BIOMETRIC DATA PROTECTION

Abdelhakim Chemlal[2], Mariem[2] Jarjar, Hassan Tabti[1], Hamid El Bourakkad[2,], Abdellatif Jarjar[2], Abdelhamid Benazzi[2]*

[1] LSIA Laboratory, FST, Sidi Mohamed Ben Abdellah University, Fez, Morocco
[2] MATSI Laboratory, ESTO, Mohammed I University, Oujda, Morocco
* Corresponding author: hassan.tabti1@usmba.ac.ma

Abstract. Biometric recognition systems are clearly vulnerable to a variety of software- and model-based attacks that can compromise different stages of the authentication process. Despite their severity, these threats are often neglected and ignored, raising critical questions: have researchers and industry stakeholders deliberately downplayed these attack risks, or is there a lack of awareness regarding the true extent of these threats? Given the serious implications of these vulnerabilities, the scientific community has proposed several countermeasures over the past two decades. Nevertheless, many persistent and sophisticated threats remain unresolved. In this work, we present a new security framework based on chaos theory and cryptographic techniques to protect confidential biometric data. After converting the biometric data into binary digital images, we apply lightweight encryption by applying bitwise Pseudo-Random binary permutation and genetic crossover to return to grayscale, to render the biometric data unintelligible and resistant to all known attacks. Extensive simulations conducted on a large and diverse fingerprint dataset have demonstrated the strong potential of this approach.

Keywords: Biometric data, S-boxes, Diffusion, Confusion, Protection, Cryptographic systems.

1 Introduction

Biometric authentication systems have made substantial advancements concerning operational efficiency, user convenience, and security when contrasted with traditional password-based approaches. Current biometric systems still require significant enhancements, as they have proven inadequate against existing attacks—let alone emerging and more sophisticated infiltration techniques. It is therefore crucial to analyse these threats, understand the knowledge and capabilities required by attackers, and explore effective countermeasures to defend against them.

Numerous studies in the literature investigate various aspects of biometric authentication techniques. However, the majority of existing research tends to focus on a single type of attack or a specific component of the biometric system. This narrow focus reveals a significant gap in comprehensive categorization and comparative analysis of the diverse

attack vectors and corresponding countermeasures within biometric authentication frameworks. As a result, both researchers and end users often lack a holistic understanding of the full threat landscape and the appropriate defensive strategies. For example, works in papers [1-12] have exclusively examined spoofing or presentation attacks. Similarly, reviews [13-20] have primarily addressed specific attacks within cancellable biometric systems.
The paper is organized into several sections. The first section outlines the various steps of the proposed method. The second section discusses the experimental results along with the security analysis. The fourth section concludes the study.

2 The suggested approach

This new strategy leverages the two most popular chaotic maps in cryptography, known for their large key space and extreme sensitivity to initial conditions, thus providing strong resistance to brute force attacks. In addition, this innovative cryptographic system is based on the following axes.

2.1 Axis 1: Chaotic Sequences selection

Our algorithm recommended the integration of the two most widely utilized chaotic maps in the cryptography domain for their ease of configuration and their marked responsiveness to initial inputs, namely logistic, skew tent maps.

- Logistic-map: The mathematical definition of this map (U_n) [14-15] is provided in Equation (1).

$$\begin{cases} u_0 \in]0{,}5\ \ 1[\quad ,\ \ \mu \in [3{,}75\ \ 4] \\ u_{n+1} = \mu u_n(1-u_n) \end{cases} \tag{1}$$

This map's Lyapunov exponent value of (Log(2)>0), indicates that it is very sensitive to beginning circumstances. Furthermore, configuring this particular card in any cryptosystem is uncomplicated.

- Skew-tent-map: The mathematical definition of the Skew Tent map (Vn) is provided in Equation (2).

$$\begin{cases} v_0 \in]0\ \ 1[\quad p \in]0{,}5\ \ 1[\\ v_{n+1} = \begin{cases} (p)^{-1}v_n & if\ \ 0 < v_n < p \\ (1-p)^{-1}\ (1-v_n) & if\ p < v_n\ < 1 \end{cases} \end{cases} \tag{2}$$

This card possesses a highly significant chaotic component for a color image encryption system. The following image encryption system is denoted by de figure below:

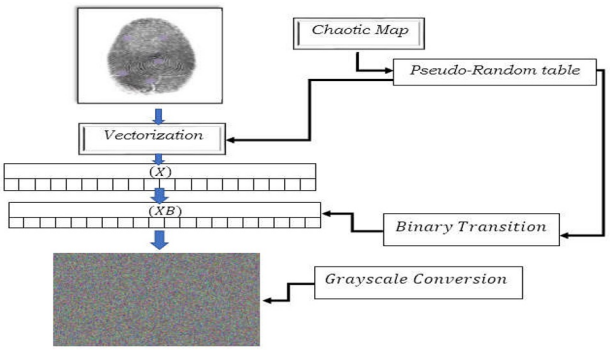

Fig. 1. Image encryption process

2.2 Axe2: Building encryption tools

This first phase, utilizes an optimized version of the Vigenère cipher at the pixel level for improved ciphering performance using two large S-Boxes. For the smooth running of this part, several parameters will be developed.

- (WC) of size (3nm; 2) confusion / diffusion table.
- (WB) of size (3nm; 2)control / decision binary table.

The construction of all these parameters is illustrated in the following diagram.:

2.2.1 Confusion/Diffusion table (***WC***) *design*

A 3nm×2 table (WC), containing coefficients in G_{256}, is employed to perform aliasing and diffusion operations at the pixel level of the original image. It has been spoken regarded as an encryption subkey, this Pseudo-Random table. The construction of this table is detailed in the algorithm 1.

Algorithm1: Confusion/Diffusion table (**WC**) design

1. $For\ \ cnt = 1\ to\ 24nm$
2. $WC(cnt;1) = \ (E(|v(cnt) - u(cnt)| * 10^{10})\%253) + 3)$
3. $WC(cnt;2) = \ (E((v(cnt) + u(cnt)) * 10^{11}\%252) + 1)$
4. $Next\ cnt$

Each single column within the array (WC) refers to an independent pseudorandom vector different from the other vectors.

2.2.2 Binary table (***WB***) *design*

Designing the binary table of size (24nm×2) is essential for controlling the cryptographic operations employed in the proposed scheme. The construction of this table is described in Algorithm 2.

Algorithm2: Binary control tables (**WB**) construction

1. $For\ cnt = 1\ to\ 24nm$
   $First\ column$
2. $if\ v(cnt) \leq u(cnt)\ Then$
3. $WB(cnt;1) = 1\ Else\ WB(cnt;1) = 0$
4. $Endif$
   $Second\ \ column$
5. $if\ WC(cnt;2) < WC(cnt;1) Then$
6. $WB(cnt;2) = 1\ Else\ WB(cnt;2) = 0$
7. $endif$
8. $Next\ cnt$

Each field in this table represents a binary array that will serve as a control mechanism for one or more ciphering processes.

2.3 Axe3: Original image preparing

2.3.1 *Image to vector conversion*

In order to reduce the correlation between adjacent pixels and maximize entropy, the original image is first obfuscated using a pseudo-random table (WC), regulated by a decision table (BT). After extracting the three color channels (RGB) and converting them into vectors (Ob), (Or), and (Og), each with dimensions 1xnm, the conversion into the vector X(x_1, x_2, ..., x_{3nm}) is performed according to the procedure described in Algorithm 3.

Algorithm3: Switching to vector

1. $for\ ct = 1\ to\ nm$
2. $If\ BT(ct; 2)\ Then$
3. $X(3ct-2) = Ob(ct) \oplus WC(3ct; 1)$
4. $X(3ct-1) = Or(ct) \oplus WC(3ct-1; 2)$
5. $X(3ct) = Og(ct) \oplus; CT(3ct-2; 1)$
6. $Else$
7. $X(3ct-2) = Or(ct) \oplus WC(3ct-1; 2)$
8. $X(3ct-1) = Ob(ct) \oplus WC(3ct; 1)$
9. $X(3ct) = Og(ct) \oplus WC(ct; 2))$
10. $End\ if$
11. $Next\ ct$

The decision-making vector $(WB(:2))$ controls the modification of the vectors's sign, effectively reducing high correlations between adjacent-pixels and maximizing entropies. This process enhances encryption strength, making it resilient against brute force and probabilistic attacks. This starting phase serves as a preliminary ciphering step for the original image. The resulting image (X) from this initial round will be subjected to the transformation to achieve a higher level of encryption. Fig. 2 depict an example of such operation.

(a) Original Image (b) Converting Image

Fig. 2. *Grayscale transition*

2.3.2 *The Original Fingerprint's Transformation*

The fingerprint's transformation unfolds across several stages, as illustrated in the Fig. 3.

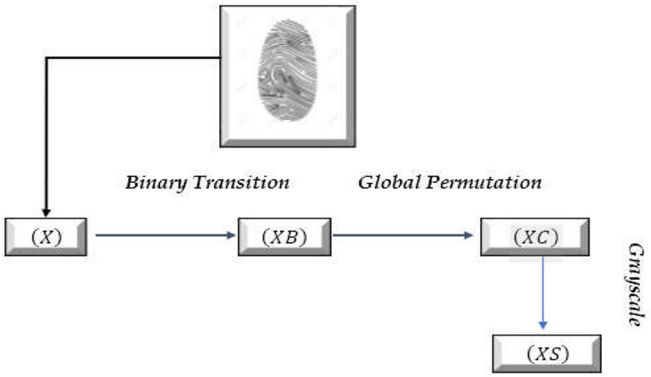

Fig. 3. Original Fingerprint's Transformation

2.3.3 *Switching to binary*

The array (X) is transformed into a binary array (XB) using the Table 1 of binary values lower than following and under the control of the vector $BT(:1)$ algorithm 3 bellow

Table 1. Table (T) of binary values

(T)	1	2
0	0	0
1	0	1
2	1	0
3	1	1

The algorithm 4 below details the Pseudo-Random conversion of vector (X) into a binary vector (XB), controlled by the decision vector $(WB(:1))$.

Algorithm4: Pseudo-Random conversion of vector (X) to binary

$For\ ct = 1\ to\ 3nm$
$x = E\left(\frac{X(ct)}{16}\right)$
$y = X(ct) - 16 * x$
$\alpha = E\left(\frac{x}{4}\right)$
$\beta = x - 4 * \alpha$
$\gamma = E\left(\frac{y}{4}\right)$
$\delta = y - 4 * \gamma$

$If\ WB(ct;1) = 0\ then$
$XB(8 * ct - 7) = T(\beta, 1)$
$XB(8 * ct - 6i) = T(\beta, 2)$
$XB(8 * ct - 5) = T(\delta, 1)$
$XB(8 * ct - 4) = T(\delta, 2)$
$XB(8 * ct - 3) = T(\alpha, 1)$
$XB(8 * ct - 2) = T(\alpha, 2)$
$XB(8 * ct - 1) = T(y, 1)$
$XB(8 * ct) = T(y, 2)$

$Else$
$XB(8 * ct - 7) = T(\delta, 1)$
$XB(8 * ct - 6i) = T(\delta, 2)$
$XB(8 * ct - 5) = T(\alpha, 1)$
$XB(8 * ct - 4) = T(\alpha, 2)$
$XB(8 * ct - 3) = T(\gamma, 1)$
$XB(8 * ct - 2) = T(\gamma, 2)$
$XB(8 * ct - 1) = T(\beta, 1)$
$XB(8 * ct) = T(\beta, 2)$
$Next\ ct$

Fig. 4 depict an example of such operation.

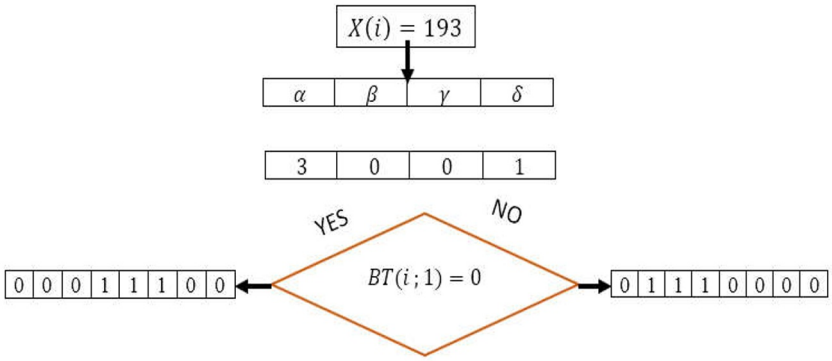

Fig. 4. Pseudo-Random binary conversion operation

This Pseudo-Random binary conversion operation is reversible.

2.3.4 *Applying a Global Swap*

The resulting vector (XB) of dimensions $(1; 24nm)$ will be subjected to the global binary rearrangement (GB) given by an increasing sorting on the $24nm$ values of the sequence (W) for the design of the vector (XC) of the same size, obtained by applying the algorithm 5 below:

Algorithm5: Global Swap application

1. $For\ ct = 1\ to\ 3nm$
2. $XC(ct) = XB\big(GB(ct)\big) \oplus \mathrm{BW}(ct; 2)$
3. $Next\ ct$

2.3.5 *Back to grayscale*

The transition to grayscale goes through the following steps:

- Switching to $\mathbb{Z}/4\mathbb{Z}$

The vector (XC) is divided into two subvectors $(XC1), (XC2)$, each of size $(1; 12nm)$. A cross-section table $(TD1)$ of size $(12nm; 3)$ is generated using the following procedure:

✓ The columns (1), (2), and (3) are the permutations (Qr1) which indicates the bit index of the vector (XC1), (Qr2) which indicates the bit index of the vector (XC2), and (Qr3) which indicates the bit index of the vector (XC1). These columns are obtained by a crossing sort on the 12nm value of the sequences (W), (U), and (V).

The construction of all columns is described by the algorithm 6.

Algorithm6: Back to grayscale

1. $For\ ct = 1\ to\ 12nm$
2. $TD(ct; 1) = Qr1(ct)$
3. $TD(ct; 2) = Qr2(ct)$
4. $TD(ct; 3) = Qr3(ct)$
5. $Next\ ct$

The generation of the vector (XV) is described by the algorithm 7.

Algorithm7: Generation of the vector (XV)

1. $For\ ct = 1\ to\ 12nm$
2. $If\ not(BT(ct\,;2))\ Then$
3. $XV(TD(i;3)) = XC1(TD(ct;1)) * 2 + XC2(TD(ct;2))$
4. $XV(TD(ct;3)) = XC2(TD(ct;2)) * 2 + XC1(TD(ct;1))$
5. $Next\ ct$

Fig. 5 depict an example of such operation.

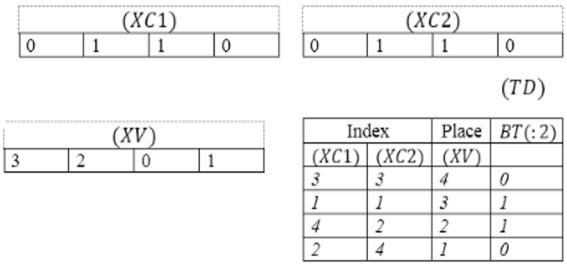

Fig. 5. Generation of the vector (XV) example

- Switching to $\mathbb{Z}/\mathbf{256}\mathbb{Z}$

The vector (XV) is divided into four subvectors $(XV1), (XV2), (XV3), (XV4)$ each of size $(1; 3nm)$. A cross-section table (TE) of size $(3nm; 5)$ is generated. The field (1) is a rearrangement (Sr1) given by a crossing sort on the 3nm value of the sequence (WC(: 1)). This column indicates the bit index of the vector (XV1). The field (2) is a rearrangement (Sr2) given by a crossing sort on the 3nm value of the sequence $\big(\mathrm{WC}(:2)\big)$. This field indicates the bit index of the vector (XV2). The field (3) is a rearrangement (Sr3) given by a crossing sort on the 3nm value of the sequence (u). This field indicates the bit index of the vector (XV3). The field (4) is a permutation (Sr4) given by a crossing sort on the 3nm value of the sequence (v). This field indicates the bit index of the vector (XV4). This field indicates the position of the calculated number within the generated vector (XS).
This construction technique is given by the algorithm 8.

Algorithm8: Switching to Z/256Z

1. $For\ i = 1\ to\ 13m$
2. $TE(i;1) = Sr1(i)$
3. $TE(i;2) = Sr2(i)$
4. $TE(i;3) = Sr3(i)$
5. $TE(i;4) = Sr4(i)$
6. $TE(i;5) = Sr3(i)$
7. $Next\ i$

The generation of the vector (XS) is given by the algorithm 9 below:

Algorithm9: Generation of the vector (XS)

1. $For\ ct = 1\ to\ 13m$
2. $If\ not(BT(ct\,;1))\ Then$
3. $XS(TE(ct;5)) = XV1(TE(ct;1)) * 64 + XV2(TE(ct;2) * 16) + XV3(TE(ct;2) * 4) + XV4(TE(ct;2)$
4. $Else$
5. $XS(TE(ct;5)) = XV1(TE(ct;1)) * 16 + XV2(TE(ct;2) * 4) + XV4(TE(ct;2) * 64) + XV3(TE(ct;2)$
6. $XS\big(TE(ct;5)\big) = VG(XS\big(TE(ct;5)\big) \oplus CT(ct;3)$
7. $Next\ ct$

The vector (XS) represents the encrypted image of the fingerprint.

3 System Simulation and Evaluation

Our simulation is conducted on a substantial number of randomly selected images from an extensive database will be processed using our proposed algorithm. The resulting performance metrics will be presented and compared with those of other existing technologies. It is understood that a robust algorithm is one capable of effectively countering any known attacks. An example of reference images subjected to the evaluation of our new algorithm is illustrated in Fig. 6.

Fig. 6. Example of image encrypted using the proposed scheme

3.1 Cryptographic key space evaluation

Brute-force attacks are cryptanalytic techniques that aim to discover the ciphering key in a systematic manner evaluating every possible combination. As a result, a larger encryption key makes such attacks increasingly impractical. In our algorithm, the secret key size exceeds 2^{128} [13-14-15], ensuring robust protection against brute-force efforts. For the simulation, the secret key is generated using three of the most commonly applied chaotic maps in cryptography. This results in a key comprising six parameters, each represented by 32 bits, yielding an overall size of$(2^{6*32}) = (2^{192}) \gg (2^{100})$.

3.2 Assessment of Key Sensitivity

The chaotic maps utilized in our algorithm demonstrate a high sensitivity to initial conditions. As a result, even a small perturbation in any parameter involved in the regeneration of the secret key will produce a different key, leading to the generation of distinct chaotic vectors. This notable sensitivity of the key in our proposed approach is exemplified in Fig. 7.

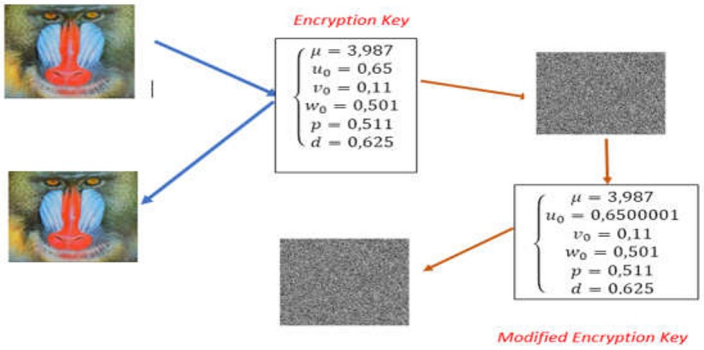

Fig. 7. Ciphering key sensibllity

A variation order of 10^{-7} in a single input is insufficient to restore the plain image.

3.3 Probabilistic Attacks Evaluation

To validate the effectiveness of the proposed data cipher technique against probabilistic attacks, several tests were conducted on various images, with the most notable results presented.

3.3.1 Histogram's analysis

A histogram represents the frequency of pixels corresponding to each grayscale in an image. The x-axis indicates the color levels, ranging from 0 to 255, while each vertical bar shows the number of occurrences of a specific color level. From a cryptographic perspective, the color distribution in an encrypted image is of particular significance, as it may reveal information about the original image. Conversely, if the histogram of the encrypted image is flat and uniform, it implies that no useful information can be extracted regarding the plain picture or the interdependence between them. Outcomes of simulated experiments of the suggested scheme are given in Fig. 6.

3.3.2 Entropies analysis

The concept of entropy is fundamental in cryptography, as it measures the randomness or unpredictability of a system. It is essential for assessing the security of cryptographic algorithms, particularly in the domains of encryption, key generation, and secure communication. Originating from information theory, developed by Claude Shannon, entropy quantifies the uncertainty or degree of randomness within a system. The entropy Ep(X) of a random variable X, with possible values s_i and corresponding probabilities $PI(x_i)$, is given by Equation 3.

$$\mathrm{Ep}(X) = -\sum_{i=0}^{255} PI(s_i) * log\big(PI(s_i)\big) \tag{3}$$

Throughout our simulations, the entropy of the encrypted pictures remains very close to the maximum measure of 8, as shown in Figure 8. This indicates that our algorithm is resilient to any entropy-based attacks.

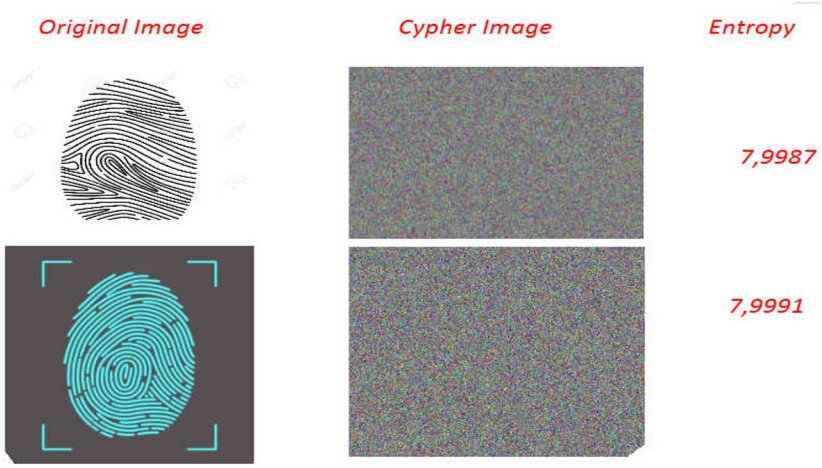

Fig. 8. Example of encrypted images entropy

3.4 Analysis of differential constants

Consider two encrypted images, C1 and C2, whose corresponding plaintext images differ by only a single pixel. The NPCR (Number of Pixels Change Rate) mathematical analysis for an image is expressed by the equation (4).

$$NPCR = \left(\frac{1}{nm} \sum_{i,j=1}^{nm} D(i,j) \right) * 100 \quad (4)$$

$$With \quad D(i,j) = \begin{cases} 1 & if \quad C_1(i,j) \neq C_2(i,j) \\ 0 & if \quad C_1(i,j) = C_2(i,j) \end{cases}$$

The mathematical analysis of the UACI (Unified Average Changing Intensity) for an image is given by Equation (5).

$$UACI = \left(\frac{1}{nm} \sum_{i,j=1}^{nm} Abs\big(C_1(i,j) - C_2(i,j)\big) \right) * 100 \quad (5)$$

Table 2. The UACI and NPCR values for selected images

Images	UACI	NPCR
Image1	33.43	99.62
Image2	33.44	99.61

The values presented in Table 2, estimated for the chosen pictures tested with the suggested method, fall within widely accepted benchmarks. Notably, the NPCR value is near to 99.60%, and the UACI value exceeds 34.40%. These outcomes demonstrate that the suggested scheme is robust against differential attacks, with this security primarily ensured by the first round of encryption.

4 Conclusion

This strategy yields simulation results based on randomly selected images from image databases, utilizing a single Vigenere lap generated from two new substitution sboxes. The inclusion of two Feistel rounds at the bit level introduces additional dynamics to the system. The use of genetic crossover at the bit level, managed by chaotic crossover tables for Pseudo-Random gray-level feedback, has significantly enhanced the time complexity of potential attacks. The results obtained have been both encouraging and promising.

References

[1] BAAQEEL, Hind et OLUSANYA OLATUNJI, Sunday. Spoofing detection on adaptive authentication System-A survey. IET Biometrics, 2022, vol. 11, no 2, p. 87-96. https://doi.org/10.1049/bme2.12060

[2] Ali, S.F., Khan, M.A. & Aslam, A.S. Fingerprint matching, spoof and liveness detection: classification and literature review. Front. Comput. Sci. 15, 151310 (2021). https://doi.org/10.1007/s11704-020-9236-4

[3] Z. Jia, C. Huang, Z. Wang, H. Fei, S. Wu and J. Feng, "Finger Recovery Transformer: Toward Better Incomplete Fingerprint Identification," in IEEE Transactions on Information Forensics and Security, vol. 19, pp. 8860-8874, 2024. https://doi.org/10.1109/TIFS.2024.3419690

[4] CHOCHOWSKI, *Marcin. The template selection in biometric systems based on binary iris codes. Journal of Telecommunications and Information Technology, 2010, no 4, p. 86-92.* https://doi.org/10.26636/jtit.2010.4.1100

[5] S. Sharma and V. Balasubramanian, "A biometric based authentication and encryption Framework for Sensor Health Data in Cloud," Proceedings of the 6th International Conference on Information Technology and Multimedia, Putrajaya, Malaysia, 2014, pp. 49-54, https://doi.org/10.1109/ICIMU.2014.7066602

[6] TOOSI, Amirhosein. Feature Fusion for Fingerprint Liveness Detection. 2018.

[7] Baghel, V.S., Prakash, S. & Agrawal, I. An enhanced fuzzy vault to secure the fingerprint templates. Multimed Tools Appl 80, 33055–33073 (2021). https://doi.org/10.1007/s11042-021-11325-w

[8] Ametefe, D.S., Sarnin, S.S., Ali, D.M. et al. Enhancing Fingerprint Authentication: A Systematic Review of Liveness Detection Methods Against Presentation Attacks. J. Inst. Eng. India Ser. B 105, 1451–1467 (2024). https://doi.org/10.1007/s40031-024-01066-3

[9] Tarif*, E.B., Wibowo, S., Wasimi, S. et al. A hybrid encryption/hiding method for secure transmission of biometric data in multimodal authentication system. Multimed Tools Appl 77, 2485–2503 (2018). https://doi.org/10.1007/s11042-016-4280-7*

[10] Maltoni, D., Maio, D., Jain, A.K., Feng, J. (2022). Securing Fingerprint Systems. In: Handbook of Fingerprint Recognition. Springer, Cham. https://doi.org/10.1007/978-3-030-83624-5_9

[11] Marasco, E., Albanese, M. (2021). FingerPIN: An Authentication Mechanism Integrating Fingerprints and Personal Identification Numbers. In: Singh, S.K., Roy, P., Raman, B., Nagabhushan, P. (eds) Computer Vision and Image Processing. CVIP 2020. Communications in Computer and Information Science, vol 1376. Springer, Singapore. https://doi.org/10.1007/978-981-16-1086-8_44

[12] Galbally, R. Haraksim and L. Beslay, "A Study of Age and Ageing in Fingerprint Biometrics," in *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 5, pp. 1351-1365, May 2019. *https://doi.org/*10.1109/TIFS.2018.2878160

[13] YANG*, Wencheng, WANG, Song, HU, Jiankun, et al. Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 2019, vol. 11, no 2, p. 141.* https://doi.org/10.3390/sym11020141

[14] K. Simoens, J. Bringer, H. Chabanne and S. Seys, "A Framework for Analyzing Template Security and Privacy in Biometric Authentication Systems," in IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 833-841, April 2012, https://doi.org/10.1109/TIFS.2012.2184092

[15] N. K. Ratha, S. Chikkerur, J. H. Connell and R. M. Bolle, "Generating Cancelable Fingerprint Templates," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561-572, April 2007, https://doi.org/10.1109/TPAMI.2007.1004

[16] K. Nandakumar and A. K. Jain, "Biometric Template Protection: Bridging the performance gap between theory and practice," in IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 88-100, Sept. 2015. https://doi.org/10.1109/MSP.2015.2427849

[17] Marta Gomez-Barrero, Javier Galbally, Reversing the irreversible: A survey on inverse biometrics, Computers & Security, Volume 90, 2020, 101700, ISSN 0167-4048. https://doi.org/10.1016/j.cose.2019.101700

[18] DONG*, Xingbo, PARK, Jaewoo, JIN, Zhe, et al. On the risk of cancelable biometrics. arXiv preprint arXiv:1910.07770, 2019.* https://doi.org/10.48550/arXiv.1910.07770
[19] Manisha, Kumar, N. Cancelable Biometrics: a comprehensive survey. Artif Intell Rev 53, 3403–3446 (2020). https://doi.org/10.1007/s10462-019-09767-8
[20] V. M. Patel, N. K. Ratha and R. Chellappa, "Cancelable Biometrics: A review," in IEEE Signal Processing Magazine, vol. 32, no. 5, pp. 54-65, Sept. 2015. https://doi.org/10.1109/MSP.2015.2434151