Experimental results: For a computer simulation, several image sequences, 176 × 144, 352 × 240 and 256 grey level, were used. The original sequences, hall-monitor and outdoor sequence were captured at 30 frame/s. Fig. 2*a* and *b* show the results of the Bayes decision with the original PDF and with the proposed blurred PDF at a frame rate of 1/30s, respectively. Fig. 2*c* and *d* show the results at a frame rate of 1/15s. In the original sequence, the first 15 frames containing only the background are used for generating the background PDF. In Fig. 2*a* and *c*, there are many falsely detected pixels. The Bayes detector with the proposed PDF has a more robust discrimination capability as shown in Fig. 2*b* and *d*. Fig. 2*c* and *d* shows the under-sampled case with half the frame rate (15 frame/s). In this case, the Bayes detector with the original background PDF shows seriously degraded detection capability due to aliasing. However, the proposed algorithm still obtains good results. Fig. 3 shows the final segmentation results of moving objects for an outdoor sequence. The moving object area is represented by a bounding box and the centroid of the object as '+'. The real trajectory of a tracked object is shown in Fig. 3*f*. False alarms due to intensity fluctuations caused by swaying leaves are completely eliminated by using the projection profiles of moving pixels.

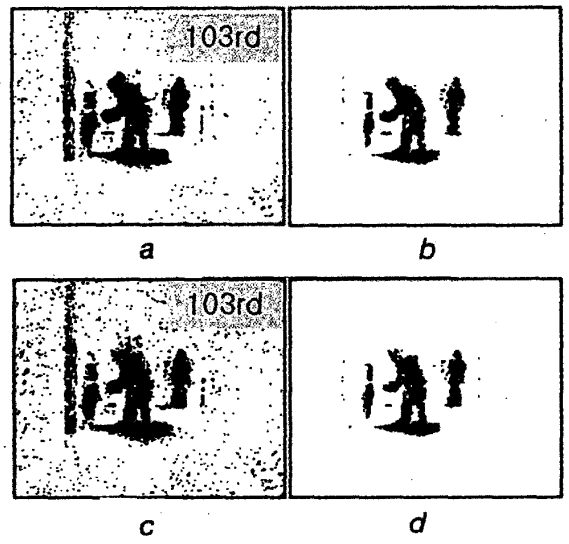

Fig. 2 *Detection of moving pixels*

Hall monitor: 103rd image
a Frame rate 1/30s, detection with original PDF
b Frame rate 1/30s, detection with proposed method
c Frame rate 1/15s, detection with original PDF
d Frame rate 1/15s, detection with proposed method

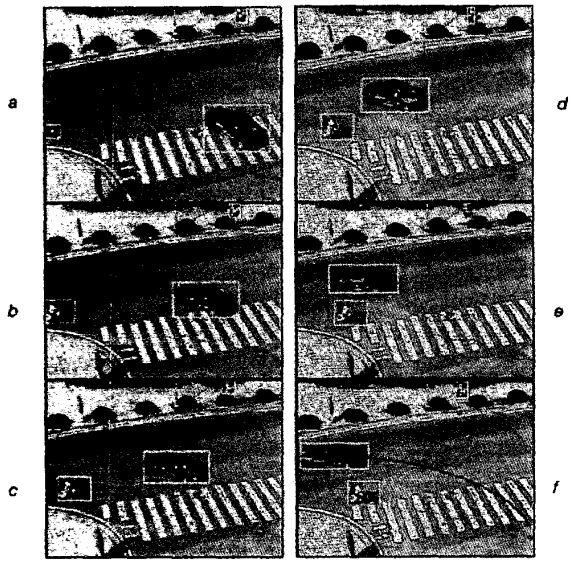

Fig. 3 *Segmentation result*

Outdoor sequence
a 350th frame
b 363th frame
c 376th frame
d 389th frame
e 402th frame
f 415th frame

Conclusions: An efficient algorithm that detects and tracks moving objects in a static camera environment has been proposed. By using the Bayes decision method with a Gaussian blurred PDF, false alarms in detecting moving objects were reduced. The proposed method showed robust segmentation and tracking results against noise, illumination change, and irregular motion. It could be used for unmanned surveillance and traffic monitoring systems.

Acknowledgment: The authors gratefully acknowledge the financial support of the Ministry of Information and Communication, Korea.

19 August 1999
Electronics Letters Online No: 19991211
DOI: 10.1049/el:19991211

Kyu-Won Lee and Jinwoong Kim (*ETRI, 161 Kajong-dong, Yusung-gu, Taejon 305-350, Korea*)

E-mail: kwlee@video.etri.re.kr

References

1 WU, S.F., and KITTLER, J.: 'A gradient-based method for general motion estimation and segmentation', *J. Vis. Commun. Image Rep,.* 1993, **4**, (1), pp. 25–38
2 BICHSEL, M.: 'Segmenting simply connected moving objects in a static scene', *IEE Trans. Pattern Anal. Mach. Intell.*, 1994, **16**, (11), pp. 1138–1142
3 LEE, K.W., RYU, S.W., LEE, S.J., and PARK, K.T.: 'Motion based object tracking with mobile camera', *Electron. Lett.*, 1998, **34**, (3), pp. 256–258
4 NAKAI, H.: 'Non-parameterized Bayes decision method for moving object detection'. Proc. ACCV'95, Singapore, 1995, pp. 447–451

Decoding of binary separable Goppa codes using Berlekamp-Massey algorithm

M. Elia, E. Viterbo and G. Bertinetti

It is shown that the Berlekamp-Massey algorithm can be applied without exceptions to decode the class of binary Goppa codes with location set $\Gamma = \{\gamma_1, ..., \gamma_n\} \subseteq GF(2^m)$ and separable Goppa polynomial $G(z) = z^t + z + \beta$ defined over $GF(2^m)$ such that $G(\gamma_i) \neq 0$ for $1 \leq i \leq n$, up to tile designed minimum distance $2t + 1$.

Introduction: Binary Goppa codes with separable Goppa polynomial of degree t can correct up to t errors. A general algorithm based on the solution of a key equation [1] was described by Patterson [3] and a key step to the solution of the key equation was the solution of a quadratic equation in a polynomial ring given in [4]. A decoding scheme for binary Goppa codes based on the Gorenstein-Peterson-Zierler (GPZ) method [7] and the Berlekamp-Massey (BM) algorithm used to produce the error locator polynomial was proposed in [5], although it requires t to be even. It seems that no decoding scheme that does not have exceptions has yet been proposed. In this Letter we consider a Goppa code with location set $\Gamma = \{\gamma_1, ..., \gamma_n\} \subseteq GF(2^m)$ and Goppa polynomial $G(z) = z^t + z + \beta$ defined over $GF(2^m)$, having simple roots (i.e. the polynomial is separable) and such that $G(\gamma_i) \neq 0$ for $1 \leq i \leq n$. This code has length n, dimension $k \geq n - mt$ and minimum distance $d \geq 2t + 1$, thus it can correct up to t errors [6]. Since the codes are binary, for error correction it is only necessary to compute the error locator polynomial $\sigma(z) = z^t + \sigma_1 z^{t-1} + ... + \sigma_{t-1} z + \sigma_t$. According to GPZ the set of elementary symmetric functions σ_1, ..., σ_t is obtained by solving the linear system of equations

$$\sum_{i=0}^{t-1} T_{i+j}\sigma_{t-i} = T_{t+j} \qquad j = 0, ..., t-1 \qquad (1)$$

which is formed by determining a sequence of $2t$ syndromes T_1, ..., T_{2t-1}. Once the system is written down it can be solved with classical methods, and in particular the efficient Berlekamp-Massey algorithm can be applied. In the following Section we show how a sequence of $2t$ syndromes can be easily computed from the received word.

Main result: Let $\mathbf{c} = (c_1, ..., c_n)$, $\mathbf{e} = (e_1, ..., e_n)$ and $\mathbf{r} = (r_1, ..., r_n)$ be the transmitted codeword, the error pattern and the received word, respectively, with $\mathbf{r} = \mathbf{c} + \mathbf{e}$. Recalling that the same code with separable Goppa polynomial $G(z)$ is generated by $G(z)^2$ [6], from the received word $\mathbf{r}$ we can compute two sets of t syndromes each, i.e.

$$S_j = \sum_{i=1}^{n} r_i \frac{\gamma_i^j}{G(\gamma_i)} \qquad j = 0, ..., t-1$$

$$T_j = \sum_{i=1}^{n} r_i \frac{\gamma_i^j}{G(\gamma_i)^2} \qquad j = 0, ..., t-1$$

It is immediately seen that $T_{2h} = S_h^2$ and, using this relation, every even indexed syndrome T_{2j} can be computed for $t - 1 < 2j < 2t - 1$. Furthermore, observing that $G(\gamma_i) = \gamma_i^t + \gamma_i + \beta$ and writing

$$\begin{aligned} T_{2t-2h-1} + T_{t-2h} + \beta T_{t-2h-1} &= \sum_{i=1}^{n} r_i \frac{\gamma_i^{2t-2h-1} + \gamma_i^{t-2h} + \beta\gamma_i^{t-2h-1}}{G(\gamma_i)^2} \\ &= \sum_{i=1}^{n} r_i \frac{\gamma_i^{t-2h-1}}{G(\gamma_i)} = S_{t-2h-1} \end{aligned}$$

every odd-indexed syndrome T_{2j+1} can be computed, for $t - 1 < 2j + 1 \leq 2t - 1$, by

$$T_{2t-2h-1} = T_{t-2h} + \beta T_{t-2h-1} + S_{t-2h-1} \qquad h = 0, ..., \left\lfloor \frac{t+1}{2} \right\rfloor$$

Given the sequence of $2t$ syndromes T_0, T_1, ..., T_{2t-2}, T_{2t-1}, application of the BM algorithm to the system of equations (eqn. 1) yields the number of errors $\ell \leq t$, as well as the coefficients σ_1, ..., σ_ℓ for the error locator polynomial $\sigma(z)$.

Example: Consider a $(2^m, 2^m - 4m, 9)$ Goppa code with location set $GF(2^m)$ and $G(z)$ $z^4 + z + \beta$, where the trace of β in $GF(2^m)$ is equal to 1. A decoding algorithm capable of correcting four errors is based on the following linear system of equations:

$$\begin{bmatrix} T_3 & T_2 & T_1 & T_0 \\ T_4 & T_3 & T_2 & T_1 \\ T_5 & T_4 & T_3 & T_2 \\ T_6 & T_5 & T_4 & T_3 \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \sigma_4 \end{bmatrix} = \begin{bmatrix} T_4 \\ T_5 \\ T_6 \\ T_7 \end{bmatrix}$$

where T_0, T_1, T_2, T_3 are computed from the received word together with S_1, S_2, S_3 and the remaining syndromes are obtained as

$$T_4 = S_2^2 \qquad T_5 = T_2 + \beta T_1 + S_1$$

$$T_6 = S_3^2 \qquad T_7 = T_4 + \beta T_3 + S_3$$

The number of corrected errors is equal to the rank of the coefficient matrix.

Conclusions: We have shown that the Gorenstein-Peterson-Zierler method for decoding BCH codes up to the designed minimum distance can be applied without exception to binary Goppa codes having $\Gamma \subseteq GF(2^m)$ as the location set and separable Goppa polynomial $z^t + z + \beta$. Therefore, the Berlekamp-Massey algorithm [8] can be used to efficiently find the error locator polynomial $\sigma(z)$ for correcting up to t errors. Furthermore, when t is small, a direct solution of the GPZ linear system of equations yields closed expressions for the coefficients of $\sigma(z)$ in terms of syndromes. In particular, the case $t = 2$ has been fully discussed in [2], where a complete decoding algorithm was proposed for two error correcting codes with $GF(2^m)$ as the location set and irreducible Goppa polynomial $G(z) = z^2 + z + \beta$. This is interesting when the decoder is hardware implemented and parallel computations are allowed. Finally, the proposed approach can be applied to binary Goppa codes with any separable Goppa polynomial: in these cases the odd indexed T_{2j+1} syndromes for $(t - 1) < 2j + 1 \leq (2t - 1)$ are obtained solving a linear system with a full coefficient matrix instead of the diagonal matrix produced by the trinomial $z^t + z + \beta$.

The complexity of the proposed algorithm with respect to Patterson's algorithm deserves further investigation regarding particular implementations.

6 July 1999
Electronics Letters Online No: 19991190
DOI: 10.1049/el:19991190

M. Elia, E. Viterbo and G. Bertinetti (*Dipartimento di Elettronica, Politecnico di Torino, Corso Duca degli Abruzzi 24, I-10129 Torino, Italy*)

E-mail: elia@polito.it

References

1 BERLEKAMP, E.R.: 'Algebraic coding theory' (McGraw-Hill, New York, 1968)
2 FENG, G.L., and TZENG, K.K.: 'On quasi-perfect property of double-error-correcting Goppa codes and their complete decoding', *Inf. Control*, 1984, **61**, pp. 132–146
3 PATTERSON, N.J.: 'The algebraic decoding of Goppa codes', *IEEE Trans.*, 1975, **IT-21**, (2), pp. 203–207
4 HUBER, K.: 'Note on decoding binary Goppa codes', *Electron. Lett.*, 1996, **32**, (2), pp. 102–103
5 HELGERT, H.J.: 'Decoding of alternant codes', *IEEE Trans.*, 1977, **IT-23**, (4), pp. 513–514
6 MacWILLIAMS, F.J., and SLOANE, N.J.A.: 'The theory of error-correcting codes' (North Holland, New York, 1977)
7 PETERSON, W.W., and WELDON, E.J. Jr.: 'Error-correcting codes' (MIT Press, Cambridge,1981)
8 BLAHUT, R.E.: 'Theory and practice of error control codes' (Addison-Wesley, New York, 1983)

Iterative probabilistic decoding and parity checks with memory

J.Dj. Golić

A method that effectively reduces the weight of parity checks used in iterative probabilistic decoding algorithms is proposed. The method is especially applicable to so-called parity checks with memory and may lead to a significant improvement in fast correlation attacks on stream ciphers based on linear feedback shift registers. A technique for generating low-weight parity checks with memory is also proposed.

Introduction: Fast correlation attacks [1] on binary linear feedback shift registers (LFSRs) in keystream generators for stream cipher applications are important cryptanalytic techniques which are based on iterative probabilistic decoding algorithms for binary symmetric channels. The attacks exploit the correlation between the known keystream sequence and a linear combination of the LFSR sequences. The goal is to reconstruct the combined LFSR sequence from an observed segment of the keystream sequence in the known-plaintext scenario. The problem is equivalent to one of decoding a truncated cyclic linear block code The success of such an attack critically depends on the number of low-weight parity checks used (see [4, 5]).

Each parity check, as a linear equation satisfied by the LFSR sequence, corresponds to a phase shift of a polynomial multiple of the LFSR feedback polynomial $f(x)$ which is called a parity-check polynomial. The weight of a parity check is defined as the number of bits involved. If $f(x)$ has low weight, then the repeated squaring will yield parity-check polynomials of the same weight [4]. If the weight of $f(x)$ is large, then a polynomial residue method [2] for generating low-weight parity-check polynomials of as small a degree as possible can be used. For a random $f(x)$ of degree r, it turns out that the expected minimal degree of a parity-check polynomial of weight w is $O(2^{r/(w-1)})$.