e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

SECURITY CHALLENGES AND PROBLEMS IN FINGE RPRINTS

Asmita Parab[*1]

[*1]Department Of Information Technology, B.K. Birla (Autonomous) College,
Kalyan – 421301, Maharashtra, India.

ABSTRACT

The need for comprehensive security in applications like national ID cards, border crossings, government benefits, and access control means that traditional methods of human identification, which rely on credentials like identification documents and PINs, fall short. Biometric recognition, based on individuals' unique physiological and behavioral traits, is growing more popular as a solution to these problems. Biometrics advantages include resistance to loss, theft, or forgery. Examples of biometrics include fingerprints, facial features, and iris scans. Although biometrics have a history of being successful in law enforcement, as they grow more common, they face new difficulties. Depending on the application's requirements, such as accuracy, throughput, user acceptance, security, resilience, and return on investment, biometric technology's effectiveness varies. The management of low-quality or incomplete data, scalability for millions of users, interoperability, privacy protection, cost reduction, and system integrity enhancement are challenges that the next generation of biometric technology must overcome. In conclusion, biometrics offer a promising way to improve security and dependability in a variety of identification applications. To solve the difficult challenges of the future, such as enhancing accuracy, ensuring data quality, and protecting user privacy while retaining cost-effectiveness and system integrity, this technology will need to evolve to get past its current constraints.

Keywords: Fingerprints, Biometrics, Accuracy, Security, Privacy.

I. INTRODUCTION

Biometric recognition is based on two basic assumptions regarding body characteristics: distinctive character and durability. Applicability and accuracy of product identification The biometric feature essentially depends on the extent to which these two premises apply to the population's hands. Fingerprints, face, and iris are among the most commonly used physiological features. Commercial biometric systems and fingerprints cover over 50% of the civilian market shares. The uniqueness and permanence of many behavioral traits proposed in the literature (e.g. signature, gait, and keystroke dynamics) is weak. As such many To date, operating systems based on these functions have been shipped. Pick a specific one The biometric mode generally depends on the type and requirements of the intended identification application. For example, voice biometrics are useful for authentication applications because the phone's voice pick-up sensor (microphone) is already built-in. The fingerprint has since become the most popular biometric for logging into laptops, cell phones, and PDAs. mall and inexpensive fingerprint sensors can easily be installed in these devices. Some, like hand geometry, are better suited for verification applications (1:1).), while others such as fingerprint, iris, and face have sufficient distinctiveness to be used for large-scale identification applications (1:N matching). One of the unique apps biometric data are negatively identified, that is, the person is not what he already was registered/registered in the system. Negative identification is required to avoid multiple registrations by the same person, which is necessary for large-scale biometric applications, e.g. B. Benefits from government-sponsored programs. Therefore during the verification processes, traceability is required for negative identification now briefly introduce some popular biometric methods.

1.1 Projections from Biometrics Technologies:

Biometric technologies are in high demand and used in various industries including security, finance, healthcare, and even personal devices. With their ability to uniquely identify individuals based on their physiological or behavioral characteristics such as fingerprints, facial features, iris patterns, and even voice, different expectations and potential outcomes are associated with biometric technologies:

Improved security:

One of the main expectations of biometrics is improved security. Biometric authentication provides a more reliable and secure way of verifying an individual's identity than traditional methods such as a password or

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

PIN. This is especially important in industries like banking, where protecting sensitive financial information is paramount.

Convenience:

Biometric technologies are practical. Users no longer need to remember complex passwords or carry physical tokens; They can simply use their unique biometrics to authenticate themselves. This convenience applies to a wide range of applications, from unlocking smartphones to accessing protected objects.

Fraud Prevention:

Biometrics can significantly reduce fraud. For example, fingerprint or facial recognition systems can thwart attempts at identity theft by ensuring that only authorized individuals have access to sensitive accounts or data.

Efficiency:

Biometric systems can streamline processes and improve efficiency. In healthcare, for example, identifying patients using biometric data can reduce errors, simplify record-keeping, and improve the overall quality of care.

Personalization:

Biometrics enable a more personalized user experience. Smart devices can adjust their settings and preferences based on the recognized user, providing personalized services and content.

Reduce password problems:

Password problems, such as forgetting or resetting your password, can be eliminated with biometrics. This not only saves time but also reduces support and operational costs.

Forensic and law enforcement applications:

In forensic and law enforcement applications, biometrics play a key role in criminal investigations. Expectations include enhanced crime-solving capabilities based on fingerprint, facial, and DNA analysis.

Privacy Issues:

While expectations are high for biometrics, there are also privacy and data security concerns. To ensure that biometric data is stored and used responsibly, a balance needs to be struck between convenience and privacy.

1.2 First Generation Fingerprints:

First-generation fingerprinting refers to traditional ink and paper fingerprinting methods that have been in use for over a century. In these methods, a person's fingerprints are taken by applying ink to the fingers and then printing them onto a paper card to create a permanent record of unique fingerprint patterns. Here are some key points about first-generation fingerprinting:

Ink and paper:

This method uses fingerprint ink, usually black or blue, and special paper or cardboard fingerprint cards.

Fingerprint patterns: Fingerprint patterns are unique to each person and come in three main types: arcs, rings, and spirals. These templates help with fingerprint classification and identification.

Rolling technique:

To capture fingerprints, ink is first applied to the fingers and then each finger is moved from one edge of the nail to the other on the fingerprint card. This rolling technique ensures that the entire fingerprint pattern is registered.

Individual Cards:

Each fingerprint is typically recorded on a separate section of the card, with space for both rolled and individual fingerprints. This preserves the uniqueness of each fingerprint.

Manual processing:

First-generation fingerprint cards require manual processing and verification by qualified fingerprint experts to identify and match fingerprints. This process can be time-consuming and prone to human error.

Historical Significance: First-generation fingerprints have long been used in law enforcement and forensics. It is an invaluable tool for identifying people, solving crimes, and verifying identities.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

Limitations:

Although the first generation of fingerprint recognition is a reliable and well-established method, it can cause smearing and other problems that can affect print quality.

Also, manual processing can be time-consuming and cards can expire over time. In recent years, fingerprinting methods such as Real-time fingerprinting, for example, have become increasingly important due to their speed, accuracy, and ability to create electronic records that can be easily stored and shared. However, first-generation ink and paper fingerprinting remains an important tool in law enforcement and forensic investigations, particularly in situations where electronic methods are not available or practical.

1.3 Second Generation Fingerprint:

Second-generation fingerprinting refers to fingerprinting methods that evolved from the traditional ink-paper techniques used for first-generation fingerprinting. These methods use advanced technology to electronically collect, store, and analyze fingerprint data. Here are some key points about second-generation fingerprinting:

Fingerprint:

Second-generation fingerprints are based on digital sensors, commonly referred to as "live scan" devices, that capture high-resolution fingerprint images without the need for ink or paper.

Fast and Accurate:

Fingerprint recognition is faster and more accurate than first-generation methods. Eliminate ink contamination and the risk of smearing, resulting in clearer and more reliable fingerprint data.

Electronic Storage:

Instead of physical fingerprint cards, fingerprints are stored electronically in databases, making it easier to search, retrieve, and share that data for various purposes, including law enforcement and background checks.

Automatic matching:

Fingerprint systems often use automated algorithms to match fingerprints, reducing the need for manual expert checks. This improves the speed and accuracy of the identification processes.

Versatile:

Second-generation fingerprints can be integrated into various systems such as access control, mobile devices, and biometric authentication applications, increasing security and convenience.

Enhanced Forensics:

Fingerprint technology enhances forensic analysis by allowing experts to get closer to the specific characteristics of fingerprints to aid in criminal investigations.

Biometric Verification:

Many modern smartphones and devices use fingerprint sensors to verify your identity and ensure secure login.

Privacy and security issues:

As with all biometric data, the storage and security of fingerprints raise privacy and security issues.

1.4 Biometric System Security

The security of implemented biometric systems can be compromised number e.g studies analyzed the likelihood of such security breaches and possible countermeasures for these deviations. General Analysis of a Biometric System for Risk Assessment Article specifies the extent to which a fraudster may compromise the security of biometric data. Although many of these attacks apply to any information system, the attacks are numbers using fake biometrics and template changes are unique to biometric systems. Let's discuss briefly the Characteristics of such attacks, which must be countered successfully in the second generation biometric systems.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

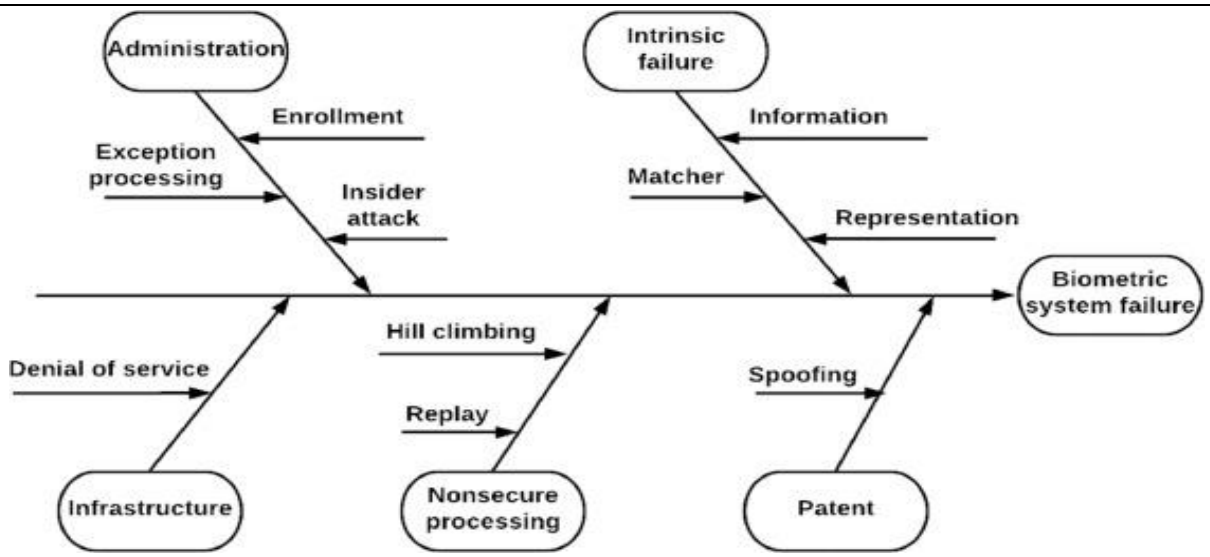

Figure 1: Biometric System

Sensor Level Attack:

A fake biometric sample can be presented to gain access to the sensor. Covert capture of biometric features can generate fake biometric data from real users, for example through fingerprints of objects touched by people.

Repeat Attack:

The opponent may intercept or capture the digital copy that records the biometric sample and reproduce this signal, bypassing the biometric sensor.

The Trojan Horse1 Attack:

The extractor function can be replaced by the program that generates sets of desired functions.

Manipulation of features: Feature vectors generated from biometric samples are replaced by a set of synthesized (wrong) functions.

Attack on the relevant device:

The relevant device may also be subject to a Trojan horse attack that generates high (or low) match scores regardless of which user is presenting the biometric sensor.

Pattern Attack:

A pattern generated at user registration/registration may be used archived locally or in a central location. This type of attack can alter the file Save the saved template or replace it with a new template.

Attack on communication channels:

Data sent through communication channels can be eavesdropped on for malicious purposes, then modified and re-entered the system.

Attack on the decision engine:

It is possible to make the final decision generated by the biometric system should be replaced by a Trojan horse program.

1.5 Biometric Alteration and Spoof Detection:

Biometrics, which rely on unique physiological or behavioral characteristics for identification, are becoming more common in security systems and personal devices. However, as biometric technology advances, so do the techniques used to alter or mimic these systems, leading to security issues. Biometric data modification and counterfeit detection are critical to maintaining the integrity and trustworthiness of biometric systems.

Biometric Alteration:

Biometric manipulation includes attempting to alter or tamper with an individual's biometric information to gain unauthorized access or to impersonate another person. For example, criminals can use a variety of methods to alter fingerprints or facial features to trick biometric systems.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

Spoof Detection:

Spoof Detection is the process of identifying and preventing attempts to deceive biometric systems by fraudulent means. This includes detecting when someone uses a fingerprint, photo, fake voice recording, or other impersonation techniques to gain access.

Importance:

Biometric tampering and counterfeit detection are critical to ensure the security and reliability of biometric authentication systems. Failure to detect these attempts could result in unauthorized access, identity theft, or other security breaches. To address this problem, advanced algorithms and technologies such as activity tracking have been developed to distinguish genuine biometric data from fake or altered representations.

Detection methods:

Recognition methods may include analysis of indicators of vitality (e.g. detecting a pulse or movement in a fingerprint), checking the consistency of biometric data with other contextual information (e.g. recognizing faces in different lighting conditions), and using machine learning algorithms for identification including anomalies. in biometric models.

II. METHODOLOGY

STEP 1:

In the first step, Python code is a script designed to traverse through a specified source folder (named "IRIS and FINGERPRINT DATASET") and its subfolders. It checks if any of these subfolders contain a folder named "Fingerprint". If found, it proceeds to copy the files from that "Fingerprint" subfolder to a specified destination folder (named "Finger data"). Before starting the traversal, the script first checks if the destination folder exists. If it doesn't, the script creates it using `os. makedirs(destination_folder)`. The `os. walk()` function is employed to recursively explore the contents of the source folder. It returns a tuple for each directory it encounters, consisting of the directory path, a list of subdirectories, and a list of files. Within the loop, it checks if "Fingerprint" is in the list of subdirectories (`dirs`). If true, it constructs the path to the "Fingerprint" subfolder using `os.path.join()`. It then iterates through the files in the "Fingerprint" subfolder and uses `shutil. copy()` to copy them to the destination folder. Each file's source and destination paths are constructed using `os.path.join()`. Throughout the process, it prints out a message indicating which file is being copied. Finally, after all images have been copied, it prints a message to signal the completion of the operation.

STEP 2:

In this step, Python code is a script designed to convert BMP images to either JPG or PNG format. It begins by importing the necessary modules, namely `os` for file operations and `cv2` (OpenCV) for image processing. The script defines two directory paths: `source_dir` and `destination_dir`, which respectively represent the source directory containing BMP images ("data") and the directory where the converted images will be saved ("data2"). Before the conversion process begins, the script checks if the destination directory exists. If it doesn't, the script creates it using `os.makedirs(destination_dir)`. The code then defines a function `convert_bmp_to_jpg_or_png` which takes a source path (`src_path`) and a destination path (`dest_path`). Inside the function, it uses OpenCV (`cv2`) to read the BMP image, and then saves it in the specified destination path, effectively converting it to JPG or PNG format. The script then uses a loop to traverse through the files in the source directory. For each file, it checks if the file extension is ".bmp" using `file. lower().ends with (".bmp")`. If true, it constructs the source and destination paths. It then calls the `convert_bmp_to_jpg_or_png` function to perform the conversion. Finally, after all BMP images have been converted, it prints a completion message indicating that the conversion process has finished and specifies the directory where the converted images can be found ("data2").

STEP 3:

This Python script utilizes the TensorFlow and Keras libraries to build, train, and save a Convolutional Neural Network (CNN) for fingerprint detection. It begins by importing the necessary modules, including TensorFlow and its components, and numpy for numerical operations. The script defines a directory path (`data2_dir`) pointing to a directory containing JPG and PNG images. It then sets various parameters for the CNN, such as the input shape (which depends on the dimensions of the images), batch size, number of epochs for training, and

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

learning rate. A function `load_and_preprocess_images` is defined to load images from file paths, resize them to match the specified input shape, normalize pixel values, and extract labels from the file names. This function returns two arrays: one containing the processed images and the other containing their corresponding labels. The script then loads and preprocesses images from the specified directory (`data2_dir`). It constructs a list of image paths and applies the `load_and_preprocess_images` function to obtain the processed images and labels.

Next, the data is split into training and validation sets using a specified split ratio. The CNN model is constructed using Keras, comprising several convolutional and pooling layers, as well as dense layers for classification. The model is then compiled with an optimizer (Adam), a loss function (binary cross-entropy for binary classification), and a metric for evaluation (accuracy). The model is trained using the training data, and the training process is tracked through the `history` object. After training, the model is saved to a file named "fingerprint_detection_model.h5".

Finally, the script prints a message indicating that the model has been trained and saved. This code essentially creates and trains a CNN for fingerprint detection, providing a foundation for further use in applications like image recognition or security systems. The output for the same with its epoch is as follows:

```
Epoch 1/10
12/12 [==============================] - 5s 323ms/step - loss: -164.2461 - accuracy: 0.0250 -
val_loss: -420.2875 - val_accuracy: 0.0000e+00
Epoch 2/10
12/12 [==============================] - 4s 314ms/step - loss: -1184.8085 - accuracy: 0.0278 -
val_loss: -1938.7061 - val_accuracy: 0.0000e+00
Epoch 3/10
12/12 [==============================] - 4s 328ms/step - loss: -4558.8042 - accuracy: 0.0278 -
val_loss: -6720.7100 - val_accuracy: 0.0000e+00
Epoch 4/10
12/12 [==============================] - 4s 310ms/step - loss: -14648.6260 - accuracy: 0.0278 -
val_loss: -19868.6074 - val_accuracy: 0.0000e+00
Epoch 5/10
12/12 [==============================] - 4s 306ms/step - loss: -39580.4102 - accuracy: 0.0278 -
val_loss: -51864.5391 - val_accuracy: 0.0000e+00
Epoch 6/10
12/12 [==============================] - 4s 348ms/step - loss: -96767.7344 - accuracy: 0.0278 -
val_loss: -121314.5469 - val_accuracy: 0.0000e+00
Epoch 7/10
12/12 [==============================] - 4s 352ms/step - loss: -224151.9062 - accuracy: 0.0278 -
val_loss: -261617.4844 - val_accuracy: 0.0000e+00
Epoch 8/10
12/12 [==============================] - 4s 364ms/step - loss: -464277.1875 - accuracy: 0.0278 -
val_loss: -521179.0625 - val_accuracy: 0.0000e+00
Epoch 9/10
12/12 [==============================] - 4s 358ms/step - loss: -890503.1875 - accuracy: 0.0278 -
val_loss: -969509.1250 - val_accuracy: 0.0000e+00
Epoch 10/10
12/12 [==============================] - 4s 344ms/step - loss: -1601161.2500 - accuracy: 0.0278 -
val_loss: -1712983.1250 - val_accuracy: 0.0000e+00
Fingerprint detection model trained and saved.
```

Figure 2: Fingerprint detection model compilation

STEP 4:

This Python script employs TensorFlow and Keras to perform predictions using a previously trained fingerprint detection model. It begins by importing the necessary libraries, including TensorFlow for machine learning operations and Keras for building and training neural networks. The script also imports functions for image processing from the Keras preprocessing module. The code defines a directory path (`test_dir`) which is assumed to contain the test images for which we want to make predictions.

The function `load_and_preprocess_test_images` is defined to load and preprocess test images. It takes a list of image paths and an input shape as arguments. The function reads each image, resizes it to the specified input shape, converts it to an array, and normalizes pixel values to be within the range of [0, 1]. The processed images are then returned as a NumPy array. The trained fingerprint detection model is loaded using `keras.models.load_model` from the saved model file ("fingerprint_detection_model.h5"). It is then compiled with `model.compile(run_eagerly=True)`.

A list of image file paths in the test directory is obtained using a list comprehension. This list is then used to load and preprocess the test images using the previously defined function. The script then makes predictions on the preprocessed test images using `model. predict`. The resulting `predictions` variable contains the model's output for each test image.

e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

Finally, the script prints the predictions. It iterates through the predictions using a loop, assuming a binary classification scenario where class 1 represents the positive class (fingerprint detected). For each prediction, it prints the image number and the probability of it belonging to the positive class. In summary, this code snippet is designed to load a pre-trained fingerprint detection model, process test images, and output predictions for each test image, indicating the probability of it being classified as a positive case.

```
1/1 [==============================] - 0s 94ms/step
Image 1: Probability of being positive class (1): 1.0
Image 2: Probability of being positive class (1): 1.0
Image 3: Probability of being positive class (1): 1.0
Image 4: Probability of being positive class (1): 1.0
Image 5: Probability of being positive class (1): 1.0
Image 6: Probability of being positive class (1): 1.0
Image 7: Probability of being positive class (1): 1.0
Image 8: Probability of being positive class (1): 1.0
Image 9: Probability of being positive class (1): 1.0
Image 10: Probability of being positive class (1): 1.0
Image 11: Probability of being positive class (1): 1.0
Image 12: Probability of being positive class (1): 1.0
Image 13: Probability of being positive class (1): 1.0
```

Figure 3: Probability output of Images

III. RESULTS AND DISCUSSION

In the Training phase, the model extracts the fingerprint image of a person 13 from real and 4 images from the forged dataset. And use the features of these images as a training dataset for the model.

In the testing phase, 13 fingerprints are taken for training and testing.

Here is a confusion matrix of the testing data:

Table 1: Confusion matrix

N = 13	Predicted YES	Predicted NO
Actual YES	8	5
Actual NO	6	4

IV. CONCLUSION

As biometric security (Fingerprint) becomes commonplace on smartphones, addressing potential vulnerabilities is crucial. While some weaknesses, like using fake samples, have been studied, there's still much to explore. It's essential to establish secure communication between different components of the system and devise effective measures to prevent biometric impersonation. Through a mixed-methods approach, ethical considerations, and acknowledgment of potential limitations, this study aims to contribute valuable insights toward enhancing the security of fingerprint recognition systems. This ongoing research is paramount in ensuring the safety of our smartphones and protecting the sensitive information they hold from potential threats.

ACKNOWLEDGEMENTS

I would like to thank my professors and friends for supporting me in this research. I am delighted to contribute my efforts in this field and I hope this paper helps further research and bring valuable insights for the researchers.

V. REFERENCES

[1] Zheng, G.; Fang, G.; Shankaran, R.; Orgun, M.A.; Zhou, J.; Qiao, L.; Saleem, K. Multiple ECG fiducial points-based random binary sequence generation for securing wireless body area networks. IEEE J. Biomed. Health Inf. 2017, 21, 655–663.

[2] Zheng, G.; Fang, G.; Shankaran, R.; Orgun, M.A. Encryption for implantable medical devices using modified one-time pads. IEEE Access 2015, 3, 825–836.

[3] Awad, A.I.; Hassanien, A.E.; Zawbaa, H.M. A Cattle Identification Approach Using Live Captured Muzzle Print Images. In Advances in Security of Information and Communication Networks; Springer: Berlin, Germany, 2013; pp. 143–152.

[4] The FBI Now Has the Largest Biometric Database in the World. Will It Lead to More Surveillance? Available online: http://www.ibtimes.com/fbi-now-has-largest-biometric-database-world-will-it-leadmore-surveillance-2345062.

[5] U.S. Security Officials Will Begin Scanning All 10 Fingerprints of Most Non-Americans Traveling to the United States. Available online: https://travel.state.gov/content/visas/en/news/u-s--security-officialswill-begin-scanning-all-10-fingerprints-.html (accessed on 27 November 2018).

[6] Maio, D.; Maltoni, D.; Capelli, R.; Franco, A.; Ferrara, M.; Turroni, F. FVC-onGoing: On-Line Evaluation of Fingerprint Recognition Algorithms. 2013. Available online: https://biolab.csr.unibo.it/fvcongoing/UI/Form/Home.aspx (accessed on 25 January 2019).

[7] Xia, Z.; Yuan, C.; Lv, R.; Sun, X.; Xiong, N.N.; Shi, Y.-Q. A novel Weber local binary descriptor for fingerprint liveness detection. IEEE Trans. Syst. Man Cybern. Syst. 2018.

[8] Yang, W.; Wang, S.; Hu, J.; Zheng, G.; Valli, C. A fingerprint and finger-vein-based cancelable multi-biometric system. Pattern Recogn. 2018, 78, 242–251.

[9] Pandya, B.; Cosma, G.; Alani, A.A.; Taherkhani, A.; Bharadi, V.; McGinnity, T.M. Fingerprint classification using a deep convolutional neural network. In Proceedings of the 2018 4th International Conference on Information Management (ICIM), Oxford, UK, 25–27 May 2018; pp. 86–91.

[10] Zheng, G.; Shankaran, R.; Orgun, M.A.; Qiao, L.; Saleem, K. Ideas and challenges for securing wireless implantable medical devices: A review. IEEE Sens. J. 2016, 17, 562–576.

[11] N.K. Ratha, J.H. Connell, R.M. Bolle, Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J. 40(3), 614–634.

[12] A.K. Jain, A. Ross, S. Prabhakar, An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. 14(1), 4–20.

[13] Lee AR, Ahn HY (2016) Fintech users' information privacy concerns and user resistance: investigating the interaction effect with regulatory focus. J Korea Inst Inf Secur Cryptol 26(1):209–226.

[14] Perez AJ, Zeadally S, Jabeur N (2018) Security and privacy in ubiquitous sensor networks. J Inf Process Syst 14:286–308.

[15] Wu J, Liu L, Huang L (2017) Consumer acceptance of mobile payment across time. Ind Manag Data Syst 117(8):1761–1776.