Watermarking and rank metric codes

Pascal Lefèvre, Philippe Carré and
Philippe Gaborit

<pascal.lefevre@univ-poitiers.fr>, <philippe.carre@univ-poitiers.fr>, <gaborit@unilim.fr>

Context

Robust digital image watermarking

1. Robust and invisible watermarking : resistance to various image processings (malicious or not) and imperceptible to users.
2. Robustness improved using the well known error correcting codes approach (3).
3. Introduction of *rank metric* in watermarking with Gabidulin rank metric codes family.

Rank metric codes (RMC)

Error correcting codes :

$m \longrightarrow$ Encoder $\longrightarrow x$

$x' = x + e \longleftarrow$ Channel $\longleftarrow x$

$x' \longrightarrow$ Decoder $\longrightarrow m'$

Gabidulin codes : by E. M. Gabidulin (1) (1985).

$\rightarrow$ Parameters : $[n, k, n-k+1]_r$

$\rightarrow$ Matrix representation of codewords

$\rightarrow$ Rank distance instead of Hamming metric over $GF(2^m)$

$\rightarrow d_{min} = \min_{x \in \mathcal{C}^*} w_R(x) = \min_{x \in \mathcal{C}^*} Rank(x)$

Examples in practice : $e = x' - x$

$$e = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

$w_H(e) = 4, rk(e) = 2$: both codes

$$e = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

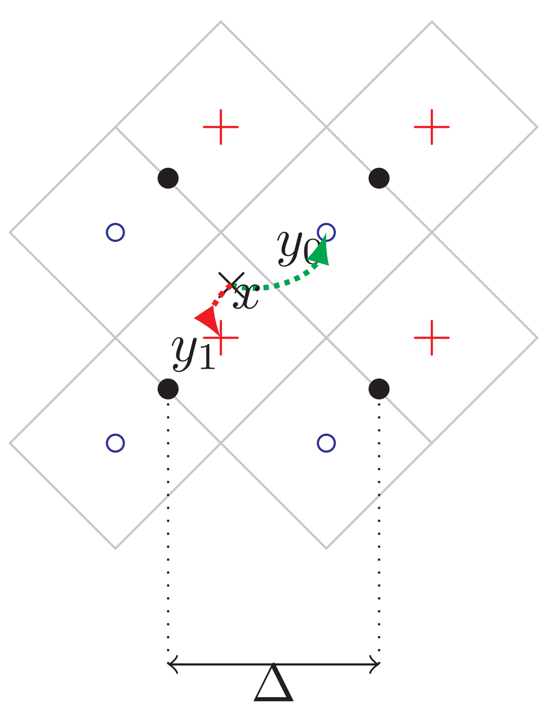
$w_H(e) = 10, rk(e) = 3$: no correction

$$e = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

$w_H(e) = 9, rk(e) = 1$: rank metric only

Lattice QIM (LQIM) (2)

Quantization space in 2D : embedding of bit m in host vector x into y_m.



LQIM + RMC vs luminance

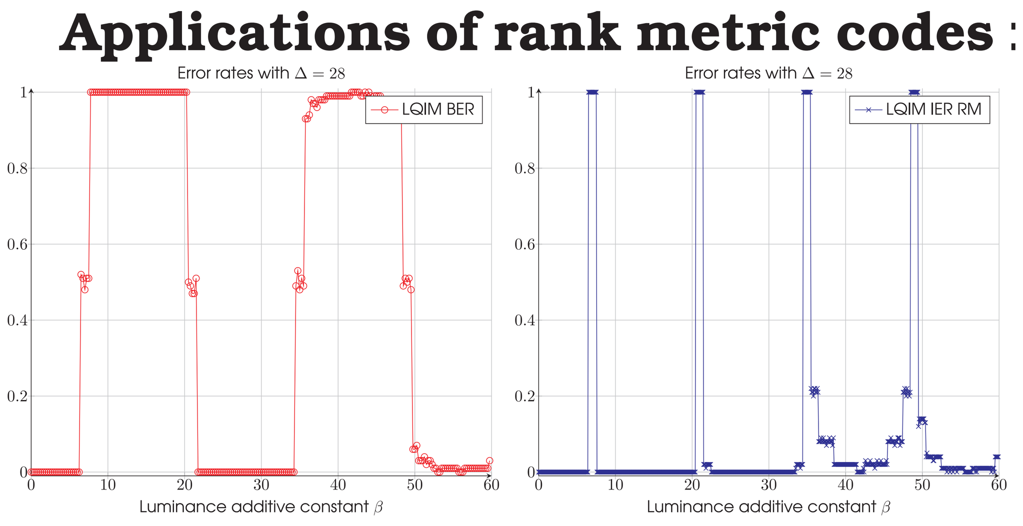
Embedding strategy : LQIM payload is a rank metric codeword.

Luminance attack model :

$$z = y + \beta \times (1, \ldots, 1) \qquad (1)$$

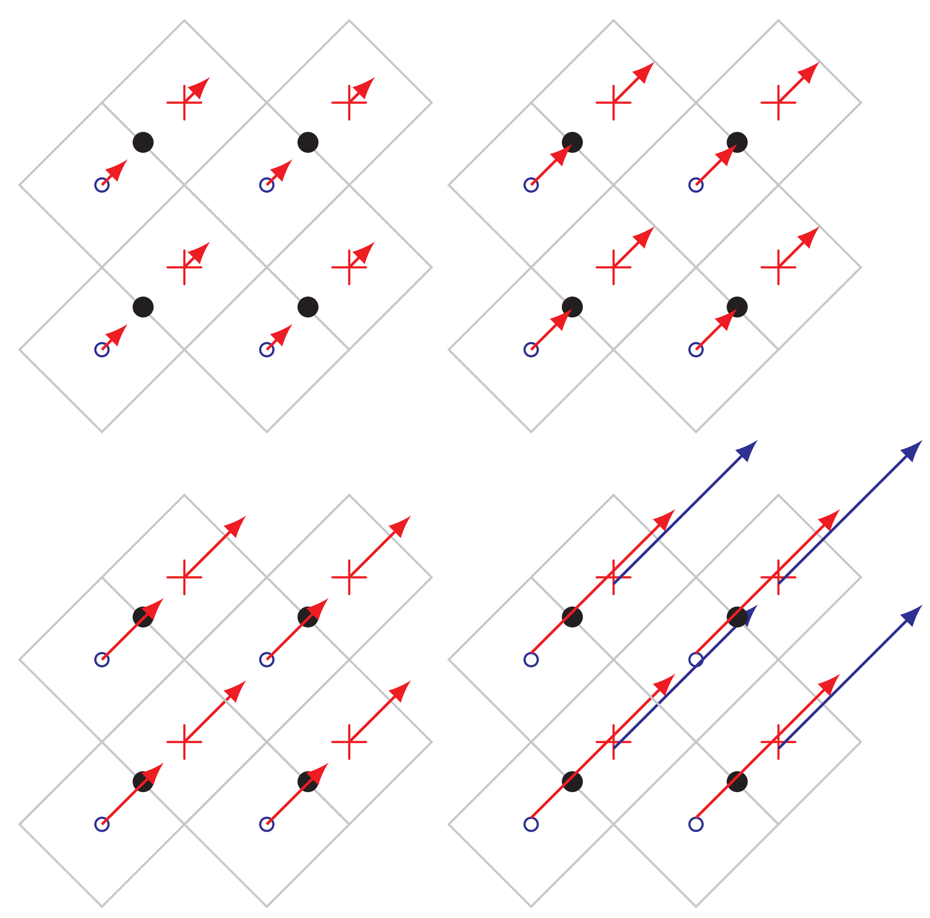
For every z, distortions are constant.

Applications of rank metric codes :



Rank metric codes handle errors when the binary payload is reversed (BER $= 1$ and IER $= 0$) except when errors are random (BER $= 0.5$).

Error structure :



Three distortions states :

$\rightarrow$ BER $= 0$: no error or binary inversion

$\rightarrow$ BER $= 0.5$: random errors

$\rightarrow$ BER $= 1$: binary inversion

References

(1) Gabidulin, Ernest Mukhamedovich - Theory of codes with maximum rank distance *Problemy Peredachi Informatsii 1985*

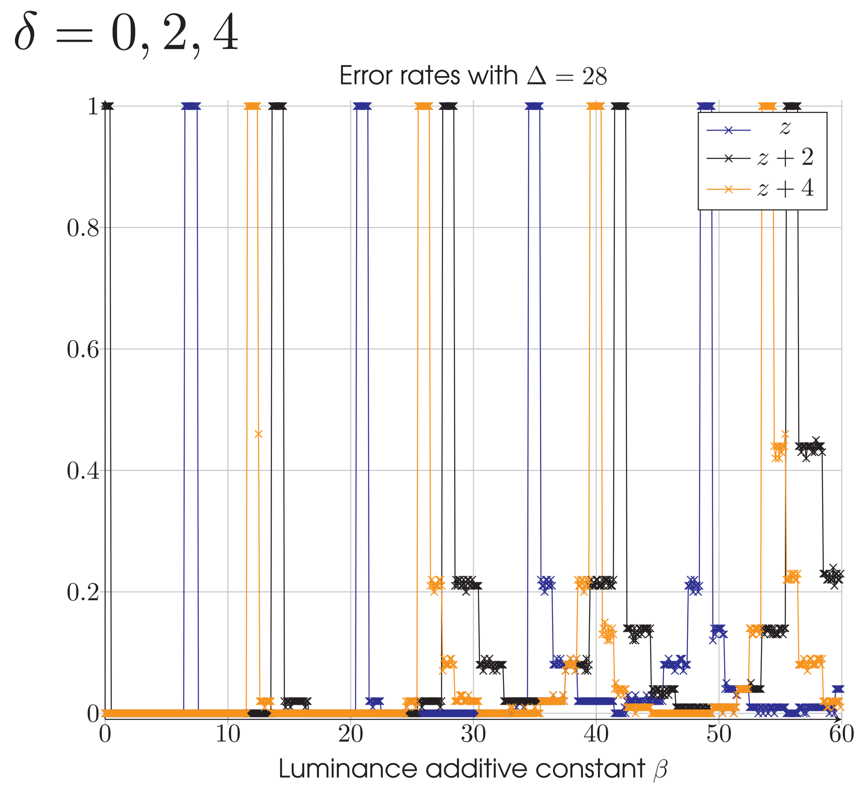
(2) Brian Chen and Gregory W. Wornell - Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding *IEEE TRANS. ON INFORMATION THEORY 1999*

(3) Error correcting codes for robust color wavelet watermarking - Abdul, Wadood and Carré, Philippe and Gaborit, Philippe *EURASIP Journal on Information Security 2013*

Multi-detection and results

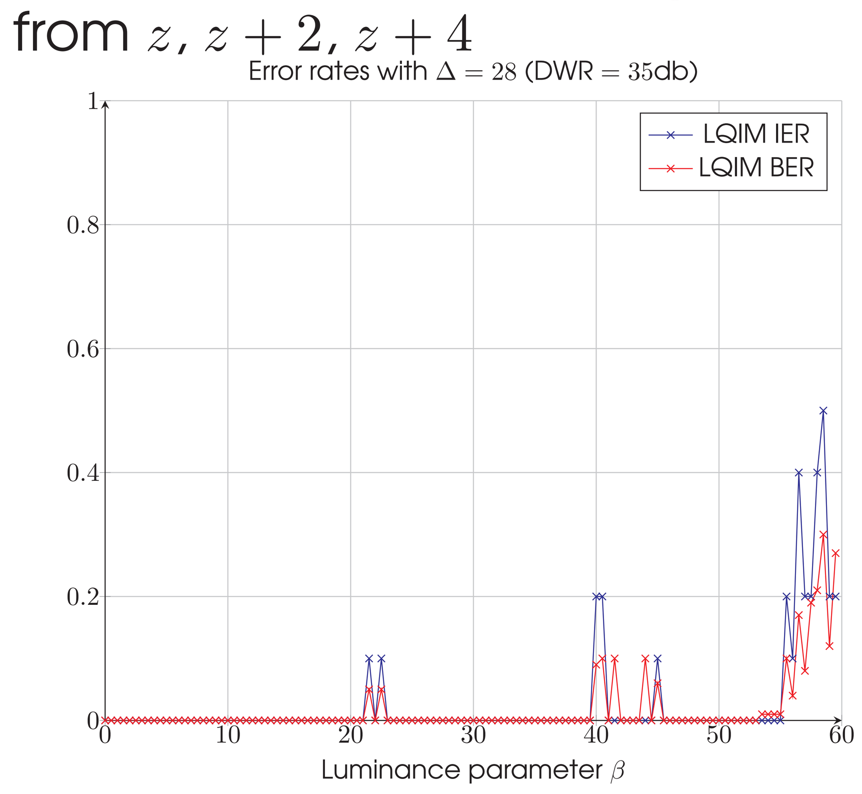
BER/IER curves are perdiodic and equation 1 is *almost* invertible.

Controlled distortions : $z + \delta$ with $\delta = 0, 2, 4$



Error spikes are shifted and don't overlap on each other.

Majority vote strategy : on BERs from z, $z + 2$, $z + 4$



Almost every errors are handled by the multi-detection strategy.

Conclusion

- Rank metric codes introduced in watermarking.
- Hamming codes are inefficient against luminance modifications.
- Rank metric codes are optimal for this error structure.
- Theoretical invariance against luminance modifications.

Perspectives

- Image cropping and collage attack are serious leads.
- Treillis coded quantization ?