Modern Applied Science; Vol. 12, No. 4; 2018
ISSN 1913-1844 E-ISSN 1913-1852
Published by Canadian Center of Science and Education

A Novel Multi-Level Security Technique Based on IRIS Image Encoding

Sadeq Al-Hamouz[1]

[1] Computer Science Department, the World Islamic Sciences and Education University, Amman, Jordan

Correspondence: Sadeq Al-Hamouz, Computer Science Department, the World Islamic Sciences and Education University, Amman, Jordan. E-mail: Sadeq.Alhamouz@wise.edu.jo

Received: February 28, 2018 Accepted: March 7, 2018 Online Published: March 19, 2018

doi:10.5539/mas.v12n4p49 URL: https://doi.org/10.5539/mas.v12n4p49

Abstract

Providing highly secured access to restricted or private areas has become highly required these days, mainly due to terrorism threats. One method of security is no longer sufficient, hence the term and technology of a "multi-level" security system was developed by integrating more than one security procedure, on both hardware and software levels. This research provides a simple, cheap, easily achievable, yet highly secured multi-level security system to control access through doors. The system integrates IRIS scan authentication, innovative IRIS image encoding, encrypted of mobile communication, and multipoint Control Unit (MCU) Security as main procedures of security. The system's novelty shows in the encoding and encryption of IRIS image data that is acquired by a mobile phone before it is sent to the authentication site, where it is decrypted by a cheap and fast MCU to retrieve the IRIS image that is fed into a Neural Network in order to grant authorization to the user.

Keywords: authorization, multipoint Control Unit (MCU), Near Field Communication (NFC), IRIS scan, image Encoding

1. Introduction

Securing confidential establishment that hold top-secret information is now done over more than one level. The old school password or IRIS scan or fingerprint recognition are becoming part of the past, science today is seeking to use multiple security procedures to enhance the security and minimize the danger of hacking into confidential systems and establishments.

a lot of research was done to enhance the security over multiple levels by employing a combination of security approaches (Scheirer, Bishop, and Boult, 2013) to make hacking into these systems a hard thing to do, if not impossible, and to add different recognizable features that would allow more subjects be verifiable (Kanade et al., 2013). Recognizing a person based on his/her physical or behavioural features using a pattern recognition technique is referred to as "biometric recognition" (Gunasekaran et al., 2014). These features are recorded and saved on some storage media (a separate database or a memory chip for example).

Many biometric methods can be used in personal identification. New techniques like the study of gait, which is the distinctive way a person walks, require lots of calculations and pre-stored data in a spatio-temporal database (Bowyer et al., 2016). Recognizing a human's facial features is another identification technique that was adopted in research (Owayjan et al., 2015) because this is the way human beings recognize each other.

Some researchers went as far as recognizing personal odour and take it as a biometric feature, as in the research of (Rodriguez-Lujan et al., 2013) where hand odour is recognized through multiple pattern recognition techniques.

The use of fingerprint and IRIS scan is the widely used biometric security measure, due to their uniqueness in recognizing a human being, since no two humans on the face of earth, not even twins, have the exact same features of those (Ngo et al., 2015).

IRIS authentication is done mostly by capturing IRIS print in advance and store it to compare it later with the live scanned at the authentication site. Yet this technique has proven to be vulnerable to attacks, like impersonation attacks (Itkis et al., 2015) as does any binary matching system. Reading fingerprint is also done using the aforementioned binary matching technique. The stored images of all ten fingerprint (and sometimes the whole palm print (Chin et al., 2014)) are compared against those captured at the authorization scene. However, different countermeasures have been studied and developed to overcome such vulnerability (Marasco and Ross, 2015) but

new spoofing and hacking methods arise every day.

With the enhancements on graphics and the use of avatars and robots, faking certain biometrics, like face features and fingerprints, has become more applicable. So efforts were put to recognize these fake features as in the work of (Galbally, Marcel, and Fierrez, 2014) who employs enhanced image quality processing to assess the features and separate fake from legitimate. This work is another proof that relying only on biometric recognition for security might not be efficient.

Security measures developers have studied and developed many techniques that combine two or more authentication techniques. Some of the combinations integrated biometrics with network and hardware technologies to enhance security and prevent hacking. The most common and easy to use is the Near Field Communication (NFC), which is a short-range, wireless communication technology that allows two devices communicate and exchange data when they are at close fields and are paired together (Coskun, Ozdenizci and Ok, 2013).

New mobile phones are trying to be the top in the market by integrating new technologies and gadgets into the mobile device. Recent version of some mobile phone vendors have included a high-quality iris scanner within the phone. The captured iris images can be used in various applications related to the phone itself (De Marsico et al., 2015), and with some tweaking, can be used for applications that are not related to the phone itself.

Iris scanners that are embedded in some mobile phones has several advantages for authentication over other biometric features. According to the survey results done by (Meng et al., 2014); IRIS is considered non-intrusive authentication measure, easily collected, has a high recognition accuracy, and can be used universally.

Encryption of data, along with biometric measures, was adopted in many research to enhance the security, like the work of (Salas, 2013) who combined elliptic curve cryptography (ECC) encryption with fingerprint, (Li et al. 2017) where palm print was combined with two-layer error correction codes, and (Yan and You, 2017) who used the fingerprint as a transformed biometric public key used in encryption.

Physical attacks to the data used to authenticate legitimate users force security enforcement measures to take extra precautions when encrypting biometric data. The researchers in (Revenkar, Anjum, and Gandhare, 2010) propose a “visual encryption” technique, where biometric images are enclosed within another image that has no relation of information with the original iris image used for authentication.

Encoding the iris image into a different format was adopted in the research of (Tan and Kumar, 2014), were some basic iris features were randomly selected as ‘geometric keys’ to encode individual images before storing them, and are used later for comparison and authentication. Encoding iris features was investigated in (Thavalengal et al., 2015) where features are stored as vector data and stored for later comparison with pre-stored vectors of the same iris image (like user authentication).

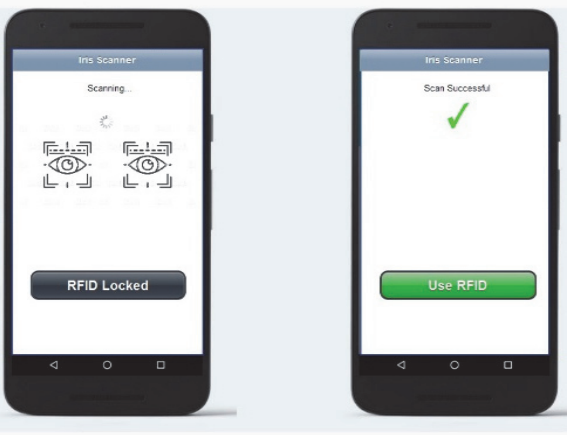

Figure 1. Mobile phone application - IRIS Successful Read

2. The System Design and Hardware Structure

The process starts by capturing an IRIS image by the mobile phone’s camera from a distance between 10 cm to 32 cm. After that the image is processed by a dedicated software to isolate IRIS segment in both internal (pupil boundaries) and external IRIS boundaries, a successful iris image capture results in an acceptance message shown

on mobile application's interface (represented by a green Tick as in the Figure 1). The output is encoded and encrypted immediately for security purposes, after being transformed into a matrix and converted into a color-coded image. Next, the encoded image will be sent to the authentication site through Near Field Communication (NFC) subroutine, to get it compared against the one stored in the database, which, by default, includes a copy of the color-coded image of the iris image of the authenticated users. When the similarity index returns true (based on a threshold value), it is said that a match with that user is found and thus the user is granted access.

To prevent personal identification information from being stolen or revealed, and to prevent impersonation attacks on the phone and connection; an encryption mechanism is needed such as RSA which is known to be strong and fast in encrypting data, with no known linear or algebraic weaknesses.

The block diagram of the entire system is illustrated in figure 2 below, showing the integration of the system's parts, where there's an NFC module that is responsible for sending encoded iris image data to the authentication site, the solenoid unit that is the main mechanism for opening the door, and a power source to feed the authentication and the door opening mechanism; all of these components are connected to the MCU that is responsible for receiving granting access commands through the NFC module from the base controller, and activates the door opening mechanism.

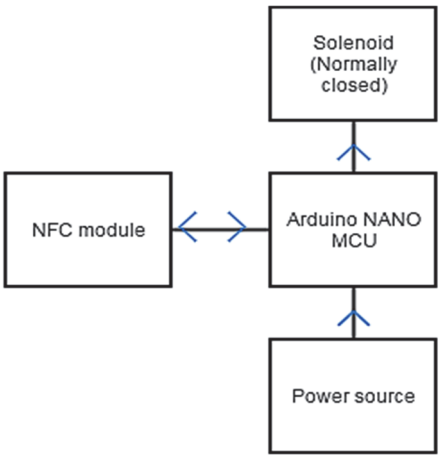

Figure 2. System's Block Diagram

3. IRIS Image Encoding

The iris scanner captures the main features of the iris, and performs localization of the boundaries to determine the correct boundaries of the iris region. An identification process takes place to separate the pupil's boundaries from the IRIS's to establish initial identification points; these points are fitted to capture the distinguish features of the IRIS in a step ahead of converting this image into a matrix before encrypting and sending it to the authentication site. Figure 3 below shows detailed steps of the IRIS scanning procedure.

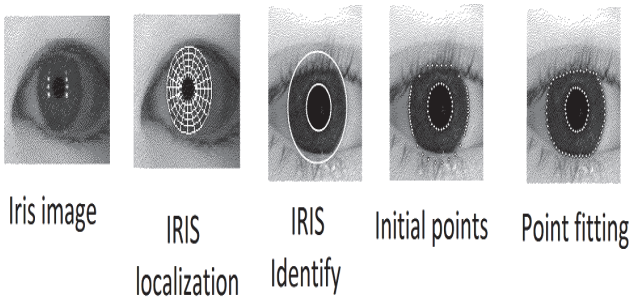

Figure 3. IRIS scan steps

The scanned IRIS image is stored as a 2D image matrix, where each entry represents a pixel of the iris image (example of features is shown in figure 4).

Figure 4. features extracted from IRIS image

Each entry of this matrix is multiplied by a pre-define vector (k), and then this matrix is converted into a Hexadecimal code that represents a colour, a segment of the encoded matrix is shown in figure 5, and the matrix after being converted into hexadecimal in shown in figure 6.

124	16	85	213	245
78	7	69	192	250
56	3	37	145	233
64	5	34	133	221
64	11	92	194	239
58	27	169	255	255
54	40	208	255	252

A

126852	16368	86955	217899	250635
79794	7161	70587	196416	255750
57288	3069	37851	148335	238359
65472	5115	34782	136059	226083
65472	11253	94116	198462	244497
59334	27621	172887	260865	260865
55242	40920	212784	260865	257796

B

Figure 5. Iris image output matrix: A: original, B: after multiplying by k

01EF84	003FF0	0153AB	03532B	03D30B
0137B2	001BF9	0113BB	02FF40	03E706
00DFC8	000BFD	0093DB	02436F	03A317
00FFC0	0013FB	0087DE	02137B	037323
00FFC0	002BF5	016FA4	03073E	03BB11
00E7C6	006BE5	02A357	03FB01	03FB01
00D7CA	009FD8	033F30	03FB01	03EF04

Figure 6. encoded image in Hexadecimal

When these hexadecimal values are visualized, they look like a mist coloured image, rather than an image of a scanned human being's iris, as in the example of figure 7.

Figure 7. The colour image resulting from encoding the iris image

The resulting matrix is ready for encryption using the known RSA algorithm that uses large prime numbers in simple mathematical operations to generate a public key. This public key is used to encrypt each entry of the colour coded image matrix, in a manner similar to the technique mentioned in the work of (Saranya and Prabhu, 2016). The private key is used to decrypt this matrix's values to restore original colour codes. The encrypted coded image is then sent to the authentication site via NFC.

4. Sending Encoded Image and Authentication Process

The flow chart in figure 8 illustrates the steps taken in encode the iris image information. Once the image encoding process finishes, the final encrypted "mist-like" image file information is sent through the NFC module to the authentication site.

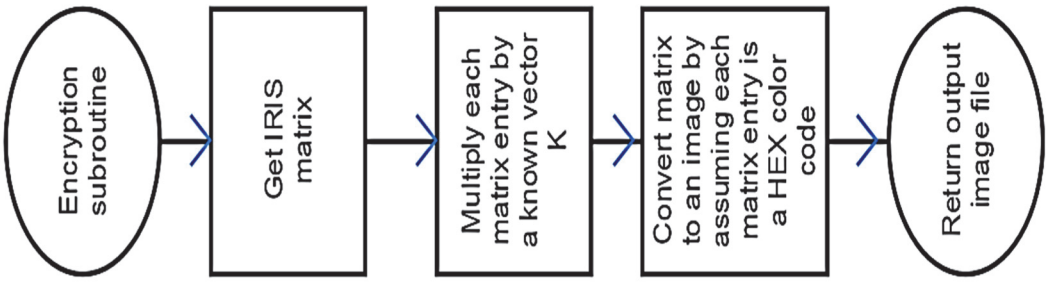

Figure 8. IRIS image coding process

The NFC subroutine starts by receiving the encoded and encrypted image, and then it will keep sending handshake requests until the user's phone gets in the range of the microcontroller unit (MCU) which sends a reply to the handshake. Once this handshake is successful, the encrypted image is sent to the authentication site. This subroutine is shown in details in figure 9.

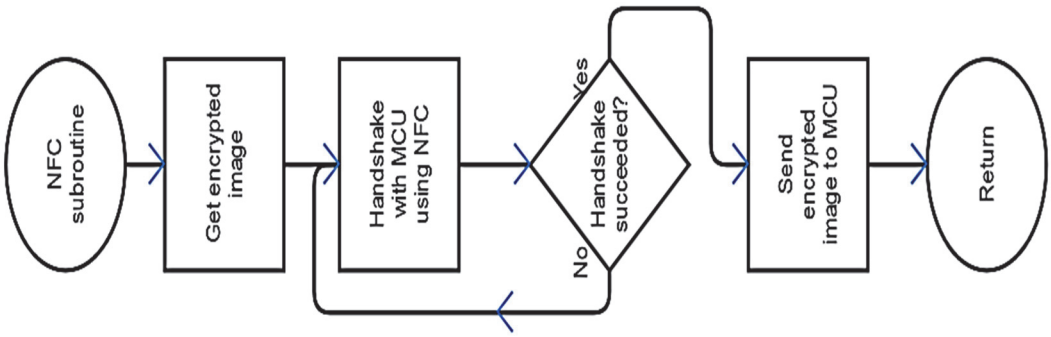

Figure 9. NFC subroutine

At the authentication side (the door site), the image matrix (encoded and encrypted) is received by the MCU after a successful handshake procedure and acceptance. Since Microcontrollers in general have limited capabilities, it is easier (and more efficient) to process a colour code matrix rather than an image with features to be extracted and compared. The decryption process is initialized using the calculated private key from the RSA algorithm, and then reversing the encoding process, this time dividing each of the image matrix entries by the pre-defined vector k to transfer the iris image data back to a 2D image matrix as described in the flowchart of figure 10.

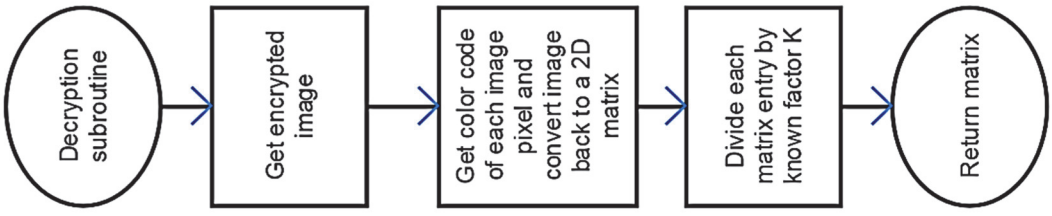

Figure 10. Image decoding and decryption process

The retrieved features from the IRIS image are used as input to the Neural Network to match the received iris image with the one stored at the site. Once the image is validated, the door opening mechanism is activated and the user is granted access to the facility. The flowchart in figure 11 shows the security checking subroutine.

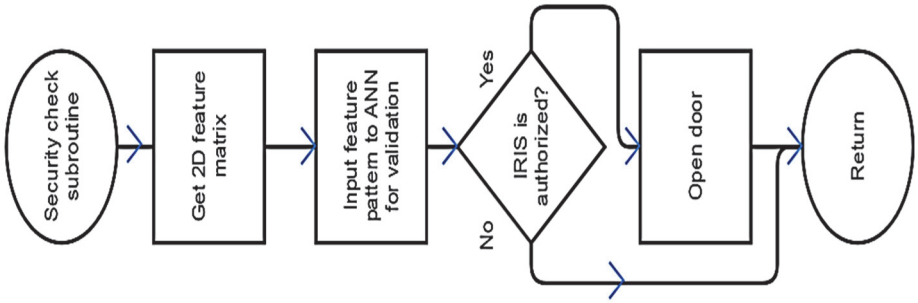

Figure 11. Final authentication subroutine

5. System Performance

A similar idea to the one proposed in this research was proposed in (Dwivedi et al., 2017), where a randomized look-up table was created and pixels of the IRIS image are mapped with values in this look-up table to generate a new coded image that cannot be returned to its original image unless the look-up table used for encoding is available.

Comparing the security technique of this research with the one in (Dwivedi et al., 2017) (hereafter named the look-up mapping technique) shows better applicability of the proposed system in terms of security and performance. In terms of security the look-up mapping technique doesn't enforce any security to the look-up table itself, where this table can be hacked when dumping device memory using K150 chip reader for example. While in the proposed technique, the encoded image is encrypted before being sent wirelessly.

When the image in the look-up mapping technique in (Dwivedi et al., 2017) is transmitted wirelessly it consumes a big space of the network's bandwidth, in addition to the need for more time in transmission and processing of the encoded image (four versions are sent).

Putting both techniques under different types of attacks returned brilliant results for the system we proposed in this research. The simple encryption procedure used in the look-up mapping technique makes the data easily sniffed in a silent attack, the system is also vulnerable to brute force attacks and packet retransmission based attacks. The data in table 1 compares the time required by some of the most common attacks against both techniques (in case there was a successful hack).

Table 1. Time required for different types of attacks to hack the encoded IRIS image

Attack type	Time needed to crack	
	look-up mapping	Proposed algorithm
Silent attack	580 seconds	N/A
Meet in the middle attack	N/A	Failed to crack after 259200 seconds
Brute force attack	130913 seconds	Failed to crack after 259200 seconds
Memory damp attack	75 seconds	180510 seconds
Data retransmission attack	Applicable easily	N/A

6. Conclusion and Future Vision

Authentication is a very important issue these days, especially with the escalation of terrorism and vandalism actions. A new multilevel security system is proposed that uses the cutting-edge technology of mobile phones iris scanners to authenticate the user on the first level.

Iris image of the user is captured, and transformed into a formatted data matrix, that cannot be recognized if it was interrupted and captured while transferred. Another advantage of this transformation is to allow the simple, yet efficient, microcontroller unit process and decode the received image faster and more reliable.

The NFC secured communication allows better performance and higher security reliability since it activates

authentication over a close range of the user and the door, since a successful handshake is required before sending the encrypted image data.

A more sophisticated implementation and testing is needed, although testing of each of the levels provided a very small (if ever found) error margin, that was mainly referred to hardware faults. Encryption of the data was set to all kinds of brute force attacks and survived them with excellence.

More levels to this security system could be integrated, like a Bluetooth authentication sub-system that makes user's interaction even less. This could be used to authenticate the MAC address of two or more smart devices used by the user, that when become within range, the "device" is authenticated, and hence the user is authenticated and granted access to some secured area. This is one suggestion among many others that could be easily, and seamlessly integrated with the system developed in this research.

References

Bowyer, K. W., Hollingsworth, K. P., & Flynn, P. J. (2016). A survey of iris biometrics research: 2008–2010. In *Handbook of iris recognition* (pp. 23-61). Springer, London. https://doi.org/10.1007/978-1-4471-6784-6_2

Chin, Y. J., Ong, T. S., Teoh, A. B. J., & Goh, K. O. M. (2014). Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion. *Information Fusion, 18*, 161-174. https://doi.org/10.1016/j.inffus.2013.09.001

Coskun, V., Ozdenizci, B., & Ok, K. (2013). A survey on near field communication (NFC) technology. *Wireless Personal Communications, 71*(3), 2259-2294. https://doi.org/10.1007/s11277-012-0935-5

De Marsico, M., Nappi, M., Riccio, D., & Wechsler, H. (2015). Mobile Iris Challenge Evaluation (MICHE)-I, biometric iris dataset and protocols. *Pattern Recognition Letters, 57*, 17-23.

Dwivedi, R., Dey, S., Singh, R., & Prasad, A. (2017). A privacy-preserving cancelable iris template generation scheme using decimal encoding and look-up table mapping. *Computers & Security, 65*, 373-386. https://doi.org/10.1016/j.cose.2016.10.004

Galbally, J., Marcel, S., & Fierrez, J. (2014). Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition. *IEEE Transactions on Image Processing, 23*(2), 710-724. https://doi.org/10.1109/TIP.2013.2292332

Gunasekaran, K., Priya, S. A., Saravanan, D., & Akilan, P. (2014). Privacy preserving multimodal biometrics in online passport recognition. *Biometrics and Bioinformatics, 6*(3), 94-98.

Itkis, G., Chandar, V., Fuller, B. W., Campbell, J. P., & Cunningham, R. K. (2015). Iris Biometric Security Challenges and Possible Solutions: For your eyes only? Using the iris as a key. *IEEE Signal Processing Magazine, 32*(5), 42-53. https://doi.org/10.1109/MSP.2015.2439717

Kanade, S., Petrovska-Delacrétaz, D., & Dorizzi, B. (2013). Obtaining cryptographic keys using multi-biometrics. In *Security and privacy in biometrics* (pp. 123-148). Springer, London. https://doi.org/10.1007/978-1-4471-5230-9_6

Li, H., Qiu, J., Dong, J., & Feng, G. (2017). Biometrics encryption combining palmprint with two-layer error correction codes. In Ninth International Conference on Digital Image Processing (ICDIP 2017) (Vol. 10420, p. 104201L). *International Society for Optics and Photonics*. https://doi.org/10.1117/12.2281672

Marasco, E., & Ross, A. (2015). A survey on antispoofing schemes for fingerprint recognition systems. *ACM Computing Surveys (CSUR), 47*(2), 28. https://doi.org/10.1145/2617756

Meng, W., Wong, D. S., Furnell, S., & Zhou, J. (2015). Surveying the development of biometric user authentication on mobile phones. *IEEE Communications Surveys & Tutorials, 17*(3), 1268-1293. https://doi.org/10.1109/COMST.2014.2386915

Ngo, D. C., Teoh, A. B., Hu, J., editors. (2015) Biometric Security. *Cambridge Scholars Publishing*.

Owayjan, M., Dergham, A., Haber, G., Fakih, N., Hamoush, A., & Abdo, E. (2015). Face recognition security system. In *New Trends in Networking, Computing, E-learning, Systems Sciences, and Engineering* (pp. 343-348). Springer, Cham. https://doi.org/10.1007/978-3-319-06764-3_42

Revenkar, P. S., Anjum, A., & Gandhare, W. Z. (2010). Secure iris authentication using visual cryptography. arXiv preprint arXiv:1004.1748.

Rodriguez-Lujan, I., Bailador, G., Sanchez-Avila, C., Herrero, A., & Vidal-De-Miguel, G. (2013). Analysis of pattern recognition and dimensionality reduction techniques for odor biometrics. *Knowledge-Based Systems*,

52, 279-289. https://doi.org/10.1016/j.knosys.2013.08.002

Salas, M. (2013). A secure framework for OTA smart device ecosystems using ECC encryption and biometrics. In *Advances in Security of Information and Communication Networks* (pp. 204-218). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-40597-6_18

Saranya, R., & Prabhu, S. (2016). Image Encryption using RSA Algorithm with Biometric Recognition. *International Journal of Engineering and Computer Science, 5*(11), 19149-19154 https://doi.org/10.18535/ijecs/v5i11.78

Scheirer, W. J., Bishop, W., & Boult, T. E. (2013). Beyond pki: The biocryptographic key infrastructure. In *Security and Privacy in Biometrics* (pp. 45-68). Springer, London. https://doi.org/10.1109/WIFS.2010.5711435

Tan, C. W., & Kumar, A. (2014). Efficient and accurate at-a-distance iris recognition using geometric key-based iris encoding. *IEEE Transactions on Information Forensics and Security, 9*(9), 1518-1526. https://doi.org/10.1109/TIFS.2014.2339496

Thavalengal, S., Andorko, I., Drimbarean, A., Bigioi, P., & Corcoran, P. (2015). Proof-of-concept and evaluation of a dual function visible/NIR camera for iris authentication in smartphones. *IEEE Transactions on Consumer Electronics, 61*(2), 137-143. https://doi.org/10.1109/TCE.2015.7150566

Yan, B., & You, L. (2017). A novel public key encryption model based on transformed biometrics. In *Dependable and Secure Computing*, 2017 IEEE Conference on (pp. 424-428). IEEE. https://doi.org/10.1109/DESEC.2017.8073861