Abstract—Fingerprint recognition is often a game-changing step in establishing evidence against criminals. However, we are increasingly finding that criminals deliberately alter their fingerprints in a variety of ways to make it difficult for technicians and automatic sensors to recognize their fingerprints, making it tedious for investigators to establish strong evidence against them in a forensic procedure. In this sense, deep learning comes out as a prime candidate to assist in the recognition of damaged fingerprints. In particular, convolution algorithms. In this paper, we focus on the recognition of damaged fingerprints by Convolutional Long Short-Term Memory networks. We present the architecture of our model and demonstrate its performance which exceeds 95% accuracy, 99% precision, and approaches 95% recall and 99% AUC.

Index Terms—Biometrics, forensics, fingerprint recognition, Deep Learning, Convolutional Long Short-Term Memory networks.

This paper was accepted, on December 5, 2020, for publication and oral presentation at the 2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP 2021) to be held in Zhuhai, China during January 8-10, 2021 and hosted by Beijing Normal University (Zhuhai).

I. INTRODUCTION

Fingerprints are traces that we leave behind every time we touch an object. The patterns created by the ridges and folds of the the fingers’ skin are different for each person, and can therefore be used to identify someone in a virtually unique and permanent way, just like other biometric data such as DNA, iris, face, voice, etc. Fingerprint patterns can serve an important role in the identification of victims of both natural and man-made disasters [1], such as earthquakes, floods, civil strife, and terrorist attacks. This proof of identity is critical not only for the investigators [2][3], but also for the families of the victims concerned. When a fingerprint is taken from a crime scene, it is compared to fingerprints stored in police databases to prove whether or not a suspect is involved in multiple actions. On the other hand, fingerprint identification is the cornerstone of national security and is the most practical biometric means for the identification of criminals, drug dealers, human traffickers, immigration law violators, terrorists, who can infiltrate the territory under false identities through the ports of entry of a given country. Similarly, fingerprints are increasingly being used as a means of choice to confirm a person’s identity in access and payment transactions [4]. This method is indeed much faster, easier and more secure than the traditional use of passwords or PIN codes, which have the disadvantages of being difficult to remember and easy to steal. For their part, criminals’ means have constantly and rapidly evolved over time, allowing them to evade the traditional means of fingerprint recognition installed at ports of entry and police checkpoints [5][6]. Among these means, criminals often choose to deliberately damage the skin of their fingers to obfuscate their fingerprints so that they appear different, for recognition algorithms, from those stored in databases. In this complex context, artificial intelligence becomes the tool of choice for identifying damaged fingerprints and their owners. In this paper, we address the problem of recognizing damaged fingerprints using Convolutional Long Short-Term Memory networks (Convolutional LSTMs) [7]. In fact, an image of a fingerprint can be seen as a set of patterns (or features) that are captured by convolutional operations. It is also seen as a sequence of entities (pixels, rows, columns, features). This notion of sequence is generally well suited to processing by specialized recurrent neural networks such as Long Short-Term Memory (LSTM) networks. This makes the subject a good candidate to be addressed by Convolutional LSTMs.

II. DAMAGED FINGERPRINTS

Damage to fingerprints is often deliberate and of several sources and types [8]. It is mainly caused by the use of strong
chemicals or by physical actions and lesions applied to the surface of fingers. This damage results in severely breaking the link between a person’s fingerprints and their identity. In this regard, it is worth emphasizing that the problem of damaged fingerprints differs substantially from the problem of falsified fingerprints, which involves fake fingerprints made of a material that sticks to the palms of the fingers to divert recognition software. In this paper, we will consider the following alterations [9] that can muddle most of fingerprint verification software.

A. Obliteration

Fingerprints on fingertips can be obliterated by various means such as burning, abrasion, application of strong chemicals and skin transplantation which cause an alteration of the morphology of the surface of the fingertips coming from a strong and damaging action on the skin cells. Fig. 1 shows an example of a fingerprint being obliterated using a chemical substance.

![Obliterated fingerprint](image)

B. Z-cut

A Z-cut is a lesion in the shape of the letter Z brought to the skin of the fingertip. This type of modification of fingerprints is increasingly observed in border control applications by suspicious travellers and illegal asylum seekers to bypass identification systems which are generally vulnerable to such manoeuvres, some wanting to evade existing regulations, others wanting access to the priority asylum procedure. Fig. 2 shows a fingerprint with a Z-cut.

![Z-cut fingerprint](image)

C. Central rotation

This alteration consists of removing a slice of the skin from a finger and planting it in a different position in the finger’s tip in a rotated way. The means to do this is not too complex and the resulting altered fingerprints are very hard to compare with the original fingerprints by automated matching systems. Fig. 3 shows a fingerprint with a central rotation.

![Central rotated fingerprint](image)

III. Deep Learning Algorithms

A. Long Short-Term Memory Networks

Long Short-Term Memory (LSTM) networks [10, 11] are basically Recurring Neural Networks (RNNs). RNNs take into account not only the current input but also the previous output (see Fig 4). That is to say, the decision made at the step \( t - 1 \) affects the decision that will be made at the next step \( t \). In other words, a standard RNN (aka vanilla RNN) is a neural network with memory. Adding memory to RNNs makes them powerful in processing sequences such as images, sound, videos, texts, etc. The sequential information is maintained in an internal memory (hidden state) that captures long-term dependencies between events that may be distant in time. Although RNNs manage sequences efficiently, they suffer from a number of issues [12]. The first is the exploding problem. This occurs when large gradient errors build up as the training progresses, which leads to very large updates in the network weights and resulting in an unstable network. The second problem is the vanishing gradient. This occurs when the gradient values become extremely low, causing the model to stop learning. Moreover, RNNs are known to be sensitive to the way the model is initialized. This can lead to model overfitting and thus strange results may occur.

![RNN process](image)
RNNs, the repetition module consists of a single hyperbolic tangent layer \( \tanh \). In LSTMs, the repetition module is much more complex and made up of three elements referred to as \textit{gates}. The first gate is called forget gate, which consists of a sigmoid neural network layer.

\[
f_t = \sigma(W_f[h_{t-1}, x_t] + b_f) \quad (1)
\]

The sigmoid function generates a vector with zeros and ones. Essentially, its role is to decide which values the cell state should retain (for ones) and which values should simply be discarded (for zeros). This vector is then multiplied (pointwise product) by the previous cell state \( c_{t-1} \).

The second gate is referred to as the input gate. Its purpose is to decide which new information needs to be added to the cell state. This is achieved through two layers. The first one is a sigmoid layer that issues a vector of zeros and one that determines what should be modified and what should remain, as given by Equation \( 2 \)

\[
i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \quad (2)
\]

The second layer is a \( \tanh \) layer that generates a vector of a candidate vector \( \tilde{c} \) to add to the cell state, as given by Equation \( 3 \)

\[
\tilde{c}_t = \tanh(W_c[h_{t-1}, x_t] + b_c) \quad (3)
\]

It is worth noticing that the \( \tanh \) function is preferred to other activation functions because it emits both positive and negative values, so that the cell state can increase or decrease.

Then, the cell state is updated considering the two previous gates as given by Equation \( 4 \)

\[
c_t = (f_t \otimes c_{t-1}) \oplus (i_t \otimes \tilde{c}_t) \quad (4)
\]

The third gate is referred to as the output gate. This gate determines what the cell will output. The output hinges upon a filtered version of the cell state. To do so, a sigmoid layer, comparable to the sigmoid layers in the previous gates, will first decide which parts of the cell state will be kept by emitting a vector of zeros and ones. Then, a \( \tanh \) function is applied to the updated cell state. At last, a pointwise product is performed on the sigmoid output vector and the filtered cell state resulting in the output state \( h_t \). This is given by Equation \( 5 \) and Equation \( 6 \)

\[
o_t = \sigma(W_o[h_{t-1}, x_t] + b_o) \quad (5)
\]

\[
h_t = o_t \otimes \tanh(c_t) \quad (6)
\]

### B. Convolutional Neural Networks

A standard Convolutional Neural Network (CNN) is a powerful Deep Learning model when dealing with images. It is made up of four layers where the output of one layer is the input of the next:

1) The convolution layer (CONV): this is the most important component of the model in that it identifies a set of features in the data received using filters. The idea is to slip a small window (filter) representing the feature along the data matrix and calculate the convolution product. Pairs (matrix, filter) are then obtained (feature map). The higher the convolution product is, the more likely the feature position in the image is;

2) The pooling layer (POOL): it is interposed between two convolution layers. It receives several input feature maps, and applies to each of them a pooling operation which consists in shrinking the size of the input matrices, while preserving their important features. To achieve this, the input matrix is divided into regular cells, and then the maximum value is kept within each cell. In practice, small square cells are used to preclude losing too much information. The same number of feature maps at the output is conserved at the input, but the matrices are much smaller. The pooling layer cuts down the number of parameters and accelerates calculations. This improves network efficiency and helps to reduce overfitting;

3) The Rectified Linear Unit (ReLU) correction layer: this layer substitutes all negative values with zeros using the ReLU activation function (Equation \( 7 \)).

\[
\text{ReLU}(x) = \max(0, x) \quad (7)
\]

This results in a neural network much faster without significantly decreasing its accuracy. This also enhances non-linearity inside the network. The whole process involving these three steps can be repeated many times.

![Fig. 5: LSTM (cell)](image-url)
4) The fully-connected layer (FC): This layer is similar to any ordinary layer in any neural network. It receives an input vector (usually flattened) and applies an activation function, to finally vote for the classes.

C. Convolutional LSTM

A Convolutional LSTM model is roughly a CNN connected to an LSTM [19]. Hence, the image passes through the convolutions layers and results in a vector flattened to a 1D array with the obtained features forming the input of the LSTM. This being said, in some implementations, internal matrix multiplications are exchanged with convolution operations where the data flows through the cells in two or three dimensions.

IV. Experiment setup

A. Dataset

First of all, it is worth mentioning that there is an observable dearth of public datasets containing damaged fingerprint images, which has hampered research in this regard. In our study, we use the Sokoto Coventry Fingerprint (SOCOFing) dataset [9]. This dataset is made up of 6000 fingerprint images taken from 600 male and female subjects. Fingerprints are synthetically altered with three different types of alteration: obliteration, Z-cut, and central rotation.

B. Data preprocessing

Fingerprint images are read with a single grayscale channel. Then, the resulting image float arrays are normalized. The third of the dataset is reserved for validation and the rest of the dataset is used for training. We use the stratify strategy when splitting data so that the validation dataset distribution, as well as the training dataset distribution, remain the same as the original one.

C. Model architecture

The first layer is a Convolutional LSTM layer with 64 filters and a ReLU activation function [13]. The second layer is a Dropout layer to ignore some number of layer outputs to prevent overfitting. The third layer is a Dense layer with 100 nodes and a ReLU activation function. The last layer is a Dense layer with the number of subjects nodes and a Softmax activation function [13]. Adam optimizer is selected [20].

V. Results and discussion

To evaluate how well our model is performing, we use the following metrics:

\[
\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} 
\]  
(8)

\[
\text{Precision} = \frac{TP}{TP + FP} 
\]  
(9)

\[
\text{Recall} = \frac{TP}{TP + FN} 
\]  
(10)

where TP, TN, FP, FN represent the true positives, true negatives, false positives, and false negatives, respectively. Accuracy measures the portion of people who are identified correctly by the model through their fingerprints. Precision is a useful metric when the cost of a false positive is high (i.e. in a forensic investigation, this means someone who is wrongly identified as guilty by the model). Recall, in contrast, is useful when a false negative matters (i.e. a criminal not being identified by the model). We also use the Area Under the Curve (AUC) metric to make sure that our model does not randomly predict its outputs. For all of these four metrics, the closer the metric is to 1, the better the model is, for the targeted property. Fig 6 illustrates the variation of the loss function (we use the categorical cross-entropy loss function) during learning time. Fig 7, Fig 8, Fig 9, and Fig 10 illustrate the variation of the accuracy (we use the categorical accuracy), precision, recall, and AUC during learning time, respectively.

![Fig. 6: Loss variation during learning time (100 Epochs)](image6)

![Fig. 7: Accuracy variation during learning time (100 Epochs)](image7)

We notice that the model reaches its optimums at epoch 27, with the values presented in Table I obtained on the validation
FIG. 8: Precision variation during learning time (100 Epochs)

FIG. 9: Recall variation during learning time (100 Epochs)

FIG. 10: Area under the curve (AUC) variation during learning time (100 Epochs)

As can be seen in Table I, our Convolutional LSTM model presents very satisfactory results for all selected metrics in the recognition of subjects with damaged fingerprints, exceeding 95% accuracy, 99% precision, and approaches 95% recall and 99% AUC. We can also see the clear contribution of Convolutional LSTM compared to conventional LSTM with all metrics. In fact, the convolution layers were able to catch the most important features from the input images. These features were provided to LSTM as sequences, and the latter coped well with them as expected. This synergy between the two layers yielded the good performance of the whole model. Comparative models have proven their performance in similar fields such as scene text recognition [21], dynamic gesture recognition [22], hyperspectral image classification [23], emotion recognition [24], event surveillance [25], traffic forecasting [26], air quality prediction [27], facial expression recognition [28], etc. These good results encourage us to explore the recognition, by comparable networks, of other biometric forms such as hand or earlobe morphology, retinal and iris physiognomy [29], voice [30, 31], and signatures [32], especially those that have been forged or falsified or altered [33]. These biometric patterns play as crucial a role as fingerprints in forensic investigative procedures and in establishing proof of innocence or indictment. The same important role can be played in the identification of victims in disasters and natural catastrophes. That said, as our model has been trained and validated on datasets of hundreds of subjects, when reality involves millions of subjects, it requires more investigation on larger real-world data. This will certainly entail many complexities and challenges that will be the focus of future work.

VI. CONCLUSION

Our research results in a well performing recurrent neural network model that can be used to examine and interpret evidence in criminal proceedings involving fingerprints, deliberately damaged by seasoned criminals. Our model can help prove the guilt or innocence of suspects. It can also help resolve a wide range of legal issues related to the identification, analysis and proof assessment. We have also mapped out future
paths that involve similar models as well as other comparable biometric forms that can be of great value in an investigation process.

ACKNOWLEDGMENT

This research was funded by the Natural Sciences and Engineering Research Council of Canada (NSERC).

REFERENCES

[1] A. Bécue, H. Eldridge, and C. Champod, “Interpol review of fingerprints and other body impressions 2016–2019,” Forensic Science International: Synergy, 2020. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2589897X20300139

[2] K. N. Win, K. Li, J. Chen, P. Fournier-Viger, and K. Li, “Fingerprint classification and identification algorithms for criminal investigation: A survey,” vol. 110, 2020, pp. 758–771. [Online]. Available: https://doi.org/10.1016/j.future.2019.10.019

[3] G. L. Marcialis, F. Roli, P. Colt, and G. Deol围棋, “A fingerprint forensic tool for criminal investigations,” in Handbook of Research on Computation Forensics, Digital Crime, and Investigation: Methods and Solutions, G. Li, Ed., IGI Global, 2010, pp. 23–52. [Online]. Available: https://doi.org/10.4018/978-1-60566-836-9.ch002

[4] M. Moalosi, H. Hlomani, and O. S. D. Phelo, “Combating credit card fraud with online behavioural targeting and device fingerprinting,” Int. J. Electron. Secur. Digit. Forensics, vol. 11, no. 1, pp. 46–69, 2019. [Online]. Available: https://doi.org/10.1007/s13219-018-00652-z

[5] S. Yoon, J. Feng, and A. K. Jain, “Altered fingerprints: Analysis and detection,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 3, pp. 451–464, 2012. [Online]. Available: https://doi.org/10.1109/TPAMI.2011.161

[6] R. Joshi, Neelam and M. Ramakrishnan, “A new classification algorithm with glicm for the altered fingerprints,” in Information Technology and Mobile Communication, V. V. Das, G. Thomas, and F. Lumban Gaol, Eds., Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 352–357.

[7] Y. Yu, X. Si, C. Hu, and J. Zhang, “A review of recurrent neural networks: Lstms and network architectures,” Neural Computation, vol. 31, no. 7, pp. 1235–1270, 2019, pmid: 31113301. [Online]. Available: https://doi.org/10.1162/NECO_a_01199

[8] J. Feng, A. K. Jain, and A. Ross, “Detecting altered fingerprints,” in 20th International Conference on Pattern Recognition, ICPP 2010, Istanbul, Turkey, 23-26 August 2010. IEEE Computer Society, 2010, pp. 1622–1625. [Online]. Available: https://doi.org/10.1109/ICPR.2010.401

[9] Y. I. Shehu, A. Ruiz-Garcia, V. Palade, and A. James, “Sokoto coventry fingerprint dataset,” CoRR, vol. abs/1807.10609, 2018. [Online]. Available: http://arxiv.org/abs/1807.10609

[10] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” Physica D: Nonlinear Phenomena, vol. 404, p. 132306, 2020. [Online]. Available: https://doi.org/10.1016/j.physd.2019.132306

[11] A. Bémen, S. Marra, M. A. Iachino, and F. C. Morabito, “High speed, programmable implementation of a tanh-like activation function and its derivative for digital neural networks,” in Proceedings of the International Joint Conference on Neural Networks, IJCNN 2007, Celebrating 20 years of neural networks, Orlando, Florida, USA, August 12-17, 2007. IEEE, 2007, pp. 506–511. [Online]. Available: https://doi.org/10.1109/IJCNN.2007.4371008

[12] A. Krizhevsky, I. Sutskever, and G. E. Hinton, “Imagenet classification with deep convolutional neural networks,” in Proceedings of the 25th International Conference on Neural Information Processing Systems - Volume 1, ser. NIPS’12. Red Hook, NY, USA: Curran Associates Inc., 2012, pp. 1097–1105.

[13] Z. Li, W. Yang, S. Peng, and F. Liu, “A survey of convolutional neural networks: Analysis, applications, and prospects,” 2020.

[14] M. Pretorius, E. Barnard, and M. H. Dave, “Kelu and sigmoidal activation functions,” in Proceedings of the South African Forum for Artificial Intelligence Research, Cape Town, South Africa, 4-6 December, 2019, ser. CEUR Workshop Proceedings, M. H. Dave and E. Barnard, Eds., vol. 2540. CEUR-WS.org, 2019, pp. 37–48. [Online]. Available: http://ceur-ws.org/Vol-2540/FAIR2019_paper_32.pdf

[15] B. Xu, N. Wang, Y. Chen, and M. Li, “Empirical evaluation of rectified activations in convolutional network,” CoRR, vol. abs/1505.00853, 2015. [Online]. Available: http://arxiv.org/abs/1505.00853

[16] L. Courtney and R. Screenivas, “Using deep convolutional LSTM networks for learning spatiotemporal features,” in Pattern Recognition - 5th Asian Conference, ACPR 2019, Auckland, New Zealand, November 26-29, 2019, Revised Selected Papers, Part II, ser. Lecture Notes in Computer Science, P. Palaiashnakote, G. S. di Baja, L. Wang, and W. Q. Yan, Eds., vol. 12047. Springer, 2019, pp. 307–320. [Online]. Available: https://doi.org/10.1007/978-3-030-41299-9_24

[17] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” 2017.

[18] Q. Wang, Y. Huang, W. Jia, X. He, M. Blumenstein, S. Lyu, and Y. Lu, “FACLSTM: convlstm with focused attention for scene text recognition,” Sci. China Inf. Sci., vol. 63, no. 2, p. 12103, 2020. [Online]. Available: https://doi.org/10.1007/s11432-019-2713-1

[19] Y. Peng, H. Tao, W. Li, H. Yuan, and T. Li, “Dynamic gesture recognition based on feature fusion network and variant convlstm,” IET Image Process., vol. 14, no. 11, pp. 2480–2486, 2020. [Online]. Available: https://doi.org/10.1049/iet-ipr.2019.1228

[20] W. Hu, H. Li, L. Tang, Y. Zhou, and Q. Du, “Spatial-spectral feature extraction via deep convlstm networks for hyperspectral image classification,” IEEE Trans. Geosci. Remote Sens., vol. 58, no. 6, pp. 4237–4250, 2020. [Online]. Available: https://doi.org/10.1109/TGRS.2019.2961947

[21] J. Huang, Y. Li, J. Tao, Z. Lian, and J. Yi, “End-to-end continuous emotion recognition from video using 3d convlstm networks,” in 2018 IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2018, Calgary, AB, Canada, April 15-20, 2018. IEEE, 2018, pp. 6837–6841. [Online]. Available: https://doi.org/10.1109/ICASSP.2018.8461963

[22] K. Zhou, Y. Zhu, and Y. Zhao, “A spatio-temporal deep architecture for surveillance event detection based on convlstm,” in 2017 IEEE Visual Communications and Image Processing, VCIP 2017, St. Petersburg, FL, USA, December 10-13, 2017. IEEE, 2017, pp. 1–4. [Online]. Available: https://doi.org/10.1109/VCIP.2017.8305063

[23] Q. Liang, Y. Wang, W. Nie, and Q. Li, “MVCLN: multi-view convolutional LSTM network for cross-media 3d shape recognition,” IEEE Access, vol. 8, pp. 139792–139802, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3021692

[24] C. Guo, W. Guo, C. Chen, X. Wang, and G. Liu, “The air quality prediction based on a convolutional LSTM network,” in Web Information Systems and Applications - 16th International Conference, WISA 2019, Qingdao, China, September 20-22, 2019, Proceedings, ser. Lecture Notes in Computer Science, W. Ni, X. Wang, W. Song, and Y. Li, Eds., vol. 11817, Springer, 2019, pp. 98–109. [Online]. Available: https://doi.org/10.1007/978-3-030-39552-7_12

[25] R. Miyoshi, N. Nagata, and M. Hashimoto, “Facial-expression recognition from video using enhanced convolutional lstm,” in 2019 Digital Image Computing: Techniques and Applications (DICTA), 2019, pp. 1–6.

[26] F. S. Langguth, “Machine learning techniques and optical systems for distant recognition from distant viewpoints,” PhD dissertation, University of Regensburg, Germany, 2020. [Online]. Available: https://epub.uni-regensburg.de/40548

[27] R. Giorgi, N. Bettin, S. Ermini, F. Montefoschi, and A. Rizzo, “An iris+voice recognition system for a smart doorbell,” in Proceedings of the 25th International Conference on Neural Information Processing Systems - Volume 1, ser. NIPS’12. Red Hook, NY, USA: Curran Associates Inc., 2012, pp. 1097–1105.
[32] H. Chen and G. S. Chirikjian, “Curvature: A signature for action recognition in video sequences,” in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition, CVPR Workshops 2020, Seattle, WA, USA, June 14-19, 2020*. IEEE, 2020, pp. 3752–3759. [Online]. Available: https://doi.org/10.1109/CVPRW50498.2020.00437

[33] C. Dalila, E. A. O. Badis, B. Saddek, and N. Amine, “Feature level fusion of face and voice biometrics systems using artificial neural network for personal recognition,” *Informatica (Slovenia)*, vol. 44, no. 1, 2020. [Online]. Available: http://www.informatica.si/index.php/informatica/article/view/2596