure the effectiveness of the proposed system in detecting the alterations that may occur in the fingerprints during authentication processes

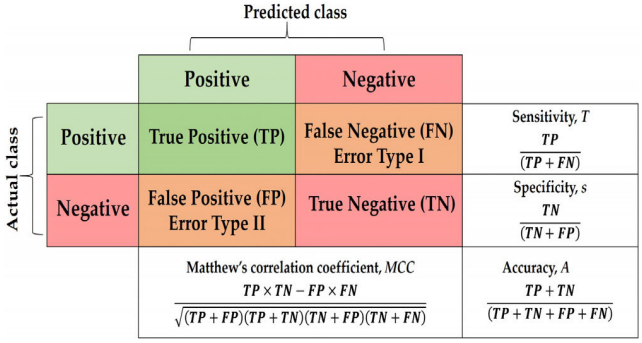

FIGURE 7. Equation matrix for binary quality metrics (adapted from [12]).

encountered in typical online banking transactions. As presented earlier in Section III, our study depends on the use of two deep learning frameworks (i.e., CNN and a hybrid one that combines ConvLSTM and CNN) for efficient detection of alterations to fingerprint of authorised users. Furthermore, the validation reported in this subsection employs fingerprint images obtained for three levels of alteration (i.e., obliteration, central rotation, and z-cut) as available in the SOCOFing dataset [19], [20].

1) RESULTS FOR OBLITERATION ALTERATION DETECTION

The obliteration alteration occurs, when the attacker destroys traces of some areas of the fingerprint to spoof the original fingerprint of a certain person. This type of alteration is considered as a hard alteration, because the outcome imbues characteristics far from those of the original fingerprint. Therefore, this type of alteration is easy to be detected. Figures 8 and 9 present accuracy and loss curves of obliteration alteration detection using the CNN DLM, while similar results for the hybrid DLM are presented in Figures 10 and 11. Furthermore, Table 1 presents evaluation outcomes for the obliteration alteration detection with both models. From the table, we notice that an average detection accuracy of 92.97% is recorded for the CNN DLM and 93.88% is recorded for the hybrid ConvLSTM model.

TABLE 1. Evaluation outcomes for obliteration alteration.

Evaluation Metric	CNN	ConvLSTM
Sensitivity	99	93.6
Specifity	74.93	94.73
PPV	92.19	98.15
NPV	96.15	83.19
Accuracy	92.97	93.88
F1 Score	95.47	95.82
MCC	80.82	84.76

2) RESULTS FOR CENTRAL ROTATION ALTERATION DETECTION

The central rotation alteration is considered as a medium alteration that is based on rotation operations on the

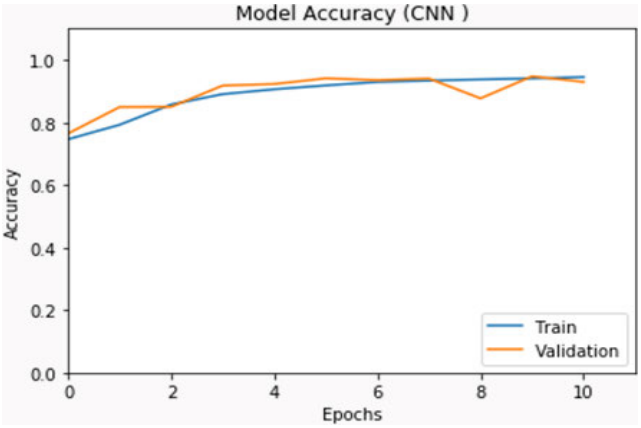

FIGURE 8. Plots of accuracy curves for obliteration alteration detection using CNN model.

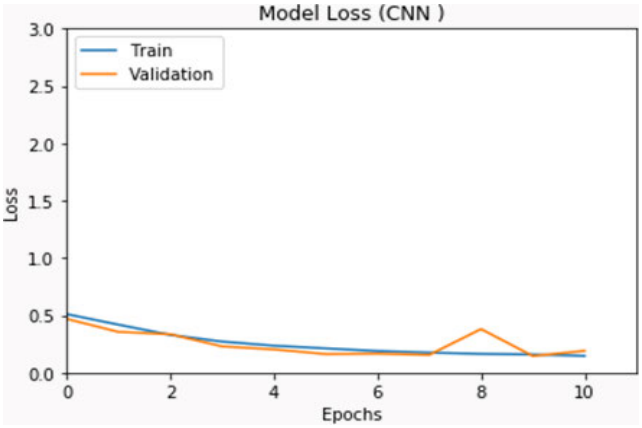

FIGURE 9. Plots of loss curves for obliteration alteration detection using CNN model.

fingerprint images. Both of our proposed deep learning models are implemented on datasets with these alterations, where simulation results revealed that the proposed models have a high performance in terms of detection accuracy. Figures 12 and 13 present plots of accuracy and loss curves for the central rotation alteration detection using the CNN DLM. Similarly, Figures 14 and 15 present plots of the accuracy and loss curves of central rotation alteration detection using the hybrid model. Furthermore, Table 2 presents the outcomes of evaluation for central rotation alteration detection using both models. As reported in this table, the CNN DLM records an accuracy of 98%, whilst the hybrid DLM attains an accuracy of 99%.

3) RESULTS FOR z-CUT ALTERATION

The proposed DLMs have been implemented on the z-cut altered fingerprint dataset [19]. Figures 18 and 19 present plots of accuracy and loss curves for z-cut alteration detection using the CNN DLM. Similarly, Figures 20 and 21 present plots of accuracy and loss curves for z-cut alteration detection using the proposed hybrid model. Furthermore, Table 3 highlights the performance of both DLMs in z-cut alteration detection. As reported in this table, the proposed CNN DLM

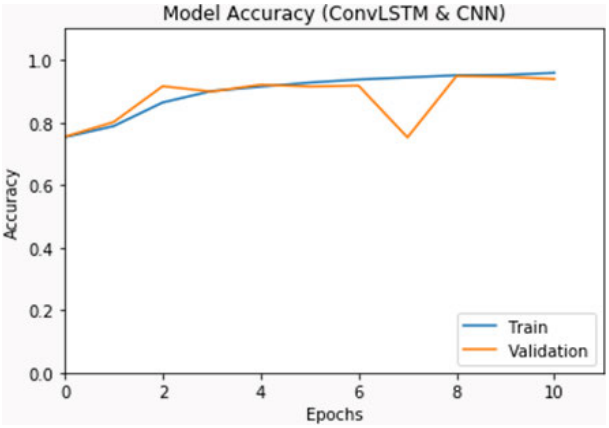

FIGURE 10. Plots of accuracy curves reported for obliteration alteration detection using the hybrid model.

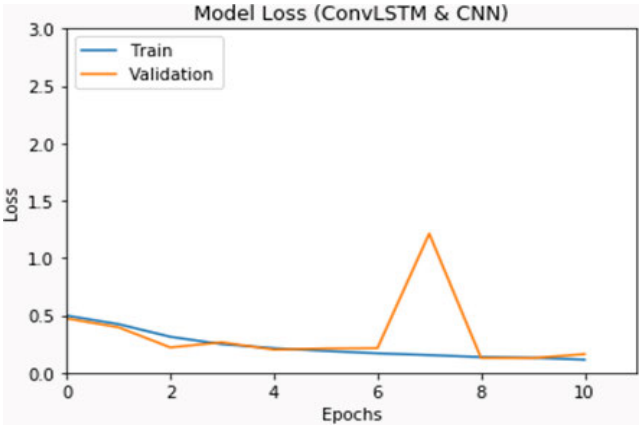

FIGURE 11. Plots of model loss curves for obliteration alteration detection using the hybrid model.

TABLE 2. Evaluation outcomes for central rotation alteration.

Evaluation Metric	CNN	ConvLSTM
Sensitivity	98.13	98.92
Specifity	98.87	99.27
PPV	99.60	99.74
NPV	94.88	97
Accuracy	98.32	99.01
F1 Score	98.86	99.33
MCC	95.73	97.46

records a detection accuracy of 98.76%, while the hybrid DLM attains an accuracy of 99.05%, which confirms the effectiveness of both models.

IV. DISCUSSION OF RESULTS

With an average detection accuracy of 97%, the results recorded in the previous section illustrate the effectiveness of both DLMs in our proposed system as tools to detect alterations to fingerprint biometrics. To further establish this performance, in this section we discuss the recorded results relative to results of a state-of-the-art technique reported in the literature.

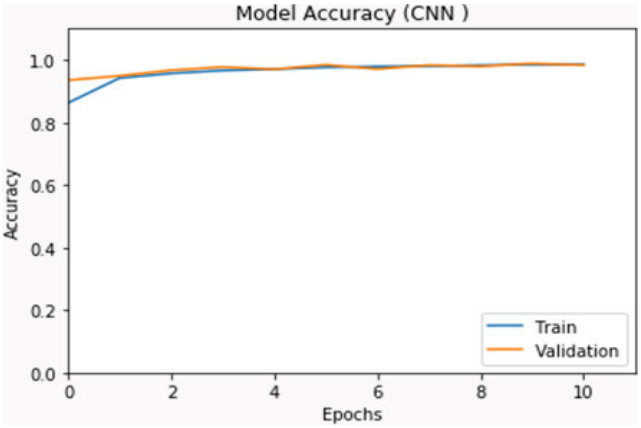

FIGURE 12. Plots of accuracy curves for central rotation alteration detection using CNN model.

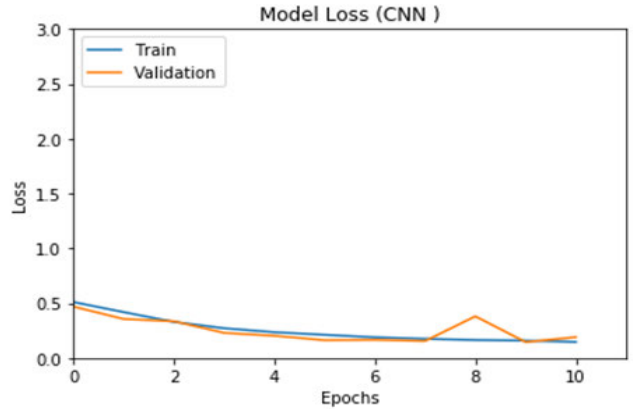

FIGURE 13. Plots of loss curves for central rotation alteration detection using CNN model.

TABLE 3. Evaluation outcomes for z-cut alteration detection.

Evaluation Metric	CNN	ConvLSTM
Sensitivity	98.38	98.94
Specifity	99.67	99.33
PPV	99.86	99.72
NPV	96.27	97.51
Accuracy	98.76	99.05
F1 Score	99.11	99.33
MCC	97.08	97.75

In [20], CNN and ResNet18 DLMs were utilised for detection of fingerprint alteration, the CNN structure was made up of convolutional layers with 20 3 3, 40 3 3, 60 3 3, and 80 3 3 kernels. Additionally, the convolutional layers were followed by two fully-connected layers with 1000 and 100 hidden units, respectively. In another model, ResNet18 pre-trained model was used.

Table 4 highlights the performance of our proposed DLMs alongside those reported in [20] in terms of alteration detection accuracy and Predictive Positive Values (PPV).

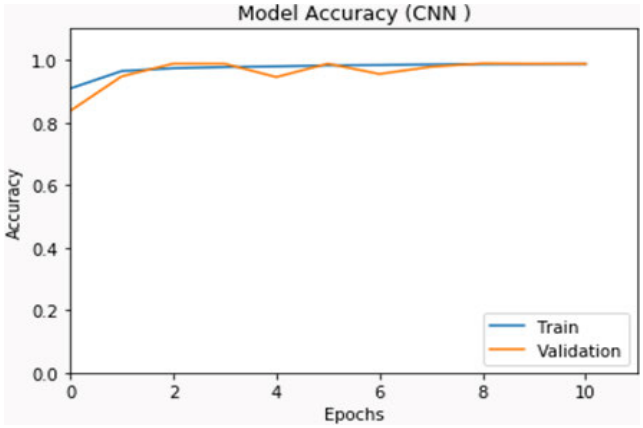

FIGURE 14. Plots of accuracy curves for z-cut alteration detection using CNN model.

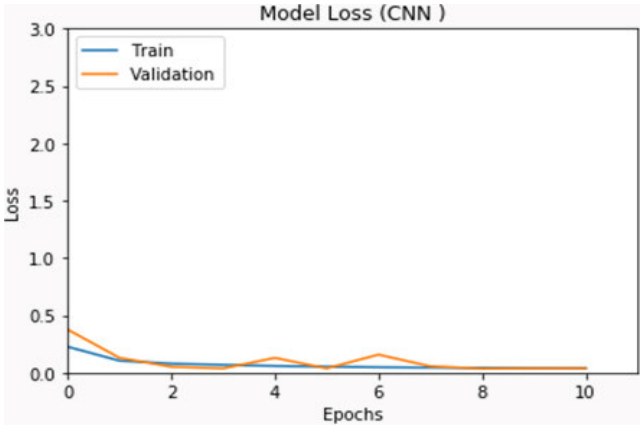

FIGURE 15. Plots of loss curves for z-cut alteration detection using CNN model.

TABLE 4. Performance analysis.

Method	Alteration	Model	PPV (%)	Accuracy (%)
[20]	Central rotation	CNN	98.34	97.37
		ResNet18	99.95	99.94
	Obliteration	CNN	99.52	99.23
		ResNet18	99.98	99.81
	z-Cut	CNN	97.27	98.51
		ResNet18	99.93	99.82
Proposed	Central rotation	CNN	99.60	98.32
		ConvLSTM	99.74	99.02
	Obliteration	CNN	92.19	92.97
		ConvLSTM	93.88	98.15
	z-Cut	CNN	99.86	98.32
		ConvLSTM	99.72	99.01

As seen from the table, both systems report acceptable levels with our system beaten to second place in terms of PPV for obliteration alteration detection, while it tops in terms of PPV for the central rotation and z-cut alterations. Furthermore, our proposed DLMs perform better than [20] in terms of detection accuracy for the central rotation alteration. These results indicate the ability of our proposed models to

match established ones with superior performance for central rotation alteration detection.

V. CONCLUDING REMARKS

With the advances in intelligent systems engineering, smart technologies will become ubiquitous in emerging smart cities. At such stages, fifth generation (5G) networks will require technologies to mitigate identity theft, enhance person identification and other Intelligent Access Control (IAC) mechanisms.

In tandem with these advances, biometric identification will become pervasive. Our study is primarily aimed at providing additional security to these platforms.

The prime challenge in such IAC systems is the ability to efficiently discriminate between the original and fake biometrics, where depending on sophistication, efforts to impugn the integrity of biometric markers could vary from easy to medium to high. Our study presented an alteration detection system using deep learning models based on CNNs and ConvLSTM. The proposed models are implemented on a dataset of fingerprint images comprising three types of alterations. Outcomes of reported simulation-based experiments ensure the effectiveness of our proposed system in the detection of fingerprint alterations with superior performance, which makes it viable for applications in 5G network-based secure smart cities.

REFERENCES

[1] R. Gad, M. Talha, A. A. A. El-Latif, M. Zorkany, A. El-Sayed, N. El-Fishawy, and G. Muhammad, "Iris recognition using multi-algorithmic approaches for cognitive Internet of Things (CIoT) framework," *Future Gener. Comput. Syst.*, vol. 89, pp. 178–191, Dec. 2018.

[2] N. Wang, Q. Li, A. A. A. El-Latif, T. Zhang, and X. Niu, "Toward accurate localization and high recognition performance for noisy iris images," *Multimedia Tools Appl.*, vol. 71, no. 3, pp. 1411–1430, Aug. 2014.

[3] R. Gad, A. A. A. El-Latif, S. Elseuofi, H. M. Ibrahim, M. Elmezain, and W. Said, "IoT security based on iris verification using multi-algorithm feature level fusion scheme," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, May 2019, pp. 1–6.

[4] J. Peng, Q. Li, A. A. A. El-Latif, N. Wang, and X. Niu, "Finger vein recognition with Gabor wavelets and local binary patterns," *IEICE Trans. Inf. Syst.*, vol. E96.D, no. 8, pp. 1886–1889, 2013.

[5] J. Peng, Q. Li, N. Wang, A. A. A. El-Latif, and X. Niu, "An effective preprocessing method for finger vein recognition," in *Proc. 5th Int. Conf. Digit. Image Process. (ICDIP)*, Jul. 2013, Art. no. 887808.

[6] J. Peng, N. Wang, A. A. A. El-Latif, Q. Li, and X. Niu, "Finger-vein verification using Gabor filter and SIFT feature matching," in *Proc. 8th Int. Conf. Intell. Inf. Hiding Multimedia Signal Process.*, Jul. 2012, pp. 45–48.

[7] J. Peng, A. A. A. El-Latif, Q. Li, and X. Niu, "Multimodal biometric authentication based on score level fusion of finger biometrics," *Optik*, vol. 125, no. 23, pp. 6891–6897, Dec. 2014.

[8] N. Wang, Q. Li, A. A. A. El-Latif, J. Peng, and X. Niu, "An enhanced thermal face recognition method based on multiscale complex fusion for Gabor coefficients," *Multimedia Tools Appl.*, vol. 72, no. 3, pp. 2339–2358, Oct. 2014.

[9] N. Wang, Q. Li, A. A. A. El-Latif, X. Yan, and X. Niu, "A novel hybrid multibiometrics based on the fusion of dual iris, visible and thermal face images," in *Proc. Int. Symp. Biometrics Secur. Technol.*, Jul. 2013, pp. 217–223.

[10] N. T. Haggag, A. Sedik, G. M. Elbanby, A. S. El-Fishawy, and A. A. Khalaf, "Classification of corneal pattern based on convolutional LSTM neural network," *Menoufia J. Electr. Eng. Res*, vol. 28, pp. 158–162, Dec. 2019.

[11] A. Alghamdi *et al.*, "Detection of myocardial infarction based on novel deep transfer learning methods for urban healthcare in smart cities," *Multimedia Tools Appl.*, 2020, doi: 10.1007/s11042-020-08769-x.

[12] A. Sedik, A. M. Iliyasu, B. A. El-Rahiem, M. E. A. Samea, A. Abdel-Raheem, M. Hammad, J. Peng, F. E. A. El-Samie, and A. A. A. El-Latif, "Deploying machine and deep learning models for efficient data-augmented detection of COVID-19 infections," *Viruses*, vol. 12, no. 7, p. 769, Jul. 2020.

[13] M. Hammad, A. M. Iliyasu, A. Subasi, E. S. L. Ho, and A. A. A. El-Latif, "A multitier deep learning model for arrhythmia detection," *IEEE Trans. Instrum. Meas.*, vol. 70, Oct. 2021, Art. no. 2502809, doi: 10.1109/TIM.2020.3033072.

[14] F. M. Al-Azrak, A. Sedik, M. I. Dessowky, G. M. El Banby, A. A. M. Khalaf, A. S. Elkorany, and F. E. A. El-Samie, "An efficient method for image forgery detection based on trigonometric transforms and deep learning," *Multimedia Tools Appl.*, vol. 79, nos. 25–26, pp. 18221–18243, Jul. 2020.

[15] M. A. Elaskily *et al.*, "A novel deep learning framework for copy-move forgery detection in images," *Multimedia Tools Appl.*, vol. 79, pp. 19167–19192, 2020, doi: 10.1007/s11042-020-08751-7.

[16] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998.

[17] M. Ranzato, F. J. Huang, Y.-L. Boureau, and Y. LeCun, "Unsupervised learning of invariant feature hierarchies with applications to object recognition," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2007, pp. 1–8.

[18] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, "Dropout: A simple way to prevent neural networks from overfitting," *J. Mach. Learn. Res.*, vol. 15, no. 1, pp. 1929–1958, 2014.

[19] Y. I. Shehu, A. Ruiz-Garcia, V. Palade, and A. James, "Sokoto coventry fingerprint dataset," 2018, *arXiv:1807.10609*. [Online]. Available: http://arxiv.org/abs/1807.10609

[20] Y. I. Shehu, A. Ruiz-Garcia, V. Palade, and A. James, "Detection of fingerprint alterations using deep convolutional neural networks," in *Proc. Int. Conf. Artif. Neural Netw.*, 2018, pp. 51–60.

AHMED SEDIK received the B.Sc. and M.Sc. degrees in engineering from the Faculty of Engineering, Tanta University, Egypt, in 2012 and 2018, respectively, and the Ph.D. degree from Minia University, Egypt, in 2020. He is currently an Assistant Professor with the Faculty of Artificial Intelligence, Kafrelsheikh University.

LO'AI TAWALBEH (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees (Hons.) in computer engineering from Oregon State University (OSU), OR, USA, in 2002 and 2004, respectively. From 2005 to 2012, he has worked as an Adjunct Professor to teach in the Master programs at the New York Institute of Technology (NYIT), DePaul's University, and Princes Sumaya University for Technology (PSUT). He is currently an Associate Professor with the Department of Computing and Cyber Security, Texas A&M University at San Antonio, TX, USA. He is also the Founder and the Director of the Cryptographic Hardware and Information Security (CHiS) Laboratory, JUST. He has won many research grants and awards. He has more than 90 research publications in many refereed international journals and conferences. His research interests include information security, cryptographic applications and crypto systems hardware implementations, and mobile cloud security. He is the chair of many international conferences and workshops in mobile cloud security, blockchain, and related cyber security areas. He is a reviewer and an associate editor of many international journals.

MOHAMED HAMMAD received the M.Sc. degree from the Information Technology Department, Faculty of Computers and Information, Menoufia University, Egypt, in 2015, and the Ph.D. degree from the School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China, in 2019. He is currently an Assistant Professor with the Faculty of Computers and Information, Menoufia University. His research interests include biomedical imaging, digital forensics, the IoT, computer vision, machine learning, deep learning, pattern recognition, and biometrics. He has published more than 20 articles in international SCI-IF journals. He has served as a Topics Board Editor for *Forensic Sciences* (MPDI) journal; a Guest Editor for many international journals, such as *International Journal of Digital Crime and Forensics* (IJDCF); and a Reviewer of more than 100 articles for many prestigious journals, such as IEEE Transactions on Systems, Man, and Cybernetics: Systems, IEEE Access, *PLOS One*, *Pattern Recognition Letters*, and *Computers in Biology and Medicine*.

AHMED A. ABD EL-LATIF (Senior Member, IEEE) received the Ph.D. degree in computer science and technology from the Harbin Institute of Technology (HIT), China. He is currently an Associate Professor of computer science with Menoufia University and the School of Information Technology and Computer Science, Nile University, Egypt. His research interests include secure wireless communication, secret media sharing, information hiding, applied cryptanalysis, perceptual cryptography, multimedia content encryption, biometrics, forensic analysis in digital images, the IoT, and quantum information processing. He is a Fellow of the Academy of Scientific Research and Technology, Egypt. He is an Associate Editor of the *Journal of Cyber Security and Mobility* and a guest editor of ISI journals.

GHADA M. EL-BANBY received the M.Sc. and Ph.D. degrees in automatic control engineering from Menoufia University, Egypt, in 2006 and 2012, respectively. She works as a Lecturer at the Department of Industrial Electronics and Control Engineering, Faculty of Electronic Engineering, Menoufia University. Her current research interests include computer vision, data fusion, systems, image processing, signal processing, medical imaging, modeling, and control.

ASHRAF A. M. KHALAF received the B.Sc. and M.Sc. degrees in electrical engineering from Minia University, Egypt, in 1989 and 1994, respectively, and the Ph.D. degree in electrical engineering from the Graduate School of Natural Science and Technology, Kanazawa University, Japan, in March 2000. He currently works as a Professor and Head of the Electronics and Communications Engineering Department, Minia University.

FATHI E. ABD EL-SAMIE received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees from Menoufia University, Minuf, Egypt, in 1998, 2001, and 2005, respectively. Since 2005, he has been a Teaching Staff Member with the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University. He worked as a Researcher with KACST-TIC in Radio Frequency and Photonics for the e-Society (RFTONICs) from 2013 to 2015. His current research interests include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications. He was a recipient of the Most Cited Paper Award from the *Digital Signal Processing* Journal, in 2008.

ABDULLAH M. ILIYASU (ABDUL M. ELIAS) (Senior Member, IEEE) received the M.E., Ph.D., and Dr.Eng. degrees in computational intelligence and intelligent systems engineering from the Tokyo Institute of Technology (Tokyo Tech.), Japan. He is currently a Research Faculty with the School of Computing, Tokyo Tech. He is also the Principal Investigator and the Team Leader of the Advanced Computational Intelligence and Intelligent Systems Engineering (ACI-ISE) Research Group, College of Engineering, Prince Sattam Bin Abdulaziz University (PSAU), Saudi Arabia. He is also a Professor with the School of Computer Science and Technology, Changchun University of Science and Technology, China. In addition to being among the pioneers of research in the emerging quantum image processing (QIP) subdiscipline, he has to his credit more than 150 publications traversing the areas of computational intelligence, quantum cybernetics, quantum image processing, quantum machine learning, cyber and information security, intelligent systems engineering, the Internet of Things, 4IR, health informatics, and electronic systems reliability. As well as being the Managing Editor of Fuji Technology Press, Japan, he is a member of Editorial Board of the *Journal of Advanced Computational Intelligence and Intelligent Informatics (JACIII)*, *Quantum Reports* journal, *International Journal of Electrical and Computer Engineering (IJECE)*, and the *Journal of Medical Imaging and Health Informatics (JMIHI)*. He is also an Associate Editor of many other journals, including IEEE Access, *Telkomnika*, and *Information Sciences*.