# Usability of the Fuzzy Vault Scheme Applied to Predetermined Palm-based Gestures as a Secure Behavioral Lock

Marcin Piekarczyk
Institute of Computer Science and Computer Methods
Pedagogical University of Cracow
2 Podchorazych Ave
30-084 Krakow, Poland
e-mail: marp@up.krakow.pl

Marek R. Ogiela
AGH University of Science and Technology
Cryptography and Cognitive Informatics Research Group
30 Mickiewicza Ave
30-059 Krakow, Poland
e-mail: mogiela@agh.edu.pl

***Abstract* — Nowadays, the crypto-biometric schemes are commonly studied to deal with the key management problem existing in cryptographic systems. In the paper we consider a well-known fuzzy vault scheme working on non-standard biometric data associated with palm-oriented gestures. We discuss the usefulness of the touch-less palm tracking system focused on handling the biomechanical characteristics of one's hand to protect the cryptographic key or other secret data. As a behavioral template the fixed finger-based gesture is applied. In order to generate unordered sets for fuzzy vault we use the global approach where features are decoded from fingertip position and velocity. Both the raw and DCT-calculated time series are preprocessed to solve the instability and variability problem strictly related to behavioral character of the data. We provide the experimental results and discuss the security issues.**

***Keywords — fuzzy vault; palm-based gestures; behavioral lock; gesture-based identification; gestures analysis***

## I. INTRODUCTION

From security point of view the varied biometric modalities constitute useful personal data sources suitable for authentication and verification purposes. Biometric systems exploit varied physical or behavioral modalities [10, 24, 28] as fingerprint, iris, face, voice, gait or handwritten signatures [20-22] to authenticate users. Biometric data is justly considered as hard to steal or direct copy and can't be forgotten or lost as ordinary passwords or access cards. In this aspect the behavioral biometrics with some extent of instability and variation are harder to be effectively applied than physical ones. However, in the last decades a lot of research has been extensively developed for both categories to investigate the potential of crypto-biometry.

Until now, the cryptographic construction named fuzzy vault and proposed by Juels and Sudan in [9] has been effectively applied to different biometric modalities like fingerprints [16, 19, 25], face [27], handwritten signatures [1-5, 11] and iris [14, 15, 26] or others [12]. Today, growing popularity of touch and gesture controlled devices gives the chance to consider untypical behavioral biometrics oriented into gestures [6-8, 23].

This work is focused on investigation the usability of predetermined palm-based gestures for fuzzy vault scheme. We discuss the capability of using the highly unstable patterns as effective behavioral key for the cryptographic construction.

The paper is structured as follows. In Section II the basic assumptions on fuzzy vault constructions proposed by Juels and Sudan [9] are briefly discussed. Section III covers the description of our implementation of the fuzzy vault for palm-based gestures. Section IV presents experimental results and in Section V we conclude the paper with some discussions on future works.

## II. FUZZY VAULT ASSUMPTIONS

In the paper we consider a classical fuzzy vault scheme where secret data are secured with a fuzzy key in the form of an unordered set of points. This cryptographic construction is very appropriate in case of biometrics where vault key in the form of biometric sample is unstable and reveal some extent of variability. We generally follow by approach proposed in [4, 25] to applied fuzzy vault for biometric data including some new solutions and adaptations forced by specific type of data. We assume exploitation of CRC codes to deal with problem of error correction. CRC code is merged with secret S in the encoding phase. This allows check in the easy way if the secret is valid or not during the decoding phase when the secret is reconstructing. Thanks to this we are able to evaluate the secret as genuine or not with error probability of $2^{-16}$ or $2^{-32}$ if CRC-16 or CRC-32 is used respectively. All calculations are done in Galois field $GF(2^{16})$ according to fuzzy vault requirements.

### A. Encoding scheme

The brief overview of the encoding algorithm is presented in Fig. 1. As the input data we have $P - bits$ value destined to be secure and feature vector $T$ derived from biometric data which plays the role of fuzzy vault key. It is important to note that due to high instability of performed gesture – what is immanent feature of this type of biometric data – we assume exploiting at least two gesture realizations in a row to extract proper template vector $T$ values.

In order to hide data with 128 bits in size (standard key length in private key cryptography schemes like AES) the secret size must be set to at least $128 + 16 = 144$ bits (CRC-16) or $128 + 32 = 160$ bits (CRC-32). Since template vector $T$ should be consisted of 16 bits units with respect to $GF(2^{16})$ we need to obtain $N = 9$ or $N = 10$ integer numbers to fulfill these requirements.

The actual encoding process works in the following way. We start with $P - bits$ value and merge it with CRC code by

concatenation to obtain $S - bits$ secret. Then we construct the polynomial of degree $D = P/16$ (1) with coefficients made up from consecutive 16 bits fragments of $S$ secret data. Utilization of CRC-32 code enables us to construct polynomial of higher degree $(D + 1)$.

$$p(x) = S_1 x^n + \ \dots \ + S_D x^1 + S_{D+1} \quad (1)$$

In the next step we calculate the polynomial projections for all the components in template vector $T$ to form secure key points (2).

$$G = \{(t_1, p(t_1)), \dots, (t_N, p(t_N))\} \quad (2)$$

Additionally, we generate a set of $M$chaff points (3), which should be chosen randomly.

$$C = \{(c_1, f_1), \dots, (c_M, f_M)\} \quad (3)$$

Finally, $G$ and $C$ sets are mixed to obtain vault set $V$ (4).

$$V = \{(v_1, w_1), \dots, (v_{N+M}, w_{N+M})\} \quad (4)$$

The security of this solution relies on the assumption that impossibility to distinguish the key and chaff points makes computationally hard the reconstruction of the secret polynomial. It is feasible only when we know enough number of the key points ($D + 1$ at least). The number of chaff points must guarantee to appropriate security level. In some reports like [4, 25] few hundreds of chaff points (200) is considered to be sufficient.

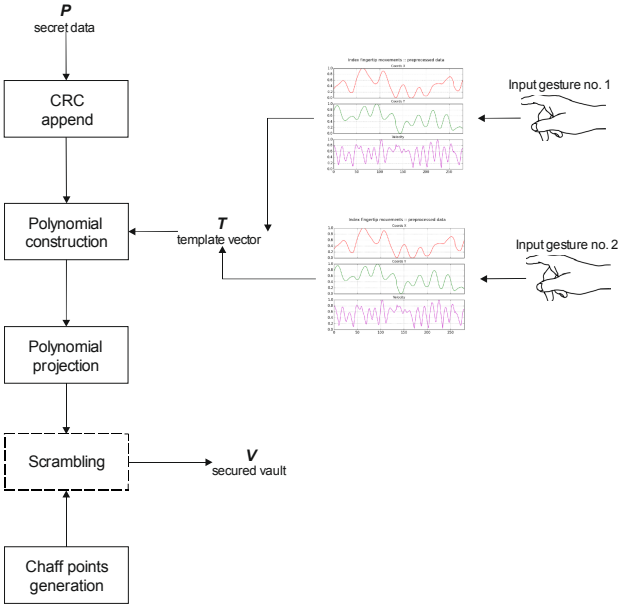


Figure 1. Fuzzy vault encoding scheme for predetermined palm-based gesture.

## B. *Decoding scheme*

We decode a secured fuzzy vault $V$ by using candidate points $CP$ extracted from gestures performed by the examined user (Fig. 2). As it was mentioned earlier we need two or more gesture realizations to calculate the proper candidate points. Moreover, $CP$ vector should count at least $D + 1$ components to be able to unlock vault at all. Subsequently, we choose from among candidate points all combinations of $D + 1$ query points (size of template vector $T$) to obtain a set of query vectors $Q$. On the basis of single query vector $Q_i$ we can select proper pairs $(v_j, w_j)$ from fuzzy vault $V$ and interpolate the secret polynomial using the *Langrange* scheme [24, 25]. After calculation of CRC code we evaluate if the polynomial and secret are valid or not. This procedure requires at the most $|Q|$ interpolations where $|Q|$ denotes the cardinality of set $Q$.

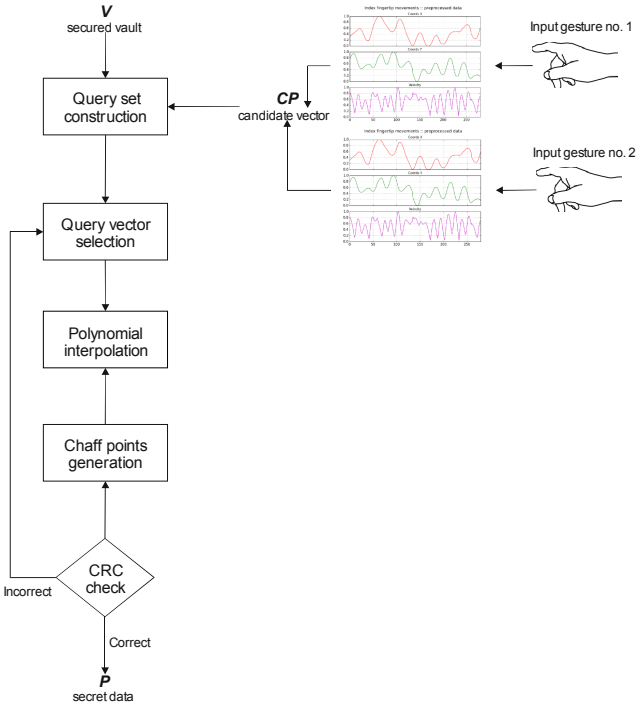


Figure 2. Fuzzy vault decoding scheme for predetermined palm-based gesture.

# III. FUZZY VAULT OVER PALM GESTURES

In the paper we research the usability of biometric data acquired from predetermined palm-based gesture for cryptographic purposes. We are especially focused on finger-based gesture types discussed in [23] to investigate their usefulness in to context of fuzzy vault scheme. The main difficulty is related to small amount of information they supply and high instability and variability patterns they provide. In order to transform gesture motion to digital signal we follow by scheme proposed in [23]. According to this approach after data acquisition and preprocessing steps we obtain the input data $I$ in the form of three discrete time series (5) associated with spatial coordinates and magnitude of the velocity (Fig. 3).

$$I = [x(t), y(t), v(t)] \quad (5)$$

We examined direct input data and also its transformation into frequency domain (Fig. 4) calculated with Discrete Cosine Transform (6) [17, 18] as source for template points. When data series are transformed by DCT-II we take into

consideration only reduced number of coefficients where most of signal energy is concentrated [23].

$$y[k] = 2 \cdot \sum_{n=0}^{N-1} x[n] \cos\left[\frac{\pi}{N}\left(\frac{2n+1}{2}\right)k\right] \quad (6)$$

$$k = 0, \ldots, N-1$$

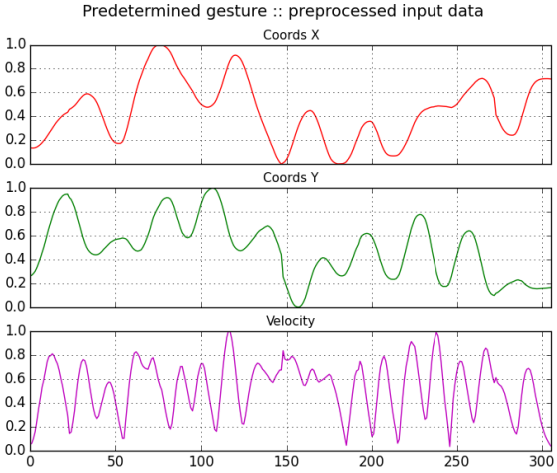


Figure 3. Example of preprocessed input data for predetermined palm-based gesture.

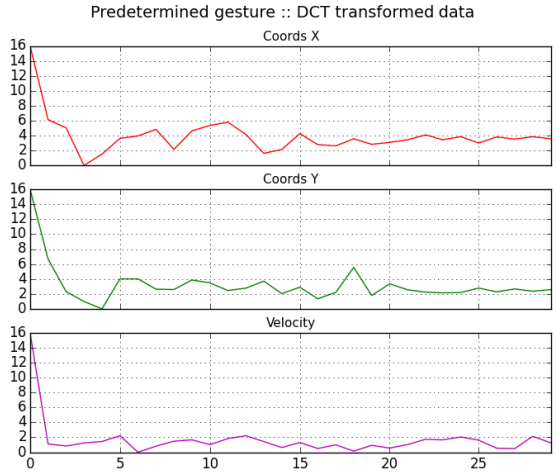


Figure 4. Example input data transformed with DCT-II – 30 first components.

In order to determine the template features we utilize the main concept described in [4] where local signal parameters like minima and maxima are calculated as candidate points. Then, every indicated point is quantized into 8-bit value by using 4-bit time and amplitude quantization like shown in Fig. 4.

At this point it is worth to pay attention on resolution obtained during the quantization. Unfortunately, the gesture type of data is very unstable and variable by nature. The increasing level of quantization does not solve this difficulty and often downgrade the effectiveness. Experiments with our data show that more detailed quantization results in generating less number of repeatable points.

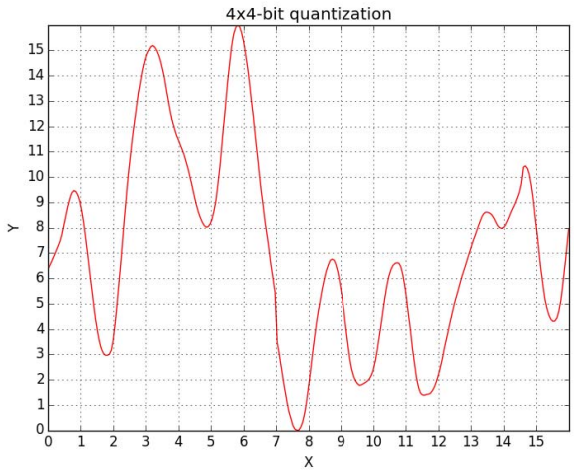


Figure 5. Example of 4x4-bit quantization for x(t) data series.

On the other hand, the 16-bit values are necessary for the fuzzy vault calculations. Due to this we propose the solution where 8-bit values obtained from gesture data are transformed into 16-bit values. It can be done through direct conversion the 8-bit input number into 16-bit value and then executing bitwise rotation (circular shit) of $L$ bit positions to the left, $L \in [1,8]$ (7-8). Thanks to this we receive the transformation from $[0,255]$ range to the same size range but with different (higher) values within 16-bit domain. In our experiments we use $L = 8$ to shift. This operation has no influence on dispersion of the values.

$$10011011 \xrightarrow{convert\ to\ 16bit} 00000000\ 10011011 \quad (7)$$

$$00000000\ 10011011 \xrightarrow{circular\ shift} 10011011\ 00000000 \quad (8)$$

The separate issue regards chaff points generation. The fuzzy vault scheme is secure only when we are able to hide template points between artificially generated false points. Usually, it is assumed that these points are generated in random way. In the case considered here diffusion of points are significantly limited to fixed range. Due to this the random generation of chaff points is not a solution [4, 9, 25] because it doesn't allow hide template points effectively. Instead of random producing of chaff points we propose to generate these points within the same 8-bit range as template points. This approach let us to supplement the 8-bit range by false points and will results in uniformly filled with values. The potential attacker won't be computationally feasible to distinguish between valid and false points as before. This construction seems to similarly secure as randomly produced chaff points but doesn't require the high quality random generator. The number of chaff points received this way is over 240 what gives sufficient level of security.

## IV. Experimental Results

To evaluate the initial accuracy the reduced gesture database was used. The database consists of gestures performed by four people. Every user performed the gesture

ten times. Two randomly chosen samples belonged to person have been chosen as representative pair designed as source for producing the template points. The other samples were exploited as tested data to unlock the vault. As a motion sensor during the data acquisition phase the Leap Motion controller [12] has been exploited. The results received during the tests are presented in Tab. I. We considered polynomial degree $D = 8$.

TABLE I. INITIAL SYSTEM PERFORMANCE

| | ***DCT-10 + raw data*** | ***DCT-5 + raw data*** | ***DCT-30*** |
|---|---|---|---|
| FRR | 64.3 | 62.5 | 41.0 |
| FAR | 25.1 | 2.0 | 2.0 |

Direct data series was checked as too unstable to be used singly. There is necessary to make some transformations to ensure that number of template points appears acceptable. We tested DCT transformed data in combination with raw series. It is important to note that it results in high level of false rejections. The further research must be focused on searching better data transformation to cope with pattern variability.

## V. CONCLUSIONS

In this article we discussed the usability of simple predetermined palm-based gestures as behavioral key for fuzzy vault system. We have proposed some new solutions to deal with problems arising from low quality data (unstable and imprecisely repeatable). Preliminary experiments provide the unsatisfactory results. Therefore work is currently being done in deep testing against the considerably larger database to evaluate usefulness of the scheme more precisely.

In the future we plan to study the applicability of such scheme to the more complicated gesture-types like signature-based or multi-fingers gestures. We also consider as important to investigate a usefulness of Locality Sensitive Hashing (LSH) to this purposes.

## ACKNOWLEDGMENT

We kindly acknowledge the support of this study by a Pedagogical University of Cracow Statutory Research Grant.

## REFERENCES

[1] G. S. Eskander, R. Sabourin and E. Granger, "Signature based Fuzzy Vaults with boosted feature selection," Computational Intelligence in Biometrics and Identity Management (CIBIM), 2011 IEEE Workshop on, IEEE, 2011, pp. 131-138.

[2] G. S. Eskander, R. Sabourin and E. Granger, "A Dissimilarity-Based Approach for Biometric Fuzzy Vaults–Application to Handwritten Signature Images," New Trends in Image Analysis and Processing–ICIAP 2013, Springer Berlin Heidelberg, 2013, pp. 95-102.

[3] G. S. Eskander, R. Sabourin and E. Granger, "Improving Signature-Based Biometric Cryptosystems Using Cascaded Signature Verification-Fuzzy Vault (SV-FV) Approach," Frontiers in Handwriting Recognition (ICFHR), 14th International Conference on, IEEE, 2014, pp. 187-192.

[4] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-García, "Cryptographic key generation using handwritten signature" Defense and Security Symposium, International Society for Optics and Photonics, 2006, pp. 62020N-62020N.

[5] M. Freire, et al. "On the applicability of off-line signatures to the fuzzy vault construction," Proc. of the 9th ICDAR, IEEE, 2007, pp. 1173-1179, doi: 10.1109/ICDAR.2007.4377100.

[6] T. Hachaj, M. R. Ogiela, M. Piekarczyk, "Dependence of Kinect sensors number and position on gestures recognition with Gesture Description Language semantic classifier," Proc. of the Federated Conference on Computer Science and Information Systems, Series: Annals of Computer Science and Information Systems, Vol. 1, 2013, pp. 571-575.

[7] T. Hachaj, M. R. Ogiela, M. Piekarczyk, "Real-time recognition of selected karate techniques using GDL approach," Image Processing and Communications: challenges 5 (ed. R. Choras), Series: Advances in Intelligent Systems and Computing, Vol. 233, Heidelberg, Springer, 2013, pp. 99-106.

[8] T. Hachaj, M. R. Ogiela, "Full-body gestures and movements recognition: user descriptive and unsupervised learning approaches in GDL classifier," Applications of Digital Image Processing XXXVII, edited by Andrew G. Tescher, Proc. of SPIE Vol. 9217, 921704, doi: 10.1117/12.2061171, 2014.

[9] A. Juels and M. Sudan, "*A fuzzy vault scheme*," in Proc. IEEE Int. Symp. Information Theory, 2002, p. 408.

[10] A. Jain, R. Bolle, S. Pankanti, eds., "Biometrics: personal identification in networked society," Vol. 479, Springer Science & Business Media, 2006.

[11] A. Kholmatov and B. Yanikoglu, "Biometric cryptosystem using online signatures," Computer and Information Sciences–ISCIS 2006, Springer Berlin Heidelberg, 2006, pp. 981-990.

[12] A. Kumar, A. Kumar and S. Schuckers. "Development of a new cryptographic construct using palmprint-based fuzzy vault," EURASIP Journal on Advances in Signal Processing, Hindawi Publishing Corporation, 2009 (13), doi:10.1155/2009/967046.

[13] Leap Motion, https://www.leapmotion.com/

[14] Y. I. Lee, et al. "Biometric key binding: Fuzzy vault based on iris images," Advances in Biometrics, Springer Berlin Heidelberg, 2007, pp. 800-808.

[15] Y. I. Lee, et al. "A new method for generating an invariant iris private key based on the fuzzy vault system," Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, Vol. 38, Issue 5, 2008, pp. 1302-1313.

[16] P. Li, et al. "An alignment-free fingerprint cryptosystem based on fuzzy vault scheme," Journal of Network and Computer Applications, Vol. 33, Issue 3, 2010, pp. 207-220.

[17] J. Makhoul, "A Fast Cosine Transform in One and Two Dimensions," IEEE Transactions on acoustics, speech and signal processing, Vol. 28(1), 1980, pp. 27-34.

[18] M. Muller, "Information Retrieval for Music and Motion," Springer-Verlag, 2007, doi: 10.1007/978-3-540-74048-3.

[19] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance", Information Forensics and Security, IEEE Transactions on, Vol. 2, Issue 4, 2007, pp. 744-757.

[20] M. R. Ogiela, M. Piekarczyk, "Random graph languages for distorted and ambiguous patterns: single layer model," Proceedings of the Sixth International Conference on Innovative Mobile and Internet Services in ubiquitous computing (IMIS2012), pp. 108-113, 4-6 July 2012, Palermo, Italy, doi: 10.1109/IMIS.2012.147.

[21] M. Piekarczyk, M. R. Ogiela, "Hierarchical Graph-Grammar Model for Secure and Efficient Handwritten Signatures Classification," Journal of Universal Computer Science, Vol. 17, Iss. 6, 2011, pp. 926 – 943, doi: 10.3217/jucs-017-06-0926.

[22] M. Piekarczyk, M. R. Ogiela, "Matrix-based hierarchical graph matching in off-line handwritten signatures recognition," Proceedings of 2nd IAPR Asian Conference on Pattern Recognition, IEEE, 2013, pp. 897-901, doi: 10.1109/ACPR.2013.164.

[23] M. Piekarczyk, M. R. Ogiela, "On Using Palm and Finger Movements as a Gesture Biometrics," Proceedings of 7th International Conference on Intelligent Networking and Collaborative Systems, IEEE, 2015, pp. 211-216, doi: 10.1109/INCoS.2015.83.

[24] U. Uludag, S. Pankanti, P. S., and A. Jain, "*Biometric cryptosystems: Issues and challenges*," Proceedings of the IEEE 92, pp. 948–960, June 2004.

[25] U. Uludag, S. Pankanti, and A. K. Jain, "*Fuzzy vault for fingerprints*," in Proc. AVBPA, Lecture Notes in Computer Science 3546, pp. 310–319, Springer, 2005.

[26] X. Wu, et al., "An iris cryptosystem for information security," Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP'08 International Conference on, IEEE, 2008, pp. 1533-1536.

[27] L. Wu and S. Yuan, "A face based fuzzy vault scheme for secure online authentication," Data, Privacy and E-Commerce (ISDPE), 2010 Second International Symposium on, IEEE, 2010, pp. 45-49.

[28] R. V. Yampolskiy, V. Govindaraju, "Behavioural biometrics: a survey and classification", International Journal of Biometrics Vol. 1(1), 2008, pp. 81-113.