# Fingerprint Alterations Type Detection Using Deep Convolutional Neural Network

**Yahaya Isah Shehu**[1], **Ariel Ruiz-Garcia**[1], **Vasile Palade**[1] **and Anne James**[2]
1 Coventry University, Faculty of Engineering, Environment and Computing.
Priory Street, CV1 5FB, Coventry, UK
[2] Nottingham Trent University, Faculty of Science and Technology,
Clifton Campus, NG11 8NS, Nottingham, UK
shehuy2,ariel.ruiz-garcia,vasile.palade@uni.coventry.ac.uk,
anne.james@ntu.ac.uk

**Abstract.** Fingerprint alteration is a challenge that poses enormous security risks. As a result, many research efforts in the scientific community have attempted to address the issue. However, non-existence of publicly available datasets that contain obfuscation and distortion of fingerprints makes it difficult to identify the type of alteration and thus the study and development of mechanism to correct the alteration and correctly identify individuals. In this work we present the publicly available Coventry Fingerprints Dataset (CovFingDataset) with unique attributes such as: ten fingerprints for 611 different subjects, gender, hand and finger name for each image, among others. We also provide a total of 55,249 images with three levels of alteration for z-cut, obliteration and central rotation synthetic alterations, which are the most common types of obfuscation and distortion. Moreover, we propose a Convolutional Neural Network (CNN) to identify this type of alterations. The proposed CNN model achieves a classification accuracy rate of 98.55%. Results are also compared with a residual CNN model pre-trained on ImageNet which produces an accuracy of 99.88%.

**Keywords: Fingerprint alteration, Obfuscation, Distortion, CNN, Obliteration, Central rotation, z-cut**.

## 1 Introduction

The field of forensic science is concerned with the body of scientific knowledge and technical methods used to solve questions related to criminal, civil and administrative law. Fingerprint can be altered through abrading [12], cutting [15] and burning [7] among other obliteration where friction ridge patterns are altered into z-cut and obliteration. Distortion of fingerprint is the next common types of alteration where unusual and un natural changes in the patterns of the friction ridge such as skin grafting [16] in form of z-cut or central rotation are done.

In this work we present a novel fingerprint dataset with unique attributes such as gender, the names of the fingers like index finger, thumb, ring finger, middle finger and little finger of both left and right hand of the subject.

Furthermore, we present preliminary experimental results on alteration type detection using a deep CNN and a residual CNN model. The two models presented were able to classify the real from the altered fingerprints in addition to determining what sort of alteration is present in the fingerprints. The real fingerprint from the ConFingDataset presented has the total number of 6110 fingerprints from 611 subjects was synthetically altered into central rotation, z-cut and obliteration which are the common types of alteration with the total of 55,249 altered fingerprints. ConFingDataset is made publically available for replication and further experimental research work with the sole aim of improving up on the security of biometric fingerprint such that criminals in the watch-list can be identified and apprehended even if their fingerprints is altered.

Boarder Control is one of the major beneficiaries of biometric, where fingerprints are used to detect and recognises individual. Those that are having past criminal records and those that are in a high profile crimes used to undergo certain alteration of their fingerprint to avoid detection more especially in refugee and asylum seeker camp [2]. This mutilation comes in either burning the fingers or using surgery to cut some part of the fingers or body and placed them onto another finger (grafting), some comes in a Z-shape, rotated centrally of obliterated just to evade detection or linking the individual with their past [2].

Fingerprint of a little proportion of visitors visiting foreign countries are matched against a database of well-known criminals or a well-known terrorist [14]. The method helps in identifying and apprehending over 1000 wanted for felony crimes [14]. This is a sign that those wanting to hide their identity in pursuit of their criminal motives may alter their fingerprints in order to break border and enter into any country without their true identity being detected. However, it is significant important to have detects such alteration types and links the altered fingerprint images to their original ones. Furthermore, determining the alteration type is equally importance so that further investigation can be carried out on the subject that will be presented with such cases.

The fingerprint can be obliterated or mutilated to systematically evade identification by the biometric system [3]. Fingerprint can as well be altered or grafted to various patterns, shapes, sizes via surgical operation must of which comes in either a z-cut or central rotation other type of alteration can be achieved by burning the fingerprints 'obliteration' which in turn changes the fingerprint patterns that the biometric system uses to match and identifies individuals based on what is previously stored as the original fingerprint [4]. However, various software application and hardware solutions are proposed to tackle the situation [5] and [6] and yet there is still room for improvement. The issue of fingerprints alteration otherwise called obfuscation, which is the purposeful exertion of an individual of concealing his/her identity by altering ridge patterns of his/her fingerprint [7]. Generally the alterations are categorised into three fundamental classifications in view of the progressions made to the ridge patterns of the fingerprint i) obliteration or decimation ii) distortion or bending and iii) imitation or impersonation of fingerprint [7]. The most common alteration types based on the examination of ridge patterns presented by [7] are obliteration and distortion which makes up 89% and 10% respectively, we can also see that only 1% is reported as imitation. This shows that more of the alteration is either obliteration or distortion which we seek to address. In addition [7] their proposed algorithm and reported technique to identifying and detecting such fingerprint alteration achieve an accuracy of 66.4%. They also emphasize on lack of public available databases that comprises obliterated and distorted fingerprints for experimentation purposes to improve upon the detection alteration algorithms. The dataset used by [7] are not publically available as it is highly secured due to the sensitivity of the data and mostly is own by force agencies. This makes it difficult for the research community to proffer better solutions and robust detection or matching algorithm that can detect with high accuracy.

Techniques to generate synthetic altered fingerprints and to prove the utility of the generated dataset for developing, tuning and evaluating algorithms for altered fingerprint detection/matching were presented in [8]. The techniques focus on obliteration and distortion by considering the three most common alterations that are encountered in real situations such as burning obliteration, central rotation and z-cut. For each of the alteration, a parametric model was introduced to modify and input (real) fingerprint. After the main pattern modification, some noise (e.g. scars, blurring) was also introduced to create more realistic pattern. The position of the alteration is randomly chosen inside the fingerprint central area to cover the most distinctive fingerprint region, since the alteration intent is to obscure the fingerprint identity [8]. This is achieved by a tool called SynThetic fingeRprint AlteratioNs GEnerator (STRANGE) which is made publically available free to download [1].

Based on reports of previous study in the area of fingerprints alteration, analysis and detection, significant gap in knowledge is identified. Most especially in the study of Yoon et al. (2012), whose research contributions are case study compilation where automatic detection, classification and evaluation of altered fingerprint is done with the view of reducing the number of individual wanting to evade identification. However this study extends [7] in determining alteration types automatically as well as introduce a new fingerprint dataset comprising real fingerprints and altered fingerprints for experimental purposes and replication of other academics researches in fingerprint alteration detection algorithms. The dataset also has some attributes that can open more research ways due to its uniqueness in identifying gender, fingers and either a left hand or a right hand for which has received little or no attention in the past. These form the current research contribution to addressing alterations of fingerprint, using the specific sets of fingerprints dataset in addition to determining the alteration type.

## 2 Dataset

A total number of 6,110 real fingerprints collected out of which 6,000 fingerprints are provided for experimental and other academic research purposes, we therefore, uses a STRANGE tool that randomly select all the real fingerprints and categorized them into three Easy, Medium, and Hard real fingerprints and altered fingerprints as well. These categories are parameter tuned according to a quality threshold during fingerprint comparison [8]. The quality of the threshold is determined by the image resolution which by default is set to 500dbi. This is to allow us use maximum of the fingerprint images in conjunction with the STRANGE tool used for the alteration. These categories are parameters that are tuned according to the performance drop during fingerprint comparison. Furthermore, each category mentioned above is divided into three types of alteration i.e. obliteration, central rotation and z-cut. Each image will have three types of alteration in the three categories; hence each image was presented with six altered images.

The dataset is divided into fake and real fingerprints. A total of 5977 real fingerprints are altered using easy parameter setting while 5689 real fingerprints are altered as medium and finally a total of 4758 fingerprints real images are altered with hard parameter settings. Each of the three real fingerprint parameter settings produced three types of alteration obliteration, central rotation and z-cut). For instance 5977 real images produced 5977 obliterated fingerprints, 5977 central rotation and 5977 z-cut alteration. This means that for 5977 real fingerprints there is going to be 17,931 altered fingerprints presented as fake in easy category. Likewise in medium category a total number of 17,067 are presented as fake and finally, 14,274 fingerprints are fake in the hard category. However, for the purpose of training and testing of the convolutional model the alteration types of the fingerprint images are combined together irrespective of the category. A total of 55,249 (17,931 + 17067 + 14,274 + 5,977) fingerprint images are randomly divided into 50% training set (27628) and 50% testing set (27621). Figure 1 below shows a sample of real fingerprint from a left hand of one subject

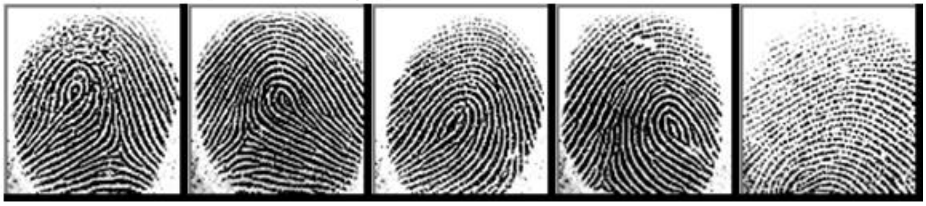

**Fig. 1.** Sample of real left hand of one subject.

After applying STRANGE tool for the three types of alterations figure 2 below display the altered fingerprint of the left hand of the same subject in figure 1.

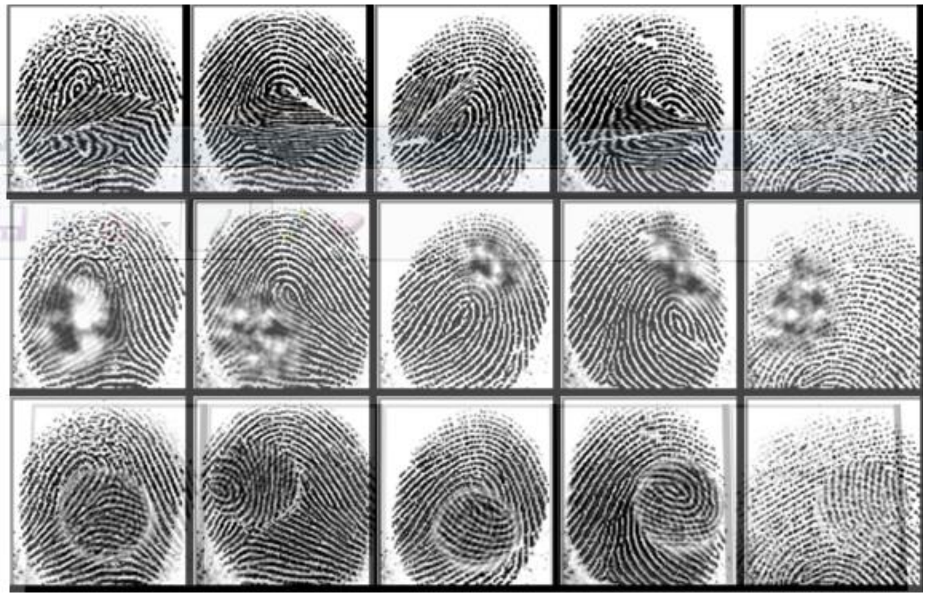

**Fig. 2.** Sample of altered left hand fingerprint into z-cut, obliteration and central rotation respectively of the same subject.

## 3 Methodology and Experimental Setup

In this work we propose a deep CNN for feature extraction and classification. Deep CNN have proven to be efficient in image processing related task and therefore are suitable for detecting fingerprints alteration types. We train and evaluate this model on the real and synthetically altered images of the CovFingDataset described above. Each class, including real images, is randomly split into 50% training and 50% testing subsets. The images are also resized to 200 x 200 using bipoloar interpolation.

### 3.1 Convolutional Neural Network

Convolutional neural networks retain spatial information through filter kernels. In this work we exploit this unique ability of CNN to train a model to classify images from the CovFingDataset into four categories: central rotation, obliteration, z-cut and real. Where real images are those without any alterations.

The deep CNN model has five convolutional layers with 20 3x3, 40 3x3, 60 3x3, 80 3x3 filter kernels. All convolutional layers use a stride of one and zero padding of size two. Moreover, the output of every convolutional layer is shaped by a rectifier linear unit (ReLU) function. Max pooling is applied to the first three convolutional layers for dimensionality reduction. e convolutional layers are followed by two fully connected layers with1000 and 100 hidden units respectively. Furthermore we employ batch normalization to standardize the distribution of each input feature across all the layers and thus speed up training and avoid exploding gradients[11].

The deep CNN is trained using stochastic gradient decent (SGD) and nesterov momentum of 0.5. We trained on min batches of size 70 and set the learning rate, *LR*, to 0.01. *LR* was decayed with a factor of 0.01 according to:

$$LR = \frac{\lambda}{1+(\omega\times\theta\,)} \tag{1}$$

where $\lambda$ denotes the initial $LR$, $\omega$ the decay factor and $\theta$ the current epoch. The loss is defined by a SoftMax operator and the cross-entropy *y* is determined according to:

$$y = -x_c + \log\left(\sum_j \exp(x_j)\right) \tag{2}$$

where *c* is the class ground-truth. Training was done for 100 epochs as further training led to overfitting.

### 3.2 Residual Convolutional Neural Network

Residual Neural Networks (ResNets) have been demonstrated to be an exceptionally effective model on image classification [9]. ResNets have an identity shortcut connection that allows for very deep architectures to be trained, and thus more complex features to be learned leading to improved classification performance. For this reason we decided to compare our model with a ResNet18, that is 18 parametrized convolutional layers, provided by [17], [18].

This network was originally trained and evaluated on ImageNet. The authors also provide deeper architectures, of up to 200 layers, pre-trained on the same dataset. However, because fingerprint images have a relatively smaller number of features and the nature of the problem being addressed here is not as complex as classifying ImageNet which has 1000 classes, we did not consider deeper architectures.

The ResNet18 model is fine-tuned on the training subset of the CovFingDataset presented in this paper for only 5 epochs. No modifications were done to the network other than replacement of the output layer to only predict four classes. Training was also done using SGD, a nesterov momentum of 0.75 and learning rate of 0.001. This is then evaluated on the test subsect.

## 4 Results and Discussion

The confusion matrixes below show the total number of each alteration types detected and also the number of fingerprint images misclassified. The result is presented in table

2 and table 3 with the three types of alteration, the real fingerprint images and the percentage accuracy of the detection of the alteration types.

**Table 1.** Confusion Matrix of our CNN.

| Central Rotation | Obliteration | Real | Z-cut | Accuracy (%) |
|---|---|---|---|---|
| 7995 | 33 | 0 | 183 | 97.37 |
| 19 | 8148 | 0 | 44 | 99.23 |
| 0 | 0 | 2988 | 0 | 100 |
| 116 | 6 | 0 | 8089 | 98.51 |
| 98.34% | 99.52% | 100% | 97.27% | 98.55 |

**Table 2.** Confusion Matrix of the pre-trained and fine-tuned ResNet18

| Central Rotation | Obliteration | Real | Z-cut | Accuracy (%) |
|---|---|---|---|---|
| 8206 | 1 | 1 | 3 | 99.94 |
| 0 | 8195 | 15 | 1 | 99.81 |
| 0 | 0 | 2986 | 2 | 99.93 |
| 4 | 0 | 11 | 8196 | 99.82 |
| 99.95% | 99.98% | 99.10% | 99.93% | 99.86 |

As indicated in table 2, 2988 cases of real fingerprint images are correctly classified as real fingerprints. This corresponds to 100% of all fingerprints. The proposed model was able to detect and classify the entire real fingerprints correctly with no false alarm. However, 98.55% of the overall predictions are correct. In addition, 183 altered fingerprint images in central rotation are mixed up with z-cut alteration and 116 z-cut altered fingerprint images are mixed up as central rotation. This is because some of the angles in the parameter setting of the tool used rotates the altered part of the images in a similar pattern coupled with the ridges pattern (radial and ulnar loop) Radial loop is a loop that comes from the side of the thumb and looped out to the pinky side of the hand, while ulnar is the opposite i.e. from the pinky side of the hand toward the thumb of the fingerprint images [10]. These angle rotation contributed to the misclassification of the alteration between the central rotation and z-cut which result in getting a high number of up to 183 and 116 altered fingerprint images presented as z-cut and central rotation respectively.

The two CNN model achieved a high accuracy in the classification of altered fingerprint. Nevertheless some misclassified fingerprints are also presented with a minimal percentage of 1.45% and 0.14% of the two models. The figures below depict some of the misclassified fingerprints.

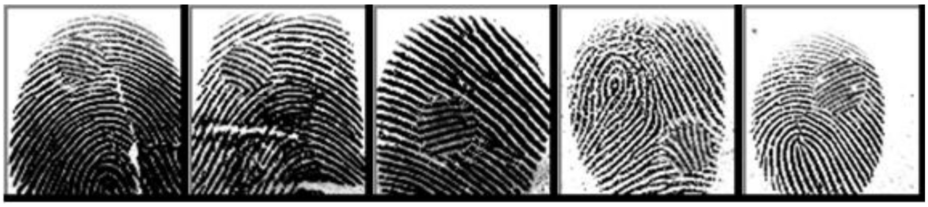

**Fig. 3.** Central rotation misclassified as z-cut

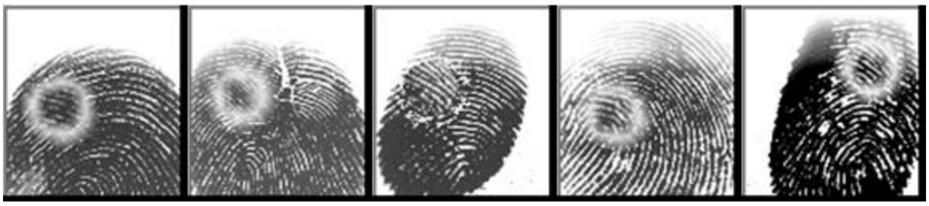

**Fig. 4.** Central rotation misclassified as obliteration

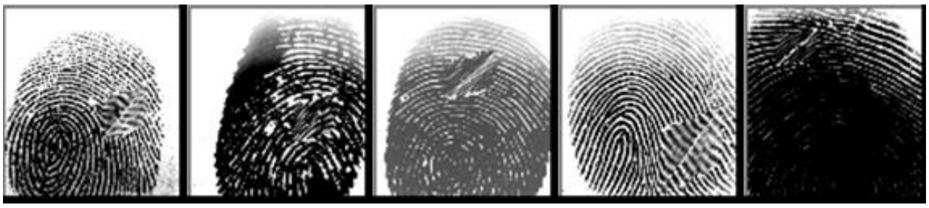

**Fig. 5.** z-cut misclassified as obliteration

From the misclassified fingerprint figures 3 and 4,e can see from the figures that the easy alteration category fingerprints are misclassified more by the CNN model because they physically appeared with little proportion of the fingerprints altered, then followed by the medium category. The hard category fingerprints are less misclassified unless with the case of patterns rotational degrees that mixed central rotation with z-cut.

Table 3 shows the pre-trained confusion matrix that achieves a global accuracy of 99.86% with a difference in misclassification of the real images. It misclassifies 2 fingerprint images as z-cut while the proposed CNN model classifies all the real fingerprint images correctly. Furthermore, 15 of the obliterated fingerprint images are misclassifies as real while 11 z-cut altered fingerprint are also misclassifies as real. This may be because some of the real images are not of good quality and looks very close to obliteration. However, some loop ridges in the fingerprint when rotated to some certain degrees might result into some pattern changes that might look like z-cut shape hence classify them as z-cut. In addition, there exist some natural cut in some of the fingerprints which the models equally detect as a z-cut (shown in figure 3 central rotation classified as z-cut). Some fingerprints also appeared to look blurring and haze which the model classified as obliteration (indicated in figure 4 where central rotation are misclassified as obliteration). Figure 5 shows altered z-cut fingerprint classified as obliteration because of the blurring defect of the real fingerprint at the top most of the images. As some of the images are from female fingers we cannot also ruled out the possibility of them wearing henna as shown in the last image of figure 5.

Evaluating the confusion matrixes above we found that the precision rate of central rotation is 97.37% and 99.94% of the pre-trained model. This shows that the pre-trained model performs better in terms of detecting altered images with central rotation alteration type. Likewise it also does better in the recall with an accuracy of 99.95% against 98.34%. The Pre-trained model performs better in almost all the alteration types' detection. However, it really get confused with separating the real images with the altered once even though the detection accuracy is high with a precision of 99.93% and recall of 99.10% , but the CNN model does better with 100% detection of both precision and recall.

Selvarani et al. (2014) uses singular points to distinguish between real fingerprint and altered ones by extracting set of features from the ridge orientation field of an input fingerprint and then apply a fuzzy classifier to classify it into real or altered 'z-cut' and also the alteration type [19], [20]. [21] have developed algorithm that classify and detect altered fingerprint z-cut and central rotation only using extracted features and support vector classifier and it was tested using synthetic fingerprints and achieved 92% accuracy above the well-known fingerprint quality software, NFIQ as it only recognised 20% of the altered fingerprints. We cannot therefore, provide a comparison on other alterations since to the best of our knowledge no one has done work on detecting these three types of alteration together.

One of the main advantages of the deep CNN proposed in this work is that the ResNet18 was pre-trained on the ImageNet dataset which has over one million images spanning over 100 classes. Compared to our model which only was trained on our dataset and for 100 epochs. Our model also has a significantly smaller number of convolutional layers, and thus an exponentially smaller number of hyperparameters. Moreover, because the CNN proposed here has a precision and recall score of 100% on real images, it can be more suitable for use in applications where detecting whether a fingerprint has been altered or not. Furthermore, the performance of the ResNet models provided by [17] heavily relies on the image pre-processing steps such as aspect ratio resizing and luminance adjustments.

## 5 Conclusion

Fingerprint alteration detection is still an issue that requires more attention in detecting and identifying altered fingerprints. In this work we have presented a novel fingerprints dataset, CovFingDataset, for research accessibility. We highlighted the importance for fingerprint alteration research and the need for digital automatic detection of altered fingerprints. We also discussed the most common types of obfuscation and distortion; central rotation, obliteration and z-cut. The dataset presented includes three different levels of alteration for each one of these types. Furthermore, the novel dataset presented in this work has number of unique attributes such as the name of the fingers of which hand does the fingers belongs to as well as the gender of the fingerprint. We have also proposed a CNN model that is not only able to detect whether a fingerprint has been altered or not but also detect the type of alteration. The CNN proposed achieve an accuracy rate of 98.55% on the testing subset of the CovFingDataset. This was compared against a ResNet18 model pre-trained on ImageNet and fine-tuned and tested on our dataset, achieving a state-of-the-art accuracy rate of 99.86. One of the main differences in performance for our model and the ResNet18 model was that even though the ResNet18 slightly outperformed our model, our model achieved a precision and recall score of 100% on real images, thus making it more suitable for real-time applications.

To the best of the authors' knowledge, no prior work has addressed these three types of alterations. However, one of the limitations of this work is that the proposed CNN was evaluated on synthetically altered images due to the lack of publicly available datasets containing actual altered images. Nonetheless, we hope that the results presented in this work can serve as a benchmark in identifying fingerprint alterations and hope that the novel dataset presented can assist the research community in developing more robust biometric fingerprint technology for the automatic detection of altered fingerprint.

Future work will also investigate the reasons why the ResNet18 model confuses non-altered fingerprints with altered ones. Moreover, we will also test our model on different datasets with different alteration types to see if it retains 100% precision and recall scores on real images.

## References

1. Biolab.csr.unibo.it. (2018). Biometric System Laboratory. [online] Available at: <http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=211&pathSubj=111%7C%7C21%7C%7C211&Req=&> [Accessed 3 Apr. 2018].
2. Petrovici, A., 2012, September. Simulating alteration on fingerprint images. In Biometric Measurements and Systems for Security and Medical Applications (BIOMS), 2012 IEEE Workshop on (pp. 1-5). IEEE.
3. Cummins, H., 1934. Attempts to alter and obliterate finger-prints. Am. Inst. Crim. L. & Criminology, 25, p.982
4. Feng, J., Jain, A.K. and Ross, A., 2010, August. Detecting altered fingerprints. In Pattern Recognition (ICPR), 2010 20th International Conference on (pp. 1622-1625). IEEE.
5. Antonelli, A., Cappelli, R., Maio, D. and Maltoni, D., 2006. Fake finger detection by skin distortion analysis. IEEE Transactions on Information Forensics and Security, 1(3), pp.360-373
6. Nixon, K.A. and Rowe, R.K., 2005, March. Multispectral fingerprint imaging for spoof detection. In Biometric Technology for Human Identification II (Vol. 5779, pp. 214-226). International Society for Optics and Photonics
7. Yoon, S., Feng, J. and Jain, A.K., 2012. Altered fingerprints: Analysis and detection. IEEE transactions on pattern analysis and machine intelligence, 34(3), pp.451-464.

8. Papi, S., Ferrara, M., Maltoni, D. and Anthonioz, A., 2016, September. On the Generation of Synthetic Fingerprint Alterations. In Biometrics Special Interest Group (BIOSIG), 2016 International Conference of the (pp. 1-6). IEEE
9. Szegedy, C., Ioffe, S., Vanhoucke, V. and Alemi, A.A., 2017, February. Inception-v4, inception-resnet and the impact of residual connections on learning. In AAAI (Vol. 4, p. 12).
10. Maio, D. and Maltoni, D., 1996, August. A structural approach to fingerprint classification. In Pattern Recognition, 1996., Proceedings of the 13th International Conference on (Vol. 3, pp. 578-585). IEEE.
11. Ioffe, S. and Szegedy, C., 2015. Batch normalization: Accelerating deep network training by reducing internal covariate shift. arXiv preprint arXiv:1502.03167.
12. Burks Jr, J.W., 1958. The Effect of Dermabrasion on Fingerprints. AMA Arch. Derm, 77, pp.8-11.
13. Müller, H., Müller, W., Squire, D.M., Marchand-Maillet, S. and Pun, T., 2001. Performance evaluation in content-based image retrieval: overview and proposals. Pattern Recognition Letters, 22(5), pp.593-601
14. Salter, M.B., 2004. Passports, Mobility, and Security: How smart can the border be?. International studies perspectives, 5(1), pp.71-91.
15. Cummins, H., 1934. Attempts to alter and obliterate finger-prints. Am. Inst. Crim. L. & Criminology, 25, p.982.
16. Wertheim, K., 1998. An extreme case of fingerprint mutilation. Journal of Forensic Identification, 48(4), p.466.
17. He, K., Zhang, X., Ren, S. and Sun, J., 2016. Deep residual learning for image recognition. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 770-778).
18. GitHub. (2018). facebook/fb.resnet.torch. [online] Available at: https://github.com/facebook/fb.resnet.torch [Accessed 29 Apr. 2018].
19. Selvarani, S.M.C.A., Jebapriya, S. and Mary, R.S., 2014, March. Automatic Identification and Detection of Altered Fingerprints. In Intelligent Computing Applications (ICICA), 2014 International Conference on (pp. 239-243). IEEE
20. Feng, J., Jain, A.K. and Ross, A., 2010, August. Detecting altered fingerprints. In Pattern Recognition (ICPR), 2010 20th International Conference on (pp. 1622-1625). IEEE
21. Yoon, S., Zhao, Q. and Jain, A.K., 2012, March. On matching altered fingerprints. In Biometrics (ICB), 2012 5th IAPR International Conference on (pp. 222-229). IEEE.