An Efficient Hybrid Authentication Mechanism Based on Biometric Fingerprint Recognition and Homomorphic Encryption

Georgiana Crihan*, Marian Crăciun, and Luminița Dumitriu

Faculty of Automation, Computer Sciences, Electronics and Electrical Engineering, Dunarea de Jos University of Galati, 2 Științei Street, Galati, Romania

Email: georgian.crihan@ugal.ro (G.C); marian.craciun@ugal.ro (M.C.); luminita.dumitriu@ugal.ro (L.D.)

*Corresponding author

Manuscript received February 10, 2024; revised March 12, 2024; accepted May 1, 2024; published May 28, 2024.

***Abstract*—In the current security environment, where the dependence on computer systems is increasing, and the technological field is constantly changing, the threats and vulnerabilities typology to networks is also growing, so a key task is to ensure the network's security access. To address these challenges, we propose an efficient hybrid network authentication mechanism that combines and integrates actual access control components based on cryptography and biometrics. These elements play a vital role in the field of information security and aim to resolve the shortcomings of conventional authentication methods and enhance the security level of sensitive data, especially in the government and military domains. In this paper, we present a mechanism that comprises biometric fingerprint recognition and card authentication based on Arduino modules with the Paillier homomorphic encryption algorithm, a reliable solution that can facilitate secure access to computer systems and networks and minimize the risk of unauthorized access. A statistical assessment is performed using several parameters such as histogram analysis, information entropy, Mean Square Error (MSE), peak signal-to-noise ratio (PSNR), correlation coefficient, and average encryption time to verify the efficiency and robustness of the encryption algorithm.**

***Keywords*—biometrics, microcontroller, cryptographic algorithms, homomorphic encryption**

I. Introduction

In the current security environment, where the typology of threats is diversifying due to digitalization in most fields of activity, the need to quickly develop robust, adaptable, scalable, and reliable defense mechanisms of identification and authentication represents a real challenge in ensuring confidentiality, integrity, and availability of network information.

Single-factor authentication proved to be vulnerable to attack vectors, and to prevent these attacks a mature, high-security authentication scheme is needed to support the dynamic profile of users in various applications. Specifically, the level of protection for the access control mechanism exponentially increases when two or more factors of the identity verification process are combined and a hybrid authentication method is adopted.

Motivated by this emergent need for a unique and scalable tool for computer authentication, we designed a secure hybrid authentication mechanism obtained through the fusion of biometric fingerprint recognition with card authentication and a homomorphic encryption algorithm used to protect the user access credentials from disclosure to unauthorized parties and facilitate secure access to computer systems and networks.

The main reason for implementing a tool based on fingerprint characteristics is because it is one of the most representative, widely used, and time-invariant parts of the human body, which plays a vital role in a person's identification and authentication. Also, this biometric feature can be used for different application requirements and deployed in a wide variety of scenarios from access security systems to computers and different types of networks: radio networks, and cloud platforms.

The fingerprint biometric authentication process comprises three main phases: enrollment, verification, and identification [1]. In the enrollment phase, the following operations are performed: biometric characteristic acquisition from the biometric sensor, genuine biometric feature extraction, and template storing in the database. A comparison between the new data capture and the reference data of the considered individual is realized during the verification phase. This biometric template is stored in the system database and encrypted with the Paillier homomorphic algorithm.

In the identification process, the system compares the extracted features from the captured biometric sample against the templates of all the subjects in the system storage; the output is a user list that may be empty or contain one (or more) identifier of matching enrollment templates. To enhance the security and privacy of the biometric template, we associated biometrics with card authentication.

One significant advantage of using a homomorphic encryption technique on biometrics is that it allows performing computation directly over encrypted data without decrypting and without degrading image recognition accuracy, and also provides data confidentiality while information are exchanged and while a non-secure-enough platform processes them.

Consequently, the research aims to build an efficient hybrid network authentication mechanism based on biometric fingerprint recognition and homomorphic encryption to be applied to computer systems, especially in military radio networks or Ethernet networks that must deal with multi-level security and strong authentication requirements.

The present work is organized as follows: in the Introduction, a brief description of the state of the art is made; Section II provides a detailed overview of the existing methods used for biometric fingerprint recognition and different cryptographic algorithms in literature; Section III presents the design of the elements involved in the new

hybrid authentication mechanism based on biometric elements combined with homomorphic encryption algorithm; Section IV presents the experimental results and research findings in detail, which is followed by the conclusion and prospects of developing new authentication mechanisms based on biometric features and fully homomorphic encryption algorithms in Section V.

II. Literature Review

There is an increasing interest in designing, implementing, and deploying intuitive techniques of fingerprint recognition combined with different modern cryptographic algorithms to achieve data privacy and protection of personal information in the architecture of the current security environment. It is worth pointing out that biometric recognition and cryptographic algorithms are among the best factors used to provide secure and reliable authentication. Several solutions have been proposed in the literature that associate fingerprint recognition with cryptographic algorithms like symmetric or asymmetric encryption, hash functions, and different biometric cryptosystems based on key generation [2, 3] and key binding techniques [4].

Ruiu *et al.* [5] presented in their project a complete cloud system that uses biometric authentication based on fingerprints integrated with the Open Stack cloud platform, a solution capable of delivering cloud services to small-medium companies that proved good performance, and privacy, and gives the user a concrete feeling of security.

In Ref. [6], an embedded fingerprint authentication system implemented in a 32-bit microcontroller with biometric template protection using a chaos encryption algorithm with 128 secret keys is developed for critical real-world applications.

Kavati *et al.* [7] proposed a new approach for securing fingerprint templates using elliptical structures generated from the fingerprint minutiae.

According to the biometric cryptosystems presented in [8], a new biometric ECC key binding process improves security, privacy, and accuracy performance aspects by employing a series of adoptive cancellable transforms and thresholding mechanisms and its implementation for fingerprint minutiae-based representation.

Some improvements and efficient achievements were introduced in Ref. [9], where a novel approach that includes fingerprint as a user-secure and trustworthy authentication along with Elliptic Curve Cryptography and Public Key Infrastructure is used for client-server authentication.

Several biometric template protection techniques have been proposed in the specialized literature, and all of them can be integrated in a unified architecture represented by ISO/IEC 24745 (2011) standard on Biometric Information Protection that provides general guidance for the protection of biometric information. According to Ref. [10], in this standard, the framework of a protected biometric template structure comprises two main elements, namely, Pseudonymous Identifier (PI) and Auxiliary Data (AD) used especially in feature transformation approach and biometric cryptosystems. This standard also establishes four main requirements for a protected template: renewability, unlinkability, irreversibility, and recognition performance.

State-of-the-art research in biometrics and cryptography shows that the systems based on these technologies are efficient and have numerous operational advantages. Therefore, new research perspectives must be dedicated to both the improvement of the performance of such systems and the improvement of user experience.

III. Proposed Methodology

Nowadays, most of the authentication technical solutions are implemented in embedded systems because these systems contain software and hardware that use a processor with confined resources, like limited computational power, limited memory, and input–output peripherals that offer high performance and flexibility at a reasonable cost, low power consumption, and scalable dimensions. For this purpose, we design and develop an embedded authentication biometric system with smart capacity to perform biometric enrollment and authentication with security guarantees, low cost, high performance, template protection guaranteed, store data, and transmit it over insecure channels.

A. Authentication System

In the proposed embedded system, we used an Arduino Pro Micro 5V/16MHz microcontroller with a Radio Frequency Identification (RFID) reader and a high-performance fingerprint scanner programmed with the Arduino Integrated Development Environment (IDE), an open-source software, suitable to meet the needs of the system, as presented in Fig. 1.

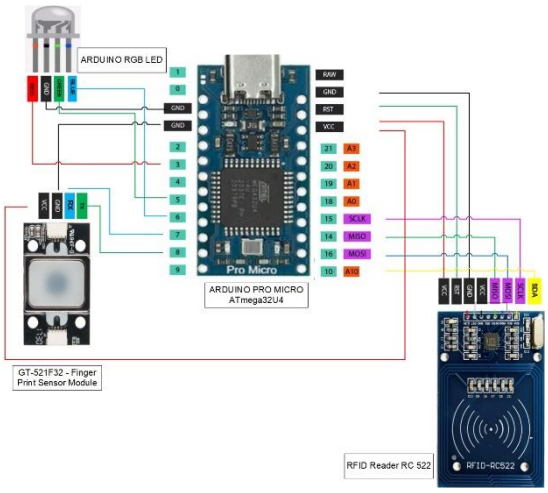

Fig. 1. Biometric authentication mechanism based on Arduino modules

The RFID RC 522 reader module represents an ID system for identification and tracking purposes that uses radio frequency identification devices. Communication between the Arduino microcontroller and RFID module uses the MFRC522 library that simplifies reading from and writing to RFID tags. In addition, the RFID tagging system consists of the tag, a reader/writer device, and a system application for data acquisition, processing, and transmission. According to ISO 14443A standard tags, the system produces an electromagnetic field of 13.56 MHz in the radio frequency HF that ranges between 10–15 MHz used to communicate with the RFID tags that continuously generate a carrier wave. Data exchanged between the reader and tag is transmitted in half-duplex mode. The time required for the tag to be fully functional is the setup time.

The enrollment process for accessing the company systems and resources by the authorized user includes two verification stages: card validation ID and fingerprint verification, as presented in Fig. 2. First, the system verifies the card serial data, and then the fingerprint module uses minutiae extraction technique to generate the user's template and send it to the microcontroller via UART serial communication (data transmission between processors) with the standard 9600bps baud rate. The fingerprint reader in the MCU device contains a 32-bit microcontroller based around an ARM® Cortex™-M3 processor core and a high-performance, low-power optical sensor, which processes the fingerprint algorithm.

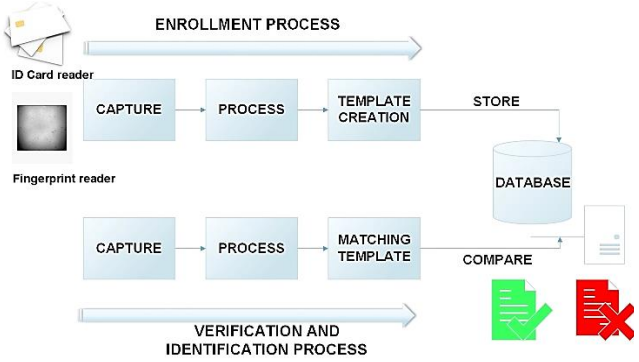

Fig. 2. Authentication process.

Once the authorized user is successfully registered in the system, the user can access the resources through the authentication process. The template data is stored in the computer system memory and the information is encrypted using the proposed encryption algorithm based on Paillier homomorphic encryption algorithm. The scanner of the fingerprint module, which provides 360° recognition is based on infrared LED technology and has a processor with a fingerprint recognition algorithm based on minutiae extraction with a false acceptance rate of FAR 0.001 and a false rejection rate of FRR 0.1.

The microcontroller performs various tasks such as ID card verification, reading the fingerprint template, storing the fingerprint template, and matching queries for authentication and human interface. The human interface helps people enroll and authenticate. Without the proper ID card reader, and software working together as intended, the user cannot access the company resources and would otherwise need live, on-site help desk support to find an alternative path for access. If a card is lost, access to the old card is revoked and a new card is issued.

B. *Encryption Algorithm*

The protection of biometric templates has attracted a lot of attention in the research community and a relevant strategy to secure the template storage of a fingerprint recognition system from attackers is to implement an appropriate cryptographic algorithm in the system so that the information is encrypted and kept in a secure area of the main processor that neither the user nor the applications can access.

The biometric templates stored in the database during the enrollment process should be protected against various attacks such as record multiplicity attack, hill-climbing attack, dictionary attack, replay attack, and masquerade attack. This objective can be achieved through the implementation of different techniques that include Cancelable Biometrics, Bio-cryptosystems, and Homomorphic Encryption [11], as mentioned in Fig. 3.

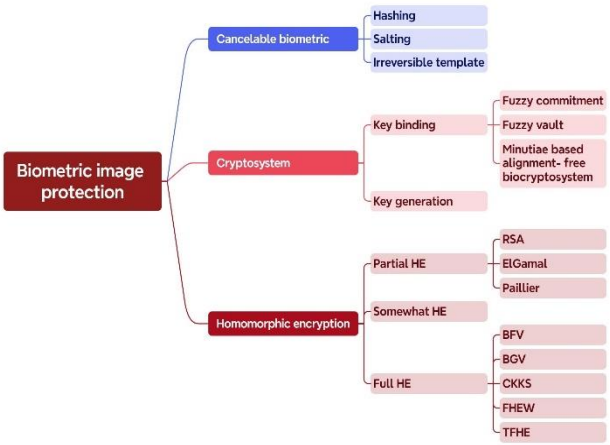

Fig. 3. Biometric template protection techniques.

In our project, we choose the implementation of the homomorphic encryption algorithm in order to safeguard biometric data, used to identify and authenticate a user according to data protection legislation such as the European's Union General Data Protection Regulation (GDPR), which provides strict guidelines for handling and dissemination of personal data [12]. Specifically, the encryption scheme used in our method is Paillier's partially homomorphic encryption algorithm, a special case of asymmetric encryption that uses a public key for encryption and a private key for decryption and ensures the protection of sensitive data in computational tasks with multiple participants. It allows us to perform additions to the encrypted data itself without decryption.

The Paillier cryptosystem supports a partially homomorphic scheme based on an addition operation, where two encrypted values can be added or subtracted together, and the decryption of the result yields the difference between the two values. For the encryption process of the biometric data, two types of keys are generated public key *(g, n)* and the private key *(λ, μ)*.

This algorithm comprises the following operations [13]:

a) Key generation

This probabilistic algorithm takes into consideration two random large prime numbers *p* and *q*, independently of each other and equal length, such that *gcd (p-1, q) = 1* and *n* computed by using the formula $n=p \times q$ and $\lambda(n) = lcm(p-1, q-1)$, which means Least Common Multiple. Also, an integer randomly as *g* should be selected, where $g \in Z^*_{n^2}$. The value of *n*, calculated above, divides the order of *g* by checking the existence of the following modular multiplicative mathematical formula:

$$\mu = (L \cdot (g^{\lambda} \times mod\ n^2))^{-1} mod\ n \tag{1}$$

where function L is defined as:

$$L(x) = \frac{x-1}{n} \tag{2}$$

The pair *(n, g)*, where *n* is the modulus and *g* is the encryption base is released as a public key, but the private

decryption key $\lambda(n)$ is kept secret.

b) Encryption

This algorithm takes as input a message m to be encrypted, where $0 <= m < n$ and outputs a cipher text:

$$c = g^m \cdot r^n \ (mod\ n^2) \tag{3}$$

The number r is selected randomly for each message m, where $0<r<n$ and $r \in Z^*_{n^2}$, with the condition $gcd\ (r, n) = 1$.

c) Decryption

This deterministic algorithm takes a cipher text to decrypt, $c \in Z^*_{n^2}$, a private key (λ, μ) and outputs the message $m = Decrypt(c; \lambda, \mu)$. The decryption process is performed as:

$$\begin{aligned} m &= \frac{L \cdot \left(c^\lambda \ mod\ n^2\right)}{L \cdot \left(g^\lambda \ mod\ n^2\right)} \cdot mod\ n \\ &= L \cdot \left(c^\lambda \ mod\ n^2\right) \cdot \mu \cdot mod\ n \end{aligned} \tag{4}$$

If an addition operation is desired to be computed with the encrypted data, a multiplication operation must be used. The reason for this is that the message encodes as an exponent. Therefore to add exponents, a multiplication operation needs to be computed on two values of the same base, which in this case is g. Since the values r_1 and r_2 are random, they can be combined to form another random value r. Considering two cipher texts according to the encryption scheme presented below, the addition and multiplication operations are defined by the following equations:

$$c_1 = g^{m_1} \cdot r_1^n (mod\ n^2) \tag{5}$$

$$c_2 = g^{m_2} \cdot r_2^n (mod\ n^2) \tag{6}$$

$$\begin{aligned} E(m_1) \cdot E(m_2) &= \left(g^{m_1} \cdot r_1^n (mod\ n^2)\right) \\ &\cdot \left(g^{m_2} \cdot r_2^n (mod\ n^2)\right) \\ &= g^{m_1+m_2} \cdot (r_1 \cdot r_2)^n (mod\ n^2)) \\ &= E(m_1) + E(m_2) \end{aligned} \tag{7}$$

IV. Experimental Results

The experimental results and the comparative analysis are presented in this section. The Paillier cryptosystem algorithm is developed in Python 3.10, 64-bit software, and applied over biometric images where each image size is 258×202 pixels and the resolution is 450 dpi. Several open-source libraries for image processing tasks were used in Python, such as Numpy, OpenCV, Matplotlib, Scipy, and Pillow, to perform the encryption algorithm and specific operations on the extracted biometric data.

According to Ref. [14], the biometric system evaluation is performed using the following four approaches: performance evaluation, evaluation of the quality of the biometric data, security evaluation, and usability evaluation.

In our research, a statistical assessment is carried out employing evaluation metrics such as histogram analysis, information entropy, Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), correlation coefficient, and average encryption time to measure the performance of image encryption system.

The proposed embedded authentication system can be considered an embedded expert system because it performs biometric enrollment and authentication with high-security guarantees, low cost, and high performance. The protected template can be stored or transmitted through an insecure channel.

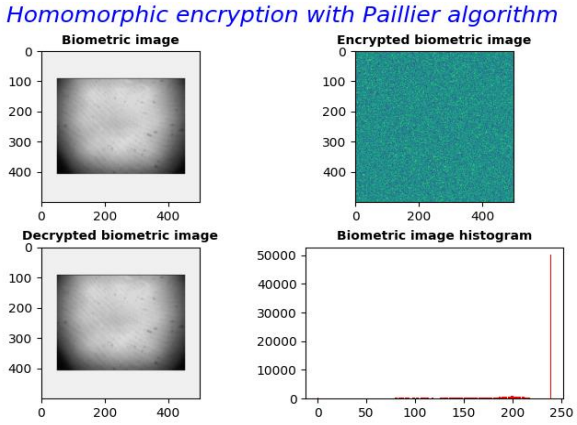

Fig. 4. Implementation of homomorphic encryption algorithm.

a) Histogram analysis

Histogram represents one of the most important metrics when examining an encrypted image, which provides the frequency of each element in graphical form (statistical data). In Fig. 5, the biometric image has its histogram pattern, compared to the encrypted biometric image characterized by a uniform histogram to avoid any suspicion that it is the clear template, as shown in Fig. 6. Therefore, the diffusion process produces a uniform histogram that is resistant to the wide variety of cyber-attacks.

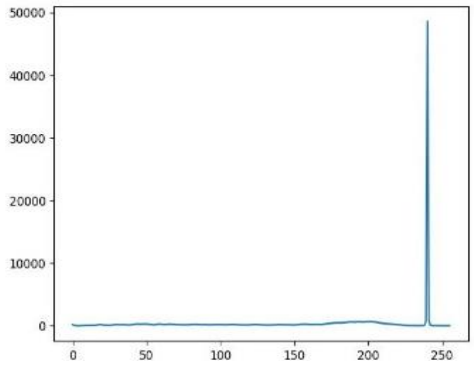

Fig. 5. Biometric image histogram.

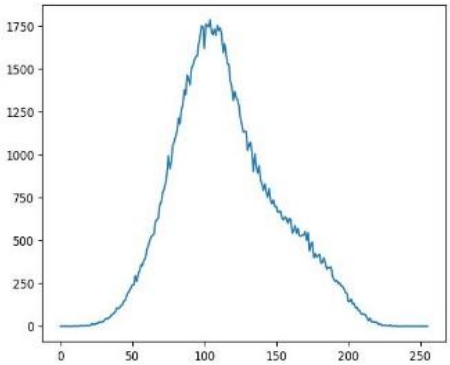

Fig. 6. Encrypted image histogram.

Analysis of the histogram of the original and encrypted templates and their contents shows that the histogram of the encrypted image is quite uniform and significantly different from that of the original image. The histogram of the encrypted image is different from the histogram of the original image, so the hacker will not be able to obtain the original image through the encrypted image histogram. A perfectly secure algorithm must produce an encrypted image with uniform and completely different histograms compared to the original image.

b) Entropy Analysis

Entropy analysis in biometric image processing represents a significant metric that measures and quantifies the degree of randomness or disorder in the structure of an image, where the random variable comprises the pixels in an image. The higher entropy of the biometric template indicates higher randomness in the image, and the higher the entropy, the higher the level of security.

Otherwise, since a certain degree of predictability exists in the encryption method, the encryption process is not random, and the system may be vulnerable to different types of attacks. The entropy of an image is affected by the number of image colors, the number of image pixels, and the distribution of image colors. Adding noise to the image increases the entropy of an image.

According to Y. Wu *et al.* [15], Shannon entropy has been widely used for years in image encryption as a general measure for information and uncertainty, and it represents the most significant entropy in applications, whose mathematical formula is given by the following equation:

$$H(x) = -\sum_{i=1}^{n} p(x_i)\, log_2\, p(x_i) \tag{8}$$

where n is the number of bits of each element of the biometric image; $p(x_i)$ represents a probability of the element x_i in the biometric image, and the entropy is expressed in bits.

In our proposed work, the entropy of the raw biometric image is H = 4.94, whereas the entropy of the encrypted biometric image is H = 7.61, and the maximum achievable value is H = 8, which means that all elements appear with the same probability. The higher the information entropy value, the higher randomness is achieved at the pixel level.

Therefore, from the numerical experiments shown in Table 1 and Fig. 7, we can observe that the value of the encryption template is higher compared to the raw biometric template, which means is highly pseudorandom. The results also show the direct dependence of the entropy on the file size, such the entropy increases as the length of the image increases.

Table 1. Entropy simulation on biometric images

Type of biometric data	Entropy
Raw biometric data 1	4.9718
Raw biometric data 2	4.9343
Raw biometric data 3	4.9166
Raw biometric data 4	4.9457
Raw biometric data 5	4.9113
Encrypted biometric data 1	7.6095
Encrypted biometric data 2	7.6123
Encrypted biometric data 3	7.6100
Encrypted biometric data 4	7.6111
Encrypted biometric data 5	7.6120
Decrypted biometric data 1	5.8139
Decrypted biometric data 2	5.8195
Decrypted biometric data 3	5.8221
Decrypted biometric data 4	5.8284
Decrypted biometric data 5	5.7760

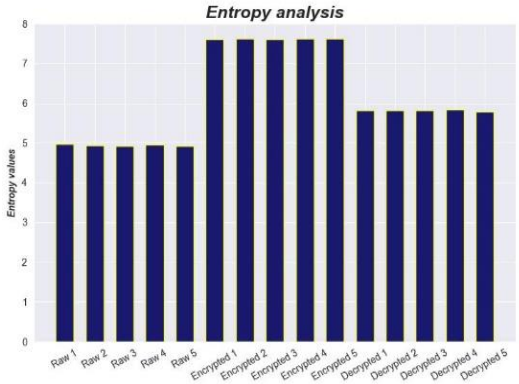

Fig. 7. Entropy graphic representation

c) Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR)

A widely used and full-reference metric for encryption quality assessment of a biometric image encryption is the Mean Square Error (MSE), computed by averaging the squared intensity differences of original and encrypted image pixels, along with the related quantity of peak Signal-to-Noise Ratio (PSNR). These metrics play a significant role in image quality assessment, and are appealing because they are easy to compute, have clear physical meaning, and are mathematically convenient in the context of optimization.

These image quality metrics are represented mathematically as follows [16]:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} [M(i,j) - F(i,j)]^2 \tag{9}$$

$$PSNR = 10 \times^{\square} ln(f_{max}/MSE)^2 \tag{10}$$

where $M \times N$ represents the matrix data of the original biometric image, F represents the matrix data of the encrypted image, m represents the number of pixel rows of the image and i represents the index of that row, n represents the number of pixel columns of the image and j represents the index of that column, and f_{max} is the maximum signal value that exists in our original image.

From the experimental results, the PSNR value increases and approaches infinity while the MSE value gradually decreases with the improvement of the bit rate in compressed image, and approaches values closer to zero which is better for image quality. The higher the bit rate of the compressed image, the better the quality of the image and the lower the errors. On the other hand, a small value of PSNR implies high numerical differences between images. However, the metrics listed below are inversely proportional and provide meaningful results for evaluating image quality, as shown in Table 2.

d) Correlation coefficient analysis

In statistical analysis, a representative factor to measure the relationship between two variables, the original biometric image and the encrypted image, is considered the correlation between adjacent pixels, known as the correlation coefficient. If the similarity between the original and encrypted image is lower, then the value of the correlation coefficient is low. The values obtained by calculating the correlation coefficient show that the system can handle statistical attacks. Therefore, the encrypted image must be completely different from the original image. To quantitatively illustrate the correlation of adjacent pixels in an image, we can calculate the correlation coefficient using the following mathematical formula [17]:

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A})^2)(\sum_m \sum_n (B_{mn} - \overline{B})^2}} \quad (11)$$

where $\bar{A}$ = mean 2(A), and $\bar{B}$ = mean 2(B).

The values of the correlation coefficient are adjusted to be in the range [–1, 1], with the extreme values having the same meaning. A value of +1 indicates a perfect positive correlation and shows that the original image and its encryption are very similar, whereas a value of –1 indicates a perfect negative correlation and shows that the given images are very different. Otherwise, if the correlation coefficient is equal to the value 0 means no linear correlation between the images, and the encrypted image is completely different from the original (i.e., good encryption). The interpretation of the coefficient becomes more difficult when its value approaches zero. It is important to emphasize that a Pearson correlation coefficient close to 0 indicates no linear relationship between the variables. However, a strong, non-linear relationship may exist instead.

When a relationship between two variables is non-linear, the rate of increase or decrease may change as one variable changes, creating a curve-like pattern in the data. Natural images usually have a strong correlation with adjacent pixels. An efficient encryption algorithm should reduce the correlation in cipher images, as shown in Table 2.

Table 2. Statistical analysis metrics

Statistic metrics Biometric images	MSE	PSNR	Correlation coefficient (Raw / Encrypted)	Correlation coefficient (Raw / Decrypted)
Biometric image 1	33193.5153	27.8729	0.1781	0.99112
Biometric image 2	32517.4143	27.8749	0.1798	0.99193
Biometric image 3	32877.4710	27.8571	0.1801	0.99066
Biometric image 4	33454.2566	27.8644	0.1779	0.99229
Biometric image 5	31051.0469	27.8946	0.1774	0.99307

e) Time analysis

Execution time is another important factor in evaluating the efficiency of the biometric system, influenced by several parameters such as the specifications and structure of the CPU, memory capacity, image size, software used, etc. The memory space required by the system is an equally meaningful factor to consider when evaluating biometric systems. It generally measures the average and maximum size of a biometric system and the maximum storage space allocated during the enrollment, verification, and identification phases. The processing time for different operations should be minimal in order to obtain an optimized system and choose the most suitable encryption algorithm [18].

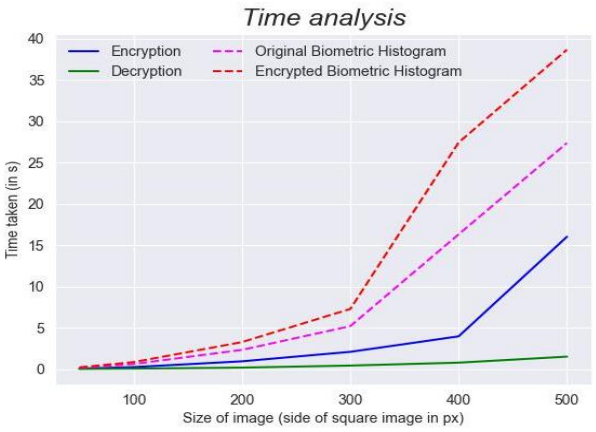

Fig. 8. Time analysis.

The experiment considers the biometric images of the users' fingerprints extracted from the Arduino system, and the execution time is generated using a Python script. The results show that the time required for different operations is strictly correlated with image size and is directly proportional, as shown in Fig. 8. Therefore, a larger dimension of the biometric template means longer computational time.

The security and time factors play a crucial role in selecting an algorithm because if we compromise on either of these factors, it may affect the system's performance in terms of safety and efficiency.

V. Conclusion

In this paper, we developed a hybrid mechanism of authentication that combines biometric fingerprint recognition with RFID card authentication and homomorphic encryption algorithms to improve the overall security and accuracy of user authentication and to ensure the confidentiality, integrity, and availability of information during network authentication. Using cryptography and biometrics, which are important components of modern access control systems, the proposed technical solution is reliable and cost-effective, and its implementation aims to reduce emerging attacks and maximize security in the current digital environment.

The assembled device is particularly attractive for both authentication and identification applications. It can be easily customized for different organizational needs and has high potential in several applications in embedded systems, especially in sensitive applications that deal with multi-level security and strong authentication requirements.

When analyzing the authentication requirements related to

the security chain, it is worth highlighting that the current mechanism accomplishes the following conditions:

- Improve the level of security against unauthorized access
- Simplify the authentication process and reduce the authentication burden on the user
- Provide an efficient identification method based on an individual's physiological characteristics
- Provide an accessible technical solution in the equation of cost versus performance.

Therefore, one of the future development directions would be the improvement of the current hybrid mechanism by using efficient fully homomorphic encryption algorithms such as BFV (Brakerski/Fan-Vercauteren) and BGV (Brakerski-Gentry-Vaikuntantan) for encrypting the biometric templates, to provide privacy-preserving computation on encrypted data and reduce computation time, to accelerate the deployment of biometric authentication using homomorphic encryption in different types of networks.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Luminita Dumitriu directed and coordinated the research in all phases; Marian Craciun provided conceptual and technical support for the design and implementation of the embedded system of authentication and reviewed the results for the statistical analysis of the data; Crihan Georgiana assembled the technical solution, performed and analyzed the results obtained after the implementation and development of the cryptographic algorithm on biometric data and wrote the original paper; All authors reviewed the manuscript draft and revised it critically on intellectual content; All authors approved the final version of the manuscript to be published.

References

[1] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of Biometrics*, New York, Springer, 2008, ISBN 978-0-387-71040-2.

[2] H. A. Zaki, "Cryptographic key generation using fingerprint biometrics," *University of Thi-Qar Journal of Science*, pp. 75–80, May 2019. doi: 10.32792/utq/utjsci/vol5/2/25.

[3] K. H. Solanki, "A new approach to symmetric key generation using combination of biometrics key and cryptographic key to enhance security of data," *International Journal of Engineering Research*, vol. 2, no. 3, 2013, ISSN: 2278-0181.

[4] A. A. A. Saggaf, "Key binding biometrics-based remote user authentication scheme using smart cards," *IET Biometrics Journal*, November 2017. doi: 10.1049/iet-bmt.2016.0146, www.ietdl.org, ISSN 2047-4938

[5] P. Ruiu, G. Caragnano, G. L. Masala, and E. Grosso, "Accessing cloud services through biometrics authentication," in *Proc. 10th International Conference on Complex, Intelligent, and Software Intensive Systems (CISIS)*, 2016, Fukuoka, Japan, July 2016, pp. 38–43. doi: 10.1109/CISIS.2016.76

[6] M. A. M. Escobar, C. C. Hernández, F. A. Pérez, and R. M. L. Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," *Expert Systems with Applications*, vol. 42, no. 21, pp. 8198–8211, Nov. 2015. doi: 10.1016/j.eswa.2015.06.035

[7] I. Kavati, A. M. Reddy, E. S. Babu, K. S. Reddy, and R. S. Cheruku, "Design of a fingerprint template protection scheme using elliptical structures," *ICT Express*, vol. 7, no. 4, pp. 497–500, Dec. 2021, doi: 10.1016/j.icte.2021.04.001

[8] Z. Jin, A. B. J. Teoh, B. M. Goi, and Y. H. Tay, "Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation," *Pattern Recognition*, vol. 56, pp. 50–62, Aug. 2016. doi: 10.1016/j.patcog.2016.02.024

[9] K. X. Tohari, A. Han, and F. L. J. Kun, "A fingerprint based bio-cryptographic security protocol designed for client/server authentication in mobile computing environment," *Security and Communication Networks*, vol. 4, pp. 487–499, 2011. doi: DOI: 10.1002/sec.225

[10] D. Maltoni, D. Maio, A. K. Jain, J. Feng, "Handbook of fingerprint recognition," *Springer International Publishing*, 2022. doi: 10.1007/978-3-030-83624-5

[11] D. K. Vallabhadas and M. Sandhya, "Securing multimodal biometric template using local random projection and homomorphic encryption," *Journal of Information Security and Applications*, vol. 70, pp. 103339, Nov. 2022. doi: 10.1016/j.jisa.2022.103339

[12] O. R. Gardner, H. Beale, and R. Zimmermann, "Fundamental texts on European private law," *Hart Publishing*, 2016. doi: 10.5040/9781782258674.

[13] S. Rana, O. Jadhav, S. Rajput, P. Bhansali, and V. Jyotinagar, "Homomorphic image encryption," *International Research Journal of Engineering and Technology (IRJET)*, vol. 6, no. 4, 2019.

[14] A. N. Alim and R. Fournier, *Signal and Image Processing for Biometrics*, London: ISTE Ltd and John Wiley and Sons, Inc, 2012.

[15] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, Feb. 2013. doi: 10.1016/j.ins.2012.07.049

[16] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error measurement to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, 2004.

[17] M. K. Nalini and R. K. Radhika, "Encryption on multimodal biometric using hyper chaotic method and inherent binding technique," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, 2021. doi: 10.14569/IJACSA.2021.0120772

[18] N. S. Noor, D. A. Hammood, A. Al-Naji, and J. Chahl, "A fast text-to-image encryption-decryption algorithm for secure network communication," *Computers*, vol. 11, no. 3, pp. 39, Mar. 2022. doi: 10.3390/computers11030039