# FUZZY SECURE SKETCH BIOMETRIC SCHEME BASED ON NON-BINARY TURBO CODES

Assanovich B. A., Veretilo Yu. N.
Information Systems and Technologies Department of Yanka Kupala State University of Grodno
National Anti-Doping Laboratory
Grodno, Minsk, Republic of Belarus
E-mail: bas@grsu.by, hullit.pakkard@gmail.com

*The implementation of a fuzzy secure sketch biometric scheme for so-called fuzzy commitment using non-binary turbo codes with several times better performance and flexibility has been proposed.*

## Introduction

Recently, the implementation of reliable cryptographic systems based on fuzzy extractors (Fuzzy Extractor) using unreliable «noisy» biometric data is of particular interest in the literature. It is known that if in such systems the arising noise caused by the fuzziness of the biometric data is additive and leads to substitution errors, an effective solution is the use of noise-immune codes with large Hamming distance. One of the known approaches to creating such a system is to use a code-offset construction [1], which forms an auxiliary sketch (Secure Sketch) stored in the database. It is applied together with the error correcting code $(n, k, d)$ and represents the offset $D$ that «shifts» the code vector $X$ of the applied noise-proof code containing the user's password $S$ by the biometric measurement value $B$, i.e.$D = B - X$. In the subsequent biometric measurement $B'$, subtraction $D - B' = Y$, decoding $Y$ and obtaining the password $S'$, generally coinciding with $S$, is performed.

To achieve the necessary efficiency (to minimize the probability of FAR and FRR), it is necessary to apply the «powerful» error-correction codes, for example BCH, increasing the Hamming distance to correct multiple errors [2], and also to non-binary noise-resistant codes (Reed-Solomon, Turbo codes) [3], where their effectiveness can be estimated by the Euclidian distance. In this paper, we propose the implementation of a fuzzy extractor based on the scheme of the so-called fuzzy commitment [2] using non-binary turbo codes. The proposed scheme has better biometric performance and implementation flexibility compared to [2,3] and has the ability to choose the type of non-binary code, arbitrary its block length and the distortion level due to data quantization to achieve the necessary confidentiality and data security.

## I. System Model

The proposed scheme includes two basic procedures: Enrollment and Authentication (see Fig.1). At the registration side, the $m$-ary Secret Password $S_m$ enters the Non-Binary Encoder, where the encoding function $NBE(S_m) \rightarrow X_m$ add the redundant symbols for error correction, forming framed data blocks $X_m$ that pass through the $m$-ary modulator and are subtracted from a block of biometric quantized data $B_q$ formed at the output of a Quantizer $D_m = B_q - X_m$. The quantizing interval used takes into account the power of the noise-resistant error-correcting code used and the specified level of the user data security. The obtained data block $D_m$ is written to the Data Base and stored together with the hash $h(S_m)$ in it. At the authentication side, the subtraction $B'_q - D_m = Y_m$ for a new data block $B'_q$ is performed, resulting in a vector $Y_m$, that becomes an input to the Non-Binary Decoder. The decoding function $NBD(Y_m) \rightarrow S'_m$ is applied giving the user password $S'_m$ as the output. Next, hash function $h(S'_m)$ was compared with hash function $h(S_m)$ where compared. If they are equal, the user is successfully authenticated.

## II. Results and conclusions

In this paper we consider the use of non-binary turbo codes constructed from non-binary convolutional component codes concatenated via a random symbol interleaver mapped onto phase-shift keying $(8 - PSK)$ constellation. The polynomials used produced coding matrix $g = [166; 176]$ over the ring $GF(8)$ for systematic 1/3-rate turbo code.

Then random secret key 8-ary $S_m$ of length 166 was turbo encoded with terminating zeroes into resulting matrix $3 \times 172$ of $X_m$ and then modulated into a constellation $8 - PSK$. Each symbol of $X_m$ was presented by $I - Q$ complex numbers giving framed data matrix $3 \times 344$. To get biometrical face features the Caltech Base has been used. Data from 511 real numbers, obtained after a special mask to get the most representative components of 4464-element HOG vectors have been used as biometric raw data [2]. The biometric quantized data $B_q$ was calculated after quantization with interval $q = 0.19635$, normalized and linearly mapped to the interval $[0, 2\pi)$ of angles presented then by two $I-Q$ components. The data block was obtained and put to the Data Base together with the hash $h(S_m)$ in it.

At the authentication stage, the subtraction $B'_q - D_m = Y_m$ for a new quantized data $B'_q$, was performed and a vector $Y_m$, was decoded after 3 iterations by the modified $BCJR$ algorithm giving

the user password $S'_m$ . Next, hash function $h(S'_m)$ to $h(S_m)$ where compared.

Preliminary experimental estimates of FAR and FRR resulted in values $FAR = 0\%$; $FRR \sim 0.1\%$, which is several times better than the known results for turbo codes [3].

The application of the proposed method allows to significantly improve the main performance indicators of biometric systems based on fuzzy extractors and to adjust the system parameters to the required length of the user's secret key and the necessary level of confidentiality.


1. Dodis Y., Reyzin L., Smith A.. Fuzzy extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. EUROCRYPT, 2004. P. 523-540
2. Assanovich B. A., Veretilo Yu. N.. Biometric database based on HOG structures and BCH codes. Information Technologies and Systems 2017 (ITS-2017). Minsk, 2017. -P. 286-287
3. Maiorana E., Blasi D., Campisi P.. Biometric Template Protection Using Turbo Codes and Modulation Constellations. IEEE WIFS, 2012. P.25-30.


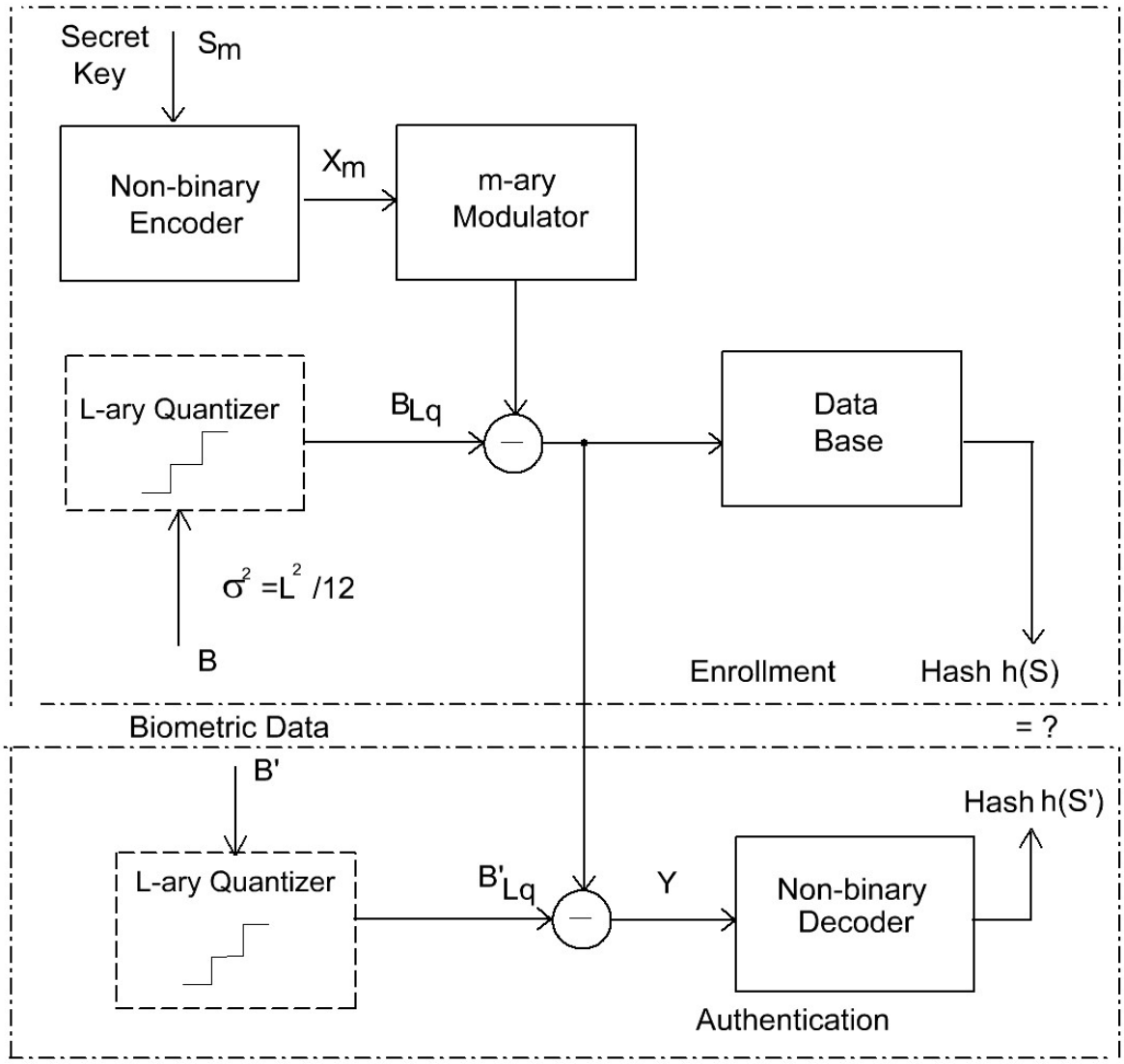


Figure 1 – System Model