WATERMARKING AND RANK METRIC CODES

Pascal Lefèvre, Philippe Carré, Philippe Gaborit

WATERMARKING AND RANK METRIC CODES

Pascal Lefèvre
Xlim UMR CNRS 7252
pascal.lefevre@univ-poitiers.fr

Philippe Carré
Xlim UMR CNRS 7252
philippe.carre@univ-poitiers.fr

Philippe Gaborit
Xlim UMR CNRS 7252
philippe.gaborit@xlim.fr

ABSTRACT

This paper presents a different way to improve the resistance of digital watermarking. Using the well known Lattice QIM in the spatial domain, we analyze the interest of using a different kind of error correcting codes: rank metric codes. These codes are already used in communications for network coding but not used in the context of watermarking. In this article, we show how this metric permits to correct errors with a specific structure and is adapted to specific image attacks. We propose a first study to validate the concept of rank metric for watermarking process. For this, we use these codes to obtain invariance against luminance additive constant change.

Index Terms— watermarking, rank metric codes, gabidulin, luminance, structured errors

1. INTRODUCTION

Image watermarking is an important area of research. An example of motivation is the strong need to protect online multimedia contents. To insure copyright and intellectual property over massive online distribution, we need efficient protection to control the distribution, stop manipulations and duplications by pirates or unaware normal users.

To be efficient, a watermark needs to be imperceptible, needs to embed high capacity payloads and has be to robust [1] against the most common image processings (malicious or not) while ensuring a secure transmission of the payload [2].

A very useful tool to enchance the robustness of a mark is the use of error-correcting codes which permit to correct errors induced by a given attack. Now, depending on the attack and on the structure of the induced errors, the type of codes used can be more or less efficient. For instance, if the error induced on the mark is random, the best results are obtained with binary codes, like BCH codes for instance (in the case of small lengths).

For other attacks, it may happen that the error comes in packet. In that case, it is better to use more structured codes over a larger alphabet (say $GF(2^m)$), like Reed-Solomon codes where decoding is done by packets [3]. One does not decode error independently on each bit, but on packet of m bits, so that an error on each bit of the packet or only one error on one bit of the packet is corrected the same way. Therefore, based on the attack, *i.e.* based on the error type, we can choose an adapted error correcting code. This point of view on the error type is rather well known and led to numerous industrial applications of these Hamming codes.

In this paper, we consider a new type of metric called *rank metric*. Error correcting codes using this metric are already often used in network coding [4] and cryptography [5]. It permits to correct errors with a specific structure. If one considers a code over $GF(2^m)$ of length m. Each coordinate of a codeword over $GF(2^m)$ is encoded by m bits, and since the code has length m, any codeword can be seen as a $m \times m$ matrix. Now, it is possible to correct errors for $m \times m$ error matrix of low rank. For instance, consider an attack on the mark which flips every bits of the mark, if one consider the usual Hamming metric, it is not possible to correct this error since all bits are false. Meanwhile, in terms of rank metric, the associated error matrix has rank 1 (because it is filled with ones only) and hence, the received modified matrix can be decoded and the original message retrieved.

Our contribution: we introduce the rank metric (section 2) and Lattice QIM method (section 3). Then, we propose a watermarking process that uses both concepts able to deal with structured errors produced by a luminance modification that are not handled by conventional Hamming codes. We explain why such structure exists in this case and provide an enhanced Lattice QIM decoder for theoretical error free decoding against this attack.

2. RANK METRIC CODES

2.1. Definitions and properties

We refer to [6] for more details on rank metric codes. Let us consider $B = (\beta_1, ..., \beta_m)$ a basis of $GF(q^m)$ over $GF(q)$. Consider now $x = (x_1, ..., x_n) \in GF(q^m)^n$. The rank of x over $GF(q)$ is the rank of the matrix $X = (x_{ij})$, where $x_{ij} = \sum_{i=1}^{m} x_{ij}\beta_i$. It is denoted by $Rank(x|GF(q))$, or by $Rank(x)$ when there is no ambiguity. Let x and y in $GF(q^m)^n$, one defines the rank distance between x and y as $d_R(x, y) = Rank(x - y)$. As the rank of a vector is independant of the basis, it is obvious that the rank metric is less precise than the Hamming metric as two vectors with different Hamming distance could have the same rank. The linear

Thanks to Délégation générale de l'Armement for funding.

rank code $\mathcal{C}$ of length n and dimension k over $GF(q^m)$ is a subspace of $GF(q^m)^n$. The minimum rank distance of $\mathcal{C}$ is defined as $d = \min(d_R(c_1, c_2), c_1, c_2 \in \mathcal{C} | c_1 \neq c_2)$.

2.2. Decoding rank metric codes

Classical bounds for Hamming distance can be adapted in rank metric context and the same type of decoding results hold. If a rank code $\mathcal{C}$ has minimum distance d and one receives a vector $y = c + e$, for $c \in \mathcal{C}$ and e an error vector of rank less than $(d-1)/2$, it may be possible to uniquely decode y in c. Unlike classical Hamming codes, only few families of codes with easy rank metric decoding are known. Gabidulin codes is one code family among them and has parameters $[n, k, n-k+1]$ over $GF(q^n)$. These codes can decode up to $(n-k)/2$ errors and can be seen as an analogous family in rank metric of the well-known Reed-Solomon codes family. Different approaches to decode Gabidulin codes have been proposed in the literature such as [7, 8].

2.3. Rank metric codes in practice

In practice, we use codes in an extension $GF(q^m)$ of $GF(2)$, and one associates a binary vector of length m to any coordinate of the codeword, so that a codeword c can be seen as a $m \times m$ binary matrix. After an attack on the watermark, codeword c is modified with error e, which also is a $m \times m$ binary matrix. To evaluate if the rank metric is better than the classical Hamming metric, we compare the embedded watermark (a codeword c) with the modified watermark ($y = c+e$). Suppose $m = 4$. Let c be a codeword and $y = c + e$ a modified codeword such that :

$$c = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}, y = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}$$

Then, the error matrix is:

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

The error matrix e has rank 2, hence, if the code can correct up to 2 rank errors, then it is possible to decode y into c. In terms of Hamming metric, if we had started from a length 16 binary code, it would correspond to an error of weight 4. In that particular case, it is possible to find both Hamming or rank metric codes which can decode this type of errors, for reasonable dimensions k. Suppose we now have an error matrix such that:

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

The Hamming weight of e is 9 and the rank of e is 4. We see that it is not possible to decode with both metrics with this error matrix. In fact, rank metric is more interesting when the error has a particular structure such as:

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

With Hamming metric, there are still 9 errors out of 16 bits transmitted, no binary code of length 16 is able to decode properly while with the rank metric, the rank of e is only 1. We can easily decode with such error (for instance, with a Gabidulin code of parameters $[4, 2, 3]$). Of course, such a structured error does not happen necessarily often. In the following, we show that this type of error may happen in a certain case where the rank metric behaves better than the classical Hamming metric in watermarking applications. In the next section, we introduce an embedding method we used to combine with rank metric codes.

3. LATTICE QIM (LQIM)

Vector quantization was introduced by B. Chen and Gregory W. Wornell ([9, 10]). To embed binary information, we have two cosets of the lattice $\Delta\mathbb{Z}^L$ cosets of dimension L and a quantizer Q_m:

$$\begin{aligned} \Lambda_0 = -\frac{\Delta}{4} + \Delta\mathbb{Z}^L, \Lambda_1 = \frac{\Delta}{4} + \Delta\mathbb{Z}^L \\ y = Q_m(x, \Delta) = \left\lfloor \frac{x}{\Delta} \right\rfloor \Delta + (-1)^{m+1} \frac{\Delta}{4}, \end{aligned} \tag{1}$$

with x a host sample, y the quantized sample and $m = 0, 1$.

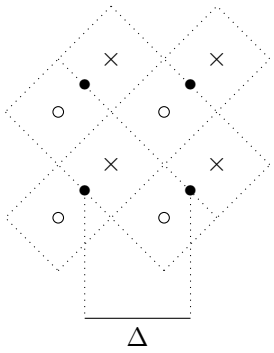

Fig. 1. Representation of the lattice or quantization space with $L = 2$ and quantization step Δ. Crosses represents quantization vectors carrying bit 1 and bit 0 are carried by circles.

Figure 1 illustrates an example of the lattice space in dimension $L = 2$. For any circle or cross (say a quantized vector y), the diamond delimited by the dotted lines will be denoted by "quantization cell". To embed information in x, one can quantize x to the nearest quantization cell center y.

For detection, we compute which coset is closer to the received vector z:

$$\begin{aligned} \hat{m} &= \underset{m\in\{0,1\}}{\arg\min}\, dist(z, \Lambda_m), \\ dist(z, \Lambda) &= \min_{y\in\Lambda} \|z - y\|_2 \end{aligned} \tag{2}$$

As an illustration, z will be decoded into y the quantization cell center where z is located. In the next section, we explain how the experiment results allow us to see the error structure produced by a luminance modification on a LQIM watermark coupled with a rank metric code.

4. STUDY OF THE LUMINANCE ATTACK

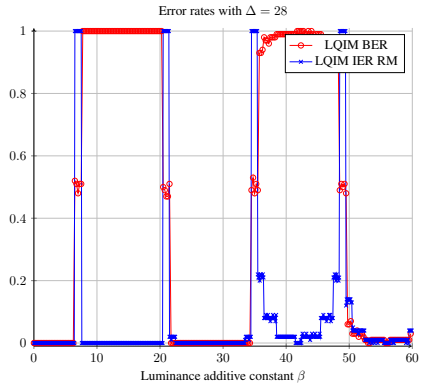

Fig. 2. Red curve : Binary error rate of LQIM method in function of β. This curve is similar when β is negative. Blue curve : Image error rate of LQIM method combined with a rank metric code in function of β. Each point of the blue curve represents the ratio of images where the error rank $Rank(e) \geq 2$ (failed decoding).

Results were made using the Corel image database where 1000 images where randomly chosen for our tests among the 10000 images available. Embedded messages are randomly generated binary sequences of 49 bits with $L = 6$ and $\Delta = 28$ so that image quality is maintained at DWR $= 35db$ in the spatial domain. Pixel values were randomly chosen in an image to embed the message (in total, $49\times6 = 294$ coefficients).

4.1. Detection analysis after attack

The first experiment shows binary error rates (BERs) between the original payload and the decoded payload in function of the luminance constant β. The following equation illustrates how the luminance additive constant change of parameter β acts on a quantized vector y:

$$z = y + \beta \times u \tag{3}$$

with $u = (1, ..., 1) \in \mathbb{R}^L$ and z a corrupted version of y. When β increases, z saturates. From a geometrical point of view (in 2D for figure 1), every z travel from one quantization cell to another flipping the embedding bit at every quantization cell change. In figure 2, one can notice that the red curve looks like a square waveform and we can distinguish three cases: $\beta = 0, 0.5, 1$. In the first case, there is no error at detection at regular intervals (such as $\beta \in [14, 21[$). Then, the third case is similar to the first case; BER $= 1$ also happens at regular intervals (such as $\beta \in [5, 14[$). This third case represents situations when every bits of the payload are flipped. The second case (BER $= 0.5$), detected payloads are random sequences. Unlike the previous cases, $\beta = 0.5$ only happens for specific values instead of intervals ($\beta = 4, 21, 40, ...$). This curve clearly shows the existence of a partially structured error form. Moreover, rank metric codes are well suited against this type of error.

4.2. Luminance error structure

When we apply a luminance modification on an image, every quantized vectors will suffer the same distortion of the form $z - y = \beta u$ according to equation 3. In other words, if we imagine the quantization space as in figure 1, every corrupted vectors z will travel through the quantization cells. Indeed, BER $= 0$ means that every z are located in a cell carrying the original bit, not necessarily the one it was quantized at embedding. When BER $= 1$, every z are located in a cell carrying the opposite version of the embedded bit. In the next subsection, we show how a rank metric code can remove the majority of errors.

4.3. Rank metric codes application

As a second experiment, we used a rank metric code of parameters $[7, 3, 5]$ (corrects at most errors of rank 2) and measured Image Error Rates (IERs) and embedded a codeword as the watermark payload. IERs are the ratio of images where the message was not decoded by the rank metric, *i.e.*, the error rank $Rank(e) \geq 2$. In figure 2, this code is very efficient because IERs are 0 for every β except at four values. When z makes the transition from one cell to another, LQIM decoder decodes with BER $= 0.5$ (which means we have full rank errors). On the other hand, a similar parameters Hamming code is $[47, 23, 11]$ and corrects at most 5 binary errors over 47 bits. In that case, the IER curve obtained with this code is identical to the red BER curve because either we have no binary error either every bits of the payload is flipped, *i.e.*, the Hamming metric is inefficient against this attack. In practice, the decoder cannot guess β and the probability to find β such that errors are not structured for rank metric codes depends on Δ : a small value means a higher probability to decode with errors. Moreover, the red curve in figure 2 does not look like a square waveform for some images due to the random nature of the pixel values they contain. Some BER values might be slightly under 1 or slightly above 0, this is why we choose, for a start, a rank metric code of parameters $(7, 3, 5)$ correcting at most errors of rank 2 to correct more errors. Theoretically,

a code correcting errors of rank at most 1 is enough. In the context of a luminance image processing, these codes provide almost perfect error correction. In the next subsection, we show how to improve the LQIM rank metric decoder.

4.4. Enhanced LQIM rank metric decoder

The luminance channel is parametrized by the additive constant β. Suppose a watermarked image is damaged by this channel. At decoding, we have the modified versions $z = y + \beta$. Equation 3 shows how to improve the decoder performances by adding a controlled luminance modifications. Periodically, one can notice that we cannot properly decode for $\beta = \sqrt{2}\Delta/4$ with $k \in \mathbb{Z}$. This case represents transition states traveling from one quantization cell to another, *i.e.*, vectors z are located at the boundaries of quantization cells.

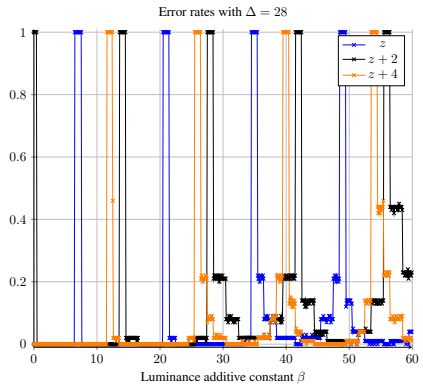

Fig. 3. Image error rates of LQIM method combined with a rank metric code in function of β with controlled distortions using $\delta = 0, 2, 4$ to shift error rates curves from one to another (spike shift).

Let $\delta_i \leq \sqrt{2}\Delta/4, \delta_i \in \mathbb{N}, 1 \leq i \leq n$. Then, from figure 3, we deduce the following property: there is a unique i such that the corrupted image with $z + \delta_i$ cannot be well decoded with LQIM rank metric decoder and for every $j \neq i$, corrupted image with $z + \delta_j$ is perfectly well decoded with LQIM rank metric decoder. By modifying z with δ_i, we guarantee to have the majority of $z + \delta_j$ perfectly decoded. A majority vote strategy on the decoding of multiple attacked image can get rid of the spikes at the only cost of time decoding. Taking $n = 3$ suffices to have good results with this decoding strategy. We have $d = \sqrt{2}\Delta/4$, $\delta_1 = 0$, $\delta_2 = d/3$ and $\delta_3 = 2d/3$. In the experiments, $d \simeq 6$ and we used $\delta_1 = 0$, $\delta_2 = 2$ and $\delta = 4$ and they represent modified versions of transmitted z. Then, we extract 3 estimations of the original payload. Using the proposed property, two out of the three payloads are correct given fixed β. In figure 4, error rates are 0 for almost every β. For non-zero values, some images may have lost some information because of the image processing, so it is impossible for the proposed method to retrieve those information.

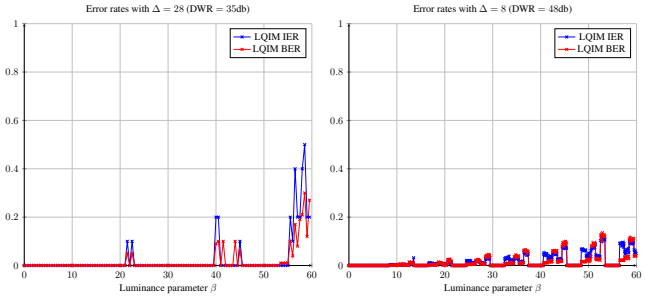

Fig. 4. Red and blue curves respectively represents BER and IER of LQIM embedding with enhanced LQIM rank metric decoder in function of β. Experiments with $\Delta = 28, 8$ are showed.

As a summary, we proposed a strategy to improve the LQIM decoder combined with a rank metric code. Cases where BER $= 0.5$ can be avoided by taking an average estimation of multiple decoded payloads where the luminance parameter was modified on purpose. With this enhanced decoder, it is possible to use smaller quantization steps for more invisible watermark (see figure 4 with $\Delta = 8$). Indeed, the correction ability of rank metric codes eliminates all errors except at some particular β values. Using the proposed property, we can shift curves *i.e.* IER spikes and compute the majority vote of payloads. Compared to other approaches against luminance image processing (such as embedding in the low frequency coefficients in the DCT domain), we innovate with a theoretically perfect resistance with weak quantization noise at the cost of some capacity (code rate k/n). Due to space constraints, we chose to focus on the luminance image processing to fully understand how rank metric codes work. Results are very interesting for luminance because of the error structure but less interesting for others attacks (such as JPEG compression and additive white gaussian noise) where the error type is less structured.

5. CONCLUSION

We introduced a new kind of error correcting codes which uses the rank distance instead of the usual Hamming distance. Then, we studied the robustness of the association of LQIM method and rank metric codes against luminance image processing. We proposed an analysis of the luminance attack and showed that rank metric codes provide great correction power because of the errors structured nature. A first application of these codes with Lattice QIM method provided good results but some errors still remain (spikes). Finally, we gave a method to enhance the LQIM rank metric decoder to obtain a theoretically error free decoding. Rank metric codes can be of great interest in digital watermarking. Of course, this result is limited to luminance modifications and similar attacks. As a perspective, we plan to study more about how rank metric codes can be applied in digital watermarking.

6. REFERENCES

[1] Matt L Miller, Ingemar J Cox, Jean-Paul MG Linnartz, and Ton Kalker, "A review of watermarking principles and practices," *Digital signal processing in multimedia systems*, pp. 461–485, 1999.

[2] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: theory and practice," *IEEE Transactions on Signal Processing*, vol. 53, no. 10, pp. 3976–3987, Oct 2005.

[3] Wadood Abdul, Philippe Carré, and Philippe Gaborit, "Error correcting codes for robust color wavelet watermarking," *EURASIP Journal on Information Security*, vol. 2013, no. 1, pp. 1, Feb 2013.

[4] Danilo Silva and Frank R Kschischang, "On metrics for error correction in network coding," *IEEE Transactions on Information Theory*, vol. 55, no. 12, pp. 5479–5490, 2009.

[5] Philippe Gaborit, Olivier Ruatta, Julien Schrek, and Gilles Zémor, "New results for rank-based cryptography," in *International Conference on Cryptology in Africa*. Springer, 2014, pp. 1–12.

[6] Ernest Mukhamedovich Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, 1985.

[7] Ernst M. Gabidulin, *A fast matrix decoding algorithm for rank-error-correcting codes*, pp. 126–133, Springer Berlin Heidelberg, Berlin, Heidelberg, 1992.

[8] Pierre Loidreau, *A Welch–Berlekamp Like Algorithm for Decoding Gabidulin Codes*, pp. 36–45, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.

[9] 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*, vol. 47, no. 4, pp. 1423–1443, 1999.

[10] P. Moulin and R. Koetter, "Data-hiding codes," *Proceedings of the IEEE*, vol. 93, no. 12, pp. 2083–2126, Dec 2005.