A FUZZY VAULT DEVELOPMENT BASED ON IRIS IMAGES

Mohammed A. Taha✉

*Department of Computer Sciences¹
cs.19.54@grad.uotechnology.edu.iq*

Hanaa M. Ahmed

Department of Computer Sciences¹

¹University of Technology

Alsinaa str., Baghdad, Iraq, 19006

✉ Corresponding author

Abstract

Biometric systems gather information from the person's biometric attributes, used extensively to authorize the individuals. Due to the obvious convenience of using specific individual traits such as face, fingerprints, palm veins, and irises, biometric authentication is becoming more common. In particular, Iris systems are in high demand for high-assurance applications, because they contain a broad feature set and remain stable. Authentication methods based on iris biometrics are now commonly used in a variety of fields. This is due to the fact that iris biometric authentication is both safer and more comfortable than conventional passwords. Template Security is a major concern in biometric systems. The template security mechanism ensures reusable, permanent, and un-linkable models. The Fuzzy Vault strategy is one of the most popular security schemes for Template protection.

Fuzzy vault has demonstrated to be an effective protection method but lacks revocability and security attacks. This article introduced an improved fuzzy vault system. The improved fuzzy vault system was introduced, which uses more than one key to protect biometric data. Different keys make the search space more detailed. The additional key was used to encrypt vault data, which stopped the intruder from accessing the information on the person's biometry. The system was tested using CASIA.v1 and IITD.v1 datasets, and findings showed that the system ensures the protection and authentication of the iris templates without compromising performance. The proposed modification gave a 0.0 % False Accepted Rate (FAR) for both the dataset and False Rejected Rate (FRR), 0.14 % for CASIA v1 and 0.12 % for IITD v1 False Rejected rate.

Keywords: Authentication, Biometrics, Fuzzy vault, Iris, Template protection, GLCM, CASIA v1, IITD v1, FAR, FRR.

DOI: 10.21303/2461-4262.2021.001997

1. Introduction

Motivation: Biometrics is a social identity analysis to authenticate or identify substance characters. Identification of biometrics people by their biological attributes, including fingerprint, iris, retina, hand anatomy, face, palm scanning or some forms of actions such as signature, gesture, and voice. Biometric technology requires massive biometric volumes template construction data that causes severe privacy leakage [1, 2]. Biometric authentication offers excellent protection because, instead of smart cards or text passwords, biometric forgery or fraud is very difficult to lose or forget. Biometric security and safety are widely used, primarily due to the precision and uniqueness of biometric features such as Iris. And there are also other attacks that the biological systems experience, such as the brute force attack, position attack, correlation attack, etc. Biological system stability is a significant threat. Thus, the safe security of biological templates caught the attention of people [1].

Contributions. This article's main aim is to propose a new improvement with an iris prototype of the fuzzy vault scheme. Typically, a biometric framework's accuracy is calculated by its False Accepted Rate (FAR) and False Rejected Rate (FRR), also known as matching accuracy [3]. To ensure accuracy, let's strive to reduce the FAR rate. Furthermore, let's aim to minimize FRR as well as time for successful authentication and usability. However, since the traditional fuzzy vault scheme uses a single biological template and the biological function parameters are stored directly in the fuzzy vault, the biological template will not be adequately protected.

To address this problem, let's propose a novel fuzzy vault scheme based on the encryption of the vault, which makes it resist the correlation and brute force attack on the fuzzy vault using the iris template.

Fuzzy vault schema, first implemented in [2], was a well-known biometric system cryptographic architecture. Because of the increasing use of biometric authentication, the fuzzy vault cryptosystem has become a well-studied research field [4]. The author proposes a shift to the fuzzy vault [5]. An additional layer of security is introduced using a password to achieve a high degree of protection. This program offers a high level of security from a secure password. If the password fails, it is similar to the standard fuzzy method. Only the same password would harden the secret key derived from the same prototype. The hardening method requires the following steps. First, the recognition system has a random user password processing feature. Second, the fuzzy vault framework then protects the transformed prototype. Finally, the vault is secured by a password-based key. The author proposes to boost the fuzzy vault scheme in [6]. An iris shuffling algorithm is used in the framework to ensure the revocable iris template based on three key aims: first, no template information should be leaked from the stored data. Second, templates can be withdrawn; once they are infected, they can be released without recovering the iris. Third, the fuzzy vault against the correlation attack should be safe. Source of reference not found. So it is not possible to compare the fuzzy vaults of the same design to determine the key used for building the fuzzy vault. In [7], the author of the article suggests a new way of solving the problems of the new fuzzy vault based on CRC. An updated generator and verifier of chaff points were added. In order to create structural chaff points at the registration stage, continuous hashing and linear projection are used. As a result, the same chaff points are regenerated for the final decision during the authentication stage. The proposed system treats chaff points as a signature for the secure key and biometric template combination. Any changes on the decoded vault are detected during the authentication process to avoid the assault of mixing substitutions. The author proposed a new fuzzy vault schema method. In [8, 9], the authors proposed a modified fuzzy vault framework, A 128-bit Advanced Encryption Standard (AES) key combination of iris data. Experimental results demonstrated that the 128-bit cryptographic keys and iris models with a fuzzy vault system were stable. There are two benefits and improvements to the new method. First, it was implemented as a pattern clustering method to address the variance in extracted iris features. Second, it was used to create fuzzy vault sets as an iris extraction algorithm based on the Independent Component Analysis (ICA). In [10], the author suggested that several models for a user be protected as a single entity. A fuzzy vault system was used to derive one multi-biometric template from individual templates. It shows that a multi-biometric vault offers better identification and more excellent protection than a uni-biometric vault. The proposed method achieves a better value of Genuine Accepted Rate (GAR) and False Accepted Rate (FAR) compared to the uni-biometric fuzzy vault. It also provides higher security than uni-biometric systems.

2. Materials and methods

Fuzzy vault is the primary biometric binding cryptographic in different applications; the fuzzy vault method has been widely studied and considered. Fuzzy vault only receives unordered input. A fuzzy vault must be translated into an unordered set of biometrics with features in an ordered set. Assume that B is a biometric prototype with f -points. A secret key K is selected and is encrypted, say as coefficients, into a polynomial P with a degree d . Biometric prototype characteristics are now based on the polynomial. Any random points are introduced to cover the genuine elements, which do not cheat on the P polynomial. As shown in **Fig. 1**, such random points are named chaff points [2, 11].

When the user submits a biometric request B , authentication is completed if the key K is regenerated only if B overlaps with A and authentication is successful, as shown in **Fig. 2** below.

On the opposite, regeneration of K is unlikely if there is insufficient overlap between A and B , authentication is ineffective. Reed Solomon (RS) procedures are used to correct the polynomial error. The inefficiency of the polynomial reconstruction is based on the non-vulnerability of this approach.

Fig. 1. Fuzzy vault encoding process [12]

Fig. 2. Fuzzy vault decoding process [12]

2. 1. Proposed System

This section explains the formal structure of our proposed scheme. The framework contains the following modules.

2. 1. 1. Vault Encoding

The method of vault encoding or registration is implemented as follows in our cryptosystem. Fig. 3 demonstrates the registration process of the device model proposed.

Iris image template extraction. The user's iris image is provided as an input in the registration process. The grey level co-occurrence matrix (GLCM) texture extraction methods [13–15] have been used to extract iris textures features.

Chaff Points Generation. To hide the real points of a potential attacker, random chaffs points are produced to provide a fair balance between the complexity and the performance of brute force attacks.

Polynomial Projection. The fuzzy vault system is a set of (X, Y) tuples, defining (X, Y) the system coordinate. The first dimension of a tuple vault, X , has a fixed value. The second dimension, Y , is generated randomly under certain conditions. Any genuine point X is drawn to the secret polynomial p , and the resulting value is saved as the second tuple variable, i. e., $Y=p(X)$. The polynomial mapping is carried out in a Galois field (GF) so that exact polynomial interpolation is

possible in vault decoding. Then, in the potential results space of polynomial projection, the chaff points are randomly mapped to a number in order not to lie on the polynomial. This mapping gives the second tuple element, Y , where Y corresponds to $p(X)$ [16, 17].

Fig. 3. Modified fuzzy vault schema

Vault encryption. The proposed change uses vault encryption. There is a suggested improvement that uses more than one key to protect encrypted biometric information. The additional keys ($K2$) used to encrypt vault data expand the search space. An attacker could not use the decoding algorithms to obtain information about user biometrics by inserting the extra key. The keyspace for the cryptographic scheme is the cumulative number of separate keys that need to be used. The safety of the algorithm depends on the key size. The high length key, the more secure the algorithm will be against a brute force attack. The main length is represented uniformly as a number of key bits [17]. A key N -bit length has the 2^N keyspace choices. The keyspace size should not be less than 2^{100} from the cryptographic perspective to provide a high degree of security [18].

Vault Scrambling and permutation. The Vault tuples with genuine points can't be separated from the tuples with chaff points by fusing the encrypted vault.

2. 2. Vault Decoding

Vault decoding or authentication is applied, as seen in Fig. 4.

Fig. 4. Authentication in the proposed system

Iris Image and Fuzzy Vault. The iris image template is extracted from GLCM in the registration process, and the actual (claimed) user's fuzzy vault provided from the database (DB) by using its unique identifier (id) as an input to the verification algorithm.

Vault Decryption. A particular key (K_2) was used during the validation process to decrypt the locked vault during the enrollment phase.

Polynomial Interpolation. Polynomial interpolation shall be performed unless the size of a candidate set at the end of one iteration with two different bases is greater than polynomial degree plus one ($n+1$). The hidden polynomial can't be interpolated if fewer candidates are found. In the case of sufficiently vault tuples, all sub-sets of size $n+1$ must be evaluated, as not all candidate vertices have genuine points. The interpolation of Lagrange in a Galois field (GF) (2^{32}) for each sub-set is achieved by using $n+1$ vault tuple, interpreted as (X, Y) sample points with X and Y being respectively, the first and second variable for the vault tuple.

Correct Secret. When no intrusion is encountered, the proper secret key (k_1) is found as well as the user is tested successfully.

3. Results and discussions

The simulation parameters used for implementation are presented in this section. It also analyzes the attack by brute force and the attack by correlation to show the consistency of the proposed method.

3. 1. Performance evaluation

3. 1. 2. Database

Both CASIA v1 [19] and the IITD Iris Image database [20] will be tested for the proposed method.

CASIA v1 consists of 756 iris images of 108 persons and seven images each taken during two separate sessions with a difference of at least one month. Both 8-bit grey images are 320 to 280 resolution and preserved in bitmap format [19].

In our experiments, let's use two key images, one for registration and the other for testing. Fig. 5 below shows some database examples.

Fig. 5. Iris images samples: *a* – CASIA v1 image [19]; *b* – IITD.v1 image [20]

The IITD.v1 image database mainly consists of iris pictures obtained from IIT Delhi students and staff.

This database was compiled by JIRIS, JPC1000, and digital CMOS camera in the Biometrics Research Laboratory from January to July 2007. The collected images have been stored in bitmap format. The database includes 2,240 images from 224 different users that are freely available to researchers. In the sample, all subjects aged 14–55 years consist of 176 men and 48 women. These pictures are 320×240 pixels in size, and all these photographs have been acquired indoors [20].

3. 1. 2. Parameter Values

Different parameters settings can be seen in Table 1.

In Table 1, there are the variables used in the proposed system for evaluation and analysis.

Table 1
Parameters setting

Parameters	
Genuine points number g	8
Chaff points number c	400
Total vault points v	408
Polynomial degree n	9

3. 1. 3. Performance

With the False Accept (FAR) and False Reject Ratios (FRR), the performance of the proposed iris-based fuzzy vault system was assessed, as seen in **Table 2**.

Table 2
Proposed system performance

Dataset	FAR	FRR	Time
CASIA.v1	0.0	0.16	0.145 ms
ITTD.v1	0.0	0.12	0.133 ms

FAR represents the number of accurate key retrievals by non-authentic device users. FRR represents the number of refusals for actual machine users [21].

3. 1. 4. Security Analysis

To extract a hidden polynomial $P(x)$ with a polynomial degree (n), a subset of $(n+1)$ vault pairs shall be required. In this case, all $(n+1)$ pairs of vault elements must contain genuine points (g), and Chaff points (c) are not concealed. In all $(v = g+c)$, vault pairs are assumed in the fuzzy vault where (v) is the total number of points in the vault, (g) is the number of genuine points, and (c) is the number of chaff points identified in vault formation. This makes it possible for the attacker $v_s = (n+1)^V$ vault size pair sub-sets $(n+1)$ overall. $g_s = (n+1)^g$ subgroups contain genuine points from these sets, which can be used to interpolate the hidden polynomial properly. This leaves $(c_s = v_s - g_s)$ pair subsets were containing genuine pairs but include at least one pair of pairs of vaults. If the chaff vault pair is only one member of the candidate sub-set $(n+1)$, the secret polynomial fails because the chaff vault pair does not lie on the secret polynomial [10]. The attacker doesn't know which vault pairs have genuine points, so they can only pick one sub-set, again and again, to interpolate at random.

An attacker needs to find an appropriate subset for accurate interpolation of the secret key to determine the estimated number of attempts [21, 22]:

$$totalattempts E(g,c) = \frac{v+1}{g+1} = \frac{\left((n+1)^v + 1\right)}{\left((n+1)^g + 1\right)} = \frac{\frac{v!}{(n+1)(v-n-1)!}}{\frac{g!}{(n+1)(g-n-1)!}}. \quad (1)$$

Let's also note from (1), which shows the number of attempts the attacker needs to break the system and obtain sensitive user information. Therefore, the proposed modification to the fuzzy vault method ensures that the number of attempts increases in a balanced manner consistent with the length of the key ($K2$) used in the fuzzy vaults encryption, which gives additional strength and protection to sensitive information. Therefore, (2) is as follows:

$$totalattempts E(g,c) = \frac{v+1}{g+1} = \frac{\left(\frac{(n+1)^v + 1}{(n+1)^g + 1}\right)}{\frac{\frac{v!}{(n+1)(v-n-1)!}}{\frac{g!}{(n+1)(g-n-1)!}}} + 2^{encryption\ key\ (K2)\ length}. \quad (2)$$

To determine the expected time for a potential attacker to access a fuzzy vault by subset interpolation randomly, let's multiply the estimated time (T) to select a genuine portion with the average time per subset of Lagrange interpolation:

$$Time = \left(\frac{v+1}{g+1} + 2^{encryption\ key\ (K2)\ length} \right) \cdot T. \quad (3)$$

Let's recognize, the average duration of interpolation increases with the polynomial degree (n). Let's summarize the effect of the (g , c , and n) parameters on the estimated time an attacker has to release the secret and present the expected value $total\ attempts\ E(g_s, c_s)$ with expanded polynomial coefficients to better display the security impact.

The expected value $total\ attempts\ E(g_s, c_s)$ decreases as only the denominator increases, so protection decreases. The expected value $total\ attempts\ E(g_s, c_s)$ increase as encryption key length increased. Expanding the number of chaff points c , $total\ attempts\ E(g_s, c_s)$ also increases, with $(v = g+c)$ increasing in the nominator. The attacker, therefore, requires further attempts to open the vault on average. Both binomial coefficients of nominators and denominators change by increasing the polynomial degree n .

3. 2. Biometric systems attacks

A variety of attacks are introduced in the biometrics framework. However, attacks on safe models significantly reduce the reliability of the biometric system. The attacks based on the template are either brute force, correlation, known key, replacement, or hill climb attacks. This work focused on both brute force and correlation attacks.

3. 2. 1. Brute force attack

An attacker tries every possible bit mixture in this type of attack before the correct data is calculated or the key is retrieved for the original function. The basic fuzzy vault depends on the degree of the polynomial. The attacker can quickly restore a lower polynomial degree. Higher degree polynomial provides increased stability [23, 24]. Polynomial degree n in the fuzzy vault, the attacker has to try for brute force ($g, n+1$) of $g+1$ element combinations, as seen in (1). The proposed modification to the standard fuzzy vault method should increase the number of attempts that the attacker makes to obtain sensitive information, as shown in (2); therefore, getting sensitive information for the user takes a very long time, as shown in (3).

3. 2. 2 Correlation attack

In the case of a correlation attack, at least two vaults belong to one individual. Two different ways can generate the vaults: (1) the fuzzy vault is formed using similar genuine points with different hidden key($k1$). (2) equivalent genuine points with various chaff points. Let the assailant two vaults be intercepted containing two points (pts) and (pts'). An attacker's goal is to find some transformation on points (pts'). i. e ($Transform\ (pts')$). Whether $distance \leq threshold$ (Th), transformed characteristics of $\{Transform\ (pts'), (pts')\}$ correlate with (pts). Let V consists of fuzzy pairs of vaults $\{pts\}$ with $distance(pts, Transform(pts')) \leq Th$. The error-correcting procedure, Reed Solomon decoder (RS), can be used to open the vault when matching pairs of (pts, pts') is lower than pairs not paired [24, 25]. Assume that genuine and chaff (pts) and (pts') are equal in size. There are points of (pts) genuine and chaff points of (pts'). The proposed modification to the fuzzy vault method should prevent a correlation attack, as encryption for the data prevents interconnection

between the data, as it is possible to encrypt the data of each user with a random key that differs from the other user, which helps prevent penetration and protect the iris template.

Table 3 compares the proposed Fuzzy Vault with the current polynomial degree 8 methods with the CASIA v1 dataset. Genuine Acceptance Rate (GAR) is defined as a percentage of the system's approved genuine users. It is given by $GAR = 100 - FRR$ [26–28].

Table 3
Methods comparison

Method	FAR	GAR	Brute force attack solution	Correlation attack solution
Proposed method	0.0	86.0	yes	yes
E. Srinivasa Reddy [3]	0.03	92.0	no	no
E. Srinivasa Reddy [5]	0.0	90.2	yes	no
Youn Joo Lee [26]	0.0004	73.686	no	no

Through **Table 3**, it is clear that the proposed method gives good results compared to other methods and provides solutions for correlation and brute force attacks.

The results of the proposed system displayed in **Table 2** are greatly influenced by the threshold value used. It represents the difference between enrolled template and query template so it must be chosen carefully. Specific use and security considerations must be taken into account when choosing the optimal parameters. For good performance, various thresholds have been made. It always depends on the context of use to decide between security and usability. There is some degradation in the GAR because of in some cases, features could not be reliably extracted from a relatively large region in the iris pattern due to factors like occlusion reflection, motion blur, contrast variation, pupil dilation, blurred image, partially open eye and defocused image. This problem can be compensated by overlooks the occluded regions in the Euclidean distance calculation. However, this problem can't be handled effectively by the proposed system leading to further false rejections. Both CASIA.1 and ITTD.1 has (0.0 %) FAR, making it suitable for a high-security application.

The main advantage of the proposed modification of fuzzy vaults adds a second layer of security against the attacker, even if the attacker succeeds in unlocking the vaults and receiving the key but still can't receive the original template as the encrypted template version has to be solved to get feature points and adds more complexity in our fuzzy vault. The proposed modification ensures that the attacker will increase the number of attempts needed to break the system and obtain sensitive user information, thus providing an effective solution to the brute force attack and correlation attack. This increase in the number of attempts depends the key length (K_2) used to encrypt fuzzy vault, giving additional strength and protection to sensitive information.

From a cryptographic standpoint, it's worth noting that the fuzzy vault architecture solves the key management problem, which is a big problem in real-world cryptosystems. The prototype implementation and experimental results indicate that a realistic application of this cryptosystem is possible, as it is more secure than commonly used iris recognition algorithms without compromising quality or runtime efficiency. At the same time, it increases the stability of existing cryptosystems by resisting correlation and brute force attacks. As a consequence, let's assume it is a viable alternative for safe and functional distributed authentication. Despite the apparent benefit of the proposed modification, it adds some complexity and extra time to encrypt and decrypt data, which is one of the disadvantages of the proposed system.

Fuzzy vault is most importantly secure due to the complexity of polynomial reconstruction and the number of randomly generated chaff points. However, the proposed system's security is also largely dependent on the encryption key length. Clearly, the higher the degree polynomial and the more chaff points, the more difficult it is to recover the true polynomial $P(x)$ for the fusion points. The addition of more chaff points or polynomial degrees will have a direct influence on runtime. The balance between security and the best usage should be determined on each specific application.

As a biometric, the proposed system is based only on the iris. Using multiple biometrics to generate fuzzy vaults that all have to be matched to authenticate is one way to improve security. Using passwords plus biometrics will enhance the system's efficiency.

4. Conclusion

This research has developed and constructed a biometric cryptosystem based on a fuzzy vault that can be utilized for authentication with strong privacy and protection. The implemented scheme uses another hidden based encryption layer to protect the vault data in the original fuzzy vault schema. The proposed system would increase the search space to make the intruder more complicated and challenging to use the template data. When testing the proposed system, it gave 0.0 % acceptable error rate (FAR) for both dataset and false rejection rate (FRR), 0.14 % for CASIA v1 and 0.12 % for ITTD v1 as well as solving the problem of brute force attack and correlation attack on the contrary, to the rest of the previous systems that give a higher FRR, but do not put solutions to these attacks.

Acknowledgements

Part of the work described in this paper is based on CASIA-IrisV1 collected by the Institute of Automation of the Chinese Academy of Sciences (CASIA).

References

- [1] You, L., Wang, T. (2018). A novel fuzzy vault scheme based on fingerprint and finger vein feature fusion. *Soft Computing*, 23 (11), 3843–3851. doi: <https://doi.org/10.1007/s00500-018-3046-8>
- [2] Juels, A., Sudan, M. (2006). A Fuzzy Vault Scheme. *Designs, Codes and Cryptography*, 38 (2), 237–257. doi: <https://doi.org/10.1007/s10623-005-6343-z>
- [3] Reddy, E. S., Babu, I. R. (2008). Authentication Using Fuzzy Vault Based on Iris Textures. 2008 Second Asia International Conference on Modelling & Simulation (AMS). doi: <https://doi.org/10.1109/ams.2008.112>
- [4] Prabhakar, S., Pankanti, S., Jain, A. K. (2003). Biometric recognition: security and privacy concerns. *IEEE Security & Privacy*, 1 (2), 33–42. doi: <https://doi.org/10.1109/msecp.2003.1193209>
- [5] Reddy, E. S., Babu, I. R. (2008). Performance of Iris Based Hard Fuzzy Vault. 2008 IEEE 8th International Conference on Computer and Information Technology Workshops. doi: <https://doi.org/10.1109/cit.2008.workshops.20>
- [6] Fouad, M., El Saddik, A., Zhao, J., Petriu, E. (2011). A fuzzy vault implementation for securing revocable iris templates. 2011 IEEE International Systems Conference. doi: <https://doi.org/10.1109/syscon.2011.5929061>
- [7] Nguyen, M. T., Truong, Q. H., Dang, T. K. (2016). Enhance fuzzy vault security using nonrandom chaff point generator. *Information Processing Letters*, 116 (1), 53–64. doi: <https://doi.org/10.1016/j.ipl.2015.08.012>
- [8] Lee, Y. J., Bae, K., Lee, S. J., Park, K. R., Kim, J. (2007). Biometric Key Binding: Fuzzy Vault Based on Iris Images. *Lecture Notes in Computer Science*, 800–808. doi: https://doi.org/10.1007/978-3-540-74549-5_84
- [9] Nandakumar, K., Jain, A. K. (2008). Multibiometric Template Security Using Fuzzy Vault. 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems. doi: <https://doi.org/10.1109/btas.2008.4699352>
- [10] Geng, S., Giannopoulou, G., Kabir-Querrec, M. (2019). Privacy Protection in Distributed Fingerprint-based Authentication. *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society – WPES'19*. doi: <https://doi.org/10.1145/3338498.3358648>
- [11] Koptyra, K., Ogiela, M. R. (2018). Multiply information coding and hiding using fuzzy vault. *Soft Computing*, 23 (12), 4357–4366. doi: <https://doi.org/10.1007/s00500-018-3089-x>
- [12] Panwar, A., Singla, P., Kaur, M. (2017). Techniques for Enhancing the Security of Fuzzy Vault: A Review. *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications*, 205–213. doi: https://doi.org/10.1007/978-981-10-3376-6_23
- [13] Rasool, R. A. (2018). Iris Feature Extraction and Recognition based on Gray Level Co-occurrence Matrix (GLCM) Technique. *International Journal of Computer Applications*, 181 (25), 15–17. doi: <https://doi.org/10.5120/ijca2018917826>
- [14] Hajari, K., Gawande, U., Golhar, Y. (2016). Neural Network Approach to Iris Recognition in Noisy Environment. *Procedia Computer Science*, 78, 675–682. doi: <https://doi.org/10.1016/j.procs.2016.02.116>
- [15] Rathgeb, C., Tams, B., Wagner, J., Busch, C. (2016). Unlinkable improved multi-biometric iris fuzzy vault. *EURASIP Journal on Information Security*, 2016 (1). doi: <https://doi.org/10.1186/s13635-016-0049-9>
- [16] Weerasinghe, T. D. B. (2012). Secrecy and Performance Analysis of Symmetric Key Encryption Algorithms. *International Journal of Information and Network Security (IJINS)*, 1 (2). doi: <https://doi.org/10.11591/ijins.v1i2.438>

- [17] Singha, S., Sen, M. (2016). Encoding algorithm using bit level encryption and decryption technique. 2016 International Conference on Computer, Electrical & Communication Engineering (ICCECE). doi: <https://doi.org/10.1109/iccece.2016.8009584>
- [18] Chitra, D., Sujitha, V. (2019). Security analysis of prealigned fingerprint template using fuzzy vault scheme. Cluster Computing, 22 (S5), 12817–12825. doi: <https://doi.org/10.1007/s10586-018-1762-6>
- [19] Woodard, D. L., Ricanek, K. (2009). Iris Databases. Encyclopedia of Biometrics, 770–774. doi: https://doi.org/10.1007/978-0-387-73003-5_168
- [20] Kumar, A., Passi, A. (2010). Comparison and combination of iris matchers for reliable personal authentication. Pattern Recognition, 43 (3), 1016–1026. doi: <https://doi.org/10.1016/j.patcog.2009.08.016>
- [21] Uludag, U., Pankanti, S., Jain, A. K. (2005). Fuzzy Vault for Fingerprints. Audio- and Video-Based Biometric Person Authentication, 310–319. doi: https://doi.org/10.1007/11527923_32
- [22] Weik, M. H. (2000). Brute-Force Attack. Computer Science and Communications Dictionary, 149–149. doi: https://doi.org/10.1007/1-4020-0613-6_1898
- [23] Nandakumar, K., Jain, A. K., Pankanti, S. (2007). Fingerprint-Based Fuzzy Vault: Implementation and Performance. IEEE Transactions on Information Forensics and Security, 2 (4), 744–757. doi: <https://doi.org/10.1109/tifs.2007.908165>
- [24] Nagar, A., Nandakumar, K., Jain, A. K. (2010). A hybrid biometric cryptosystem for securing fingerprint minutiae templates. Pattern Recognition Letters, 31 (8), 733–741. doi: <https://doi.org/10.1016/j.patrec.2009.07.003>
- [25] Li, P., Yang, X., Cao, K., Tao, X., Wang, R., Tian, J. (2010). An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. Journal of Network and Computer Applications, 33 (3), 207–220. doi: <https://doi.org/10.1016/j.jnca.2009.12.003>
- [26] Lee, Y. J., Park, K. R., Lee, S. J., Bae, K., Kim, J. (2008). A New Method for Generating an Invariant Iris Private Key Based on the Fuzzy Vault System. IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 38 (5), 1302–1313. doi: <https://doi.org/10.1109/tsmcb.2008.927261>
- [27] Ahmed, H. M., Taha, M. A. (2021). A Brief Survey on Modern Iris Feature Extraction Methods. Engineering and Technology Journal, 39 (1A), 123–129. doi: <https://doi.org/10.30684/etj.v39i1a.1680>
- [28] Taha, M., Ahmed, H. (2021). Second-Order Statistical Methods GLCM for Authentication Systems. Iraqi Journal for Electrical and Electronic Engineering, 17 (1), 1–6. doi: <https://doi.org/10.37917/ijeee.17.1.10>

Received date 09.03.2021

Accepted date 30.07.2021

Published date 13.09.2021

© The Author(s) 2021

This is an open access article
under the Creative Commons CC BY license

How to cite: Taha, M. A., Ahmed, H. M. (2021). A fuzzy vault development based on iris images. EUREKA: Physics and Engineering, 5, 3–12. doi: <https://doi.org/10.21303/2461-4262.2021.001997>