A SOLUTION TO GAIN ATTACK ON WATERMARKING SYSTEMS: LOGARITHMIC HOMOGENEOUS RATIONAL DITHER MODULATION

M. A. Akhaee, A. Amini, G. Ghorbani, and F. Marvasti

Advanced Communication Research Institute of Sharif University of Technology, Tehran, Iran
http://acri.sharif.edu

ABSTRACT

Among the many attacks against watermarked data, the gain attack is less supported with countermeasures. The effectiveness of this attack becomes more evident in quantization-based embedding algorithms such as Dither Modulation (DM). In this paper, the general solution for both block and sample type DM schemes that are robust against gain attacks is considered. Among the solutions, we concentrate on a subclass of the algorithms which are insensitive to additive noise attacks; i.e., we introduce watermarking schemes which are both robust against gain and additive noise attacks. The simulation results confirm the desired performance of the final algorithm against these attacks while outperform other gain invariant schemes.

***Index Terms*—** Gain attack, rational dither modulation, watermarking.

1. INTRODUCTION

Digital watermarking is a process in which some information is embedded within a digital media so that the inserted data becomes part of the media. Among several proposed algorithms, Quantization Index Modulation (QIM) [1] has attained great popularity due to its lossless performance when lattice-based codebooks are used. Among lattice-based codebooks using scalar and uniform quantizers Dither Modulation (DM) is a popular scheme for its simplicity [1].

The main drawback of QIM algorithm is its vulnerability against gain attack which can easily occur through a simple channel. Three types of solutions have been proposed to tackle this problem: i) Adopting auxiliary pilots through the watermarked signal ii) using spherical codewords with correlator decoding [2] and iii) introducing a domain in which the embedding process is invariant to gain attack [3].

The first solution decreases the security of the algorithm, since pilots are deterministic objects in the main signal and can be easily detected. The second approach imposes high computational cost which increases the complexity of the QIM algorithm. Although the third approach preserves both the security and simplicity of the QIM method. Based on rational dither modulation (RDM) idea two methods are introduced which use RDM in frequency [4] and logarithmic domain [5] to make the algorithm robust to LTI filtering and gamma correction attack, respectively. However, the embedding function introduced in [3] and used in [4] and [5] is presented without any support. In this paper, the main focus is on the design of such functions.

In this paper, we first identify the functions which are invariant to gain attack. For this purpose, we consider the functions which act on a block of the host signal (a vector) and produce a scalar. After mathematically investigating the general features of these functions, we narrow down to a subclass which provides robustness against noise attack. The latter restriction is fulfilled by studying the sensitivity against additive white noise by means of the l_2-norm of the gradient function; we choose the embedding function in such a way that the sensitivity be uniform at different points. This characteristic seems to be a proper choice for uniform quantization levels. After quantizing the output of the function, the reverse procedure is performed to achieve the watermarked data. In order to attain the minimum embedding distortion, optimization using Lagrange coefficients has been employed.

2. GENERAL GAIN INVARIANT FUNCTIONS

The aim is to introduce block based embedding domains which are insensitive to gain attack. The structure of the studied method is as follows:

Let the vector $\mathbf{x}_{n\times 1}$ represent the input block which is a part of the host signal. By introducing a proper function $f : \mathbb{R}^n \to \mathbb{R}$, we convert the vector $\mathbf{x}$ into a scalar x. The produced value is then quantized according to a Dither Modulation (DM) rule ($Q_{b_k}(x)$). Finally, using an inverse-like function $\tilde{f}_{\mathbf{x}} : \mathbb{R} \to \mathbb{R}^n$, we generate a block ($\hat{\mathbf{x}}_{n\times 1}$)with the same size as the input for which we have $f(\hat{\mathbf{x}}) = Q_{b_k}(x)$; i.e., the original block $\mathbf{x}$ will be replaced with this new block $\hat{\mathbf{x}}$. Therefore, it is preferable that the Mean Squared Error (MSE) of this replacement be minimized.

To introduce the desired watermarking scheme, we first focus on the choice of the function f; afterwards, we will investigate how the respective $\tilde{f}_{\mathbf{x}}$ should be chosen.

For robustness against gain attack, the mentioned function f should satisfy the following condition:

$$\forall\, \mathbf{x} \in \mathbb{R}^n\,,\ \alpha \in \mathbb{R}: \quad f(\alpha \cdot \mathbf{x}) = f(\mathbf{x}) \tag{1}$$

where α is introduced to show the imposed gain as an attack. If we assume $\mathbf{x} = [x_1, \ldots, x_n]^T$, by setting $\alpha = \frac{1}{x_1}$ in the above equation, we obtain:

$$x_1 \neq 0\ \Rightarrow f(x_1, \ldots, x_n) = f\big(1, \underbrace{\frac{x_2}{x_1}}_{\tilde{x}_1}, \ldots, \underbrace{\frac{x_n}{x_1}}_{\tilde{x}_{n-1}}\big) \tag{2}$$

Thus, by knowing $f(1, \tilde{x}_1, \ldots, \tilde{x}_{n-1})$, f is almost completely known everywhere ($x_1 \neq 0$). Therefore, by having the values of f at the points in the plane $x_1 = 1$, f is completely determined (except for points of the plane $x_1 = 0$). If f is continuous, the values of f at the points of the plane $x_1 = 0$ could also be estimated by knowing the values at the points in the plane $x_1 = 1$:

$$\begin{aligned} &\forall\, \delta > 0,\ \exists\, \epsilon_\delta > 0, \forall\, 0 < \epsilon < \epsilon_\delta : \\ &\big|f(0, x_2, \ldots, x_n) - f(\epsilon, x_2, \ldots, x_n)\big| < \delta \\ \Rightarrow \quad &\big|f(0, x_2, \ldots, x_n) - f\big(1, \frac{x_2}{\epsilon}, \ldots, \frac{x_n}{\epsilon}\big)\big| < \delta \end{aligned} \tag{3}$$

or equivalently:

$$f(0, x_2, \ldots, x_n) = \lim_{\epsilon \to 0} f\big(1, \frac{x_2}{\epsilon}, \ldots, \frac{x_n}{\epsilon}\big) \quad (4)$$

Consequently, choosing the function $f : \mathbb{R}^n \to \mathbb{R}$ is equivalent to choosing the function $g : \mathbb{R}^{n-1} \to \mathbb{R}$:

$$\begin{cases} \tilde{\mathbf{x}} \triangleq [\frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}]^T \\ g(\tilde{\mathbf{x}}) \triangleq f(1, \tilde{x}_1, \ldots, \tilde{x}_{n-1}) \end{cases} \quad (5)$$

On the other hand, if we choose g and then define f with respect to g, the produced function will be robust against gain attack which means that the general solution for the gain attack problem is to select f through an arbitrary function g.

3. PROPOSED DATA EMBEDDING DOMAIN

By choosing an arbitrary continuous function $g : \mathbb{R}^{n-1} \to \mathbb{R}$ and then converting it to $f : \mathbb{R}^n \to \mathbb{R}$, we obtain a variety of options for function g which is robust against gain attack. We can further improve the watermarking scheme by imposing some restrictions on the function g so as to achieve desired characteristics in return.

3.1. Robustness Against Additive Noise

Among the possible options, we choose robustness against additive white noise which is usually regarded as a key feature in communication problems. For this purpose, we consider the gradient of the function f; the l_2-norm of the gradient vector is believed to be a good measure of the sensitivity of the method against additive white noise. It should be mentioned that by scaling the function f, its gradient will also be scaled; thus, for the mentioned measure, the l_2-norm of the gradient at each point should be considered relative to that of the other points. We will later point out this issue.

$$\begin{aligned} & f(x_1, \ldots, x_n) = g\big(\frac{x_2}{x_1}, \ldots, \frac{x_n}{x_1}\big) \\ \Rightarrow\ & \nabla f\big|_{\mathbf{x}} = \frac{1}{x_1} \begin{bmatrix} -\tilde{\mathbf{x}}^T \\ \mathbf{I}_{(n-1)\times(n-1)} \end{bmatrix} \cdot \nabla g\big|_{\tilde{\mathbf{x}}} \end{aligned} \quad (6)$$

where $\mathbf{I}_{(n-1)\times(n-1)}$ represents the identity matrix of the size $n-1$. Now we can describe the l_2-norm of the vector $\nabla f\big|_{\mathbf{x}}$ as a function of the l_2-norm of $\nabla g\big|_{\tilde{\mathbf{x}}}$:

$$\big\|\nabla f(\mathbf{x})\big\|^2 = \frac{1}{x_1^2}\Big(\big\|\nabla g(\tilde{\mathbf{x}})\big\|^2 + \big|\langle \nabla g(\tilde{\mathbf{x}}), \tilde{\mathbf{x}}\rangle\big|^2\Big) \quad (7)$$

Before continuing the analysis, we should mention that no matter how g is chosen, gradient of f is not well-defined at the origin:

$$\begin{aligned} \big\|\nabla f(\alpha\, \mathbf{x})\big\|^2 &= \frac{1}{\alpha^2 x_1^2}\Big(\big\|\nabla g(\tilde{\mathbf{x}})\big\|^2 + \big|\langle \nabla g(\tilde{\mathbf{x}}), \tilde{\mathbf{x}}\rangle\big|^2\Big) \\ &= \frac{1}{\alpha^2}\big\|\nabla f(\mathbf{x})\big\|^2 \\ \Rightarrow\ & \lim_{\alpha \to 0} \big\|\nabla f(\alpha\, \mathbf{x})\big\|^2 = \infty \end{aligned} \quad (8)$$

Decreasing the sensitivity of the scheme to the input additive white noise is almost equivalent to decreasing $\|\nabla f(\alpha\ \mathbf{x})\|$. Comparing the main two terms in (7) ($\|\nabla g(\tilde{\mathbf{x}})\|^2$ and $|\langle \nabla g(\tilde{\mathbf{x}}), \tilde{\mathbf{x}}\rangle|^2$), we see that if $\langle \nabla g(\tilde{\mathbf{x}}), \tilde{\mathbf{x}}\rangle \neq 0$, for large values of $\|\tilde{\mathbf{x}}\|$, the dominant term will be $\big|\langle \nabla g(\tilde{\mathbf{x}}), \tilde{\mathbf{x}}\rangle\big|^2$. The naive choice for g is to force it to satisfy $\langle \nabla g(\tilde{\mathbf{x}}), \tilde{\mathbf{x}}\rangle \equiv 0$; by this constraint we will always have $\nabla g(\tilde{\mathbf{x}}) \perp \tilde{\mathbf{x}}$, which means that g remains constant along the lines passing through the origin, or in simple words $g(a\ \tilde{\mathbf{x}}) = g(\tilde{\mathbf{x}})$ for all $a \in \mathbb{R}$. Therefore,

$$\begin{aligned} \big\|\nabla f(ax_1, x_2 \ldots, x_n)\big\|^2 &= \frac{1}{a^2 x_1^2}\big\|\nabla g\big(\frac{\tilde{\mathbf{x}}}{a}\big)\big\|^2 \\ &= \frac{1}{a^2 x_1^2}\big\|\nabla g(\tilde{\mathbf{x}})\big\|^2 \end{aligned}$$

$$\Rightarrow \lim_{a \to 0} \big\|\nabla f(ax_1, x_2 \ldots, x_n)\big\| = \infty \quad (9)$$

which means that with this choice of g, at the points of the plane $x_1 = 0$, the method is too sensitive against noise.

As can be seen in (7), gradient of f not only depends on the vector $\tilde{\mathbf{x}}$ but also the element x_1; since g is only a function of $\tilde{\mathbf{x}}$, it is desirable to somehow approximate x_1 using $\tilde{\mathbf{x}}$. For this reason, we assume that the elements of the vector $\mathbf{x}$ have i.i.d. zero-mean distribution with variance σ_{sig}^2 (not necessarily gaussian). With this assumption, if n is large enough, we have:

$$\begin{aligned} \|\tilde{\mathbf{x}}\|^2 &= \frac{x_2^2 + \cdots + x_n^2}{x_1^2} \approx \frac{(n-1)E\{x_i^2\}}{x_1^2} \\ \Rightarrow\ & \frac{1}{x_1^2} \approx \frac{\|\tilde{\mathbf{x}}\|^2}{(n-1)\sigma_{sig}^2} \end{aligned} \quad (10)$$

Using the above approximation, we can rewrite (7) as:

$$\big\|\nabla f(\mathbf{x})\big\|^2 \approx \frac{\|\tilde{\mathbf{x}}\|^2}{(n-1)\sigma_{sig}^2}\Big(\big\|\nabla g(\tilde{\mathbf{x}})\big\|^2 + \big|\langle \nabla g(\tilde{\mathbf{x}}), \tilde{\mathbf{x}}\rangle\big|^2\Big) \quad (11)$$

Now it is time to describe the measure on the gradient. As previously mentioned, the norm of the gradient itself is not a good measure; we choose g in such a way that the l_2 norm of the gradient vector of f at different points be almost the same. In this way, the sensitivity against additive noise will almost be the same at different points which justifies the use of uniform quantization levels.

$$\begin{aligned} & \big\|\nabla f(\mathbf{x})\big\|^2 \approx \text{const.} \Rightarrow \\ & \|\tilde{\mathbf{x}}\|^2\Big(\big\|\nabla g(\tilde{\mathbf{x}})\big\|^2 + \big|\langle \nabla g(\tilde{\mathbf{x}}), \tilde{\mathbf{x}}\rangle\big|^2\Big) \approx \text{const.} \end{aligned} \quad (12)$$

To fulfill the above condition, we select g to be a function of $\|\tilde{\mathbf{x}}\|$; i.e., there exists $h : \mathbb{R} \to \mathbb{R}$ such that $g(\tilde{\mathbf{x}}) = h(\|\tilde{\mathbf{x}}\|)$. Thus, we have:

$$\begin{aligned} & \nabla g(\tilde{\mathbf{x}}) = \frac{h^{'}(\|\tilde{\mathbf{x}}\|)}{\|\tilde{\mathbf{x}}\|} \cdot \tilde{\mathbf{x}} \\ \Rightarrow\ & \begin{cases} \big\|\nabla g(\tilde{\mathbf{x}})\big\|^2 = \big|h^{'}(\|\tilde{\mathbf{x}}\|)\big|^2 \\ \langle \nabla g(\tilde{\mathbf{x}}), \tilde{\mathbf{x}}\rangle = h^{'}(\|\tilde{\mathbf{x}}\|) \cdot \|\tilde{\mathbf{x}}\| \end{cases} \end{aligned} \quad (13)$$

where $h^{'}$ stands for the derivative of h. Now we can restate the gradient of f using $h^{'}$ as:

$$\nabla f(\mathbf{x}) = \frac{\|\tilde{\mathbf{x}}\|^2\big(\|\tilde{\mathbf{x}}\|^2 + 1\big)}{(n-1)\sigma_{sig}^2} \cdot \big|h^{'}(\|\tilde{\mathbf{x}}\|)\big|^2 \quad (14)$$

Combining (12) and (14) we get:

$$z \in \mathbb{R} \ \Rightarrow\ z^2(z^2+1) \cdot |h^{'}(z)|^2 = \text{Const.} \quad (15)$$

It is easy to solve the above equation for h:

$$\exists\gamma,\beta\in\mathbb{R}:\quad h(z)=\gamma\ln\left(\frac{\sqrt{z^2+1}-1}{\sqrt{z^2+1}+1}\right)+\beta \tag{16}$$

Using the relations between the functions f, g and h, the above choice of h can be translated to f as shown below. We refer to these functions as Logarithmic Homogeneous Rational DM (LHRDM):

$$\exists\gamma,\beta\in\mathbb{R}: f(\mathbf{x})=\gamma\ln\left(\frac{\sqrt{x_1^2+\cdots+x_n^2}-|x_1|}{\sqrt{x_1^2+\cdots+x_n^2}+|x_1|}\right)+\beta \tag{17}$$

3.2. Data Embedding

For data hiding, any kind of quantization-based watermarking method can be used. Due to the advantages of QIM method which were discussed earlier, we employ this approach for data embedding in our scheme. For simplicity, we assume a binary modulation for digital insertion of data.

$$y=Q_{b_k}(f(\mathbf{x})) \tag{18}$$

where $b_k\in\{-1,1\}$ and y is the watermarked scalar value. In the decoder side where the received data may have undergone some possible attacks, the value z will be produced as the mentioned scalar. The decoding process is performed according to the minimum Ecludean distance rule as:

$$\hat{b}=\arg\min_{-1,1}\|z_k-Q_{b_k}(z_k)\| \tag{19}$$

In the encoder, after quantizing $f(\mathbf{x})$, the quantized scalar should be converted back to an input block to replace the original vector. To this aim we introduce an inverse-like function $\tilde{f}_{\mathbf{x}}:\mathbb{R}\to\mathbb{R}^n$, which produces a block ($\hat{\mathbf{x}}_{n\times 1}$) with the same size as the input for which we have $f(\hat{\mathbf{x}})=y$. Since the inverse function is not unique, we define the requested vector by an optimization problem as will be shown below; we find the best l_2 approximation of the input vector which results in the quantized scalar using the introduced function:

- For a given vector $\mathbf{a}=[a_1,\ldots,a_n]^T$ and the value α, find the vector $\mathbf{x}$ closest to $\mathbf{a}$ (Euclidean distance) which satisfies:

$$k(\mathbf{x})=\frac{\sqrt{x_1^2+\cdots+x_n^2}-|x_1|}{\sqrt{x_1^2+\cdots+x_n^2}+|x_1|}=\alpha \tag{20}$$

To solve the above minimization problem, we use the Lagrange coefficients method. Thus, we define the following parameters:

$$\begin{aligned} R_{\mathbf{x}} &\triangleq \sqrt{x_1^2+\cdots+x_n^2}\\ R_{\mathbf{a}} &\triangleq \sqrt{a_1^2+\cdots+a_n^2}\\ \hat{\alpha} &\triangleq k(\mathbf{a})=\frac{\sqrt{a_1^2+\cdots+a_n^2}-|a_1|}{\sqrt{a_1^2+\cdots+a_n^2}+|a_1|} \end{aligned} \tag{21}$$

therefore,

$$k(\mathbf{x})=\frac{R_{\mathbf{x}}-|x_1|}{R_{\mathbf{x}}+|x_1|} \tag{22}$$

It is easy to convert the condition $k(\mathbf{x})=\alpha$, to the form

$$(1-\alpha)R_{\mathbf{x}}-(1+\alpha)|x_1|=0 \tag{23}$$

A similar equation is valid for the vector $\mathbf{a}$:

$$\begin{aligned} &(1-\hat{\alpha})R_{\mathbf{a}}-(1+\hat{\alpha})|a_1|=0\\ &\Rightarrow(1-\hat{\alpha})^2(a_1^2+\cdots+a_n^2)=(1+\hat{\alpha})^2a_1^2\\ &\Rightarrow a_2^2+\cdots+a_n^2=\frac{4\hat{\alpha}}{(1-\hat{\alpha})^2}\cdot a_1^2 \end{aligned} \tag{24}$$

Now the desired vector $\mathbf{x}$ can be regarded as the solution of the following conditional minimization problem:

$$\begin{cases}\text{Cost:} & J(\mathbf{x})=\sum_{i=1}^{n}(x_i-a_i)^2\\ \text{Condition:} & C(\mathbf{x})=(1-\alpha)R_{\mathbf{x}}-(1+\alpha)|x_1|=0\end{cases} \tag{25}$$

Using the Lagrange method, at the optimum point we have:

$$\begin{aligned} &\exists\,\lambda\in\mathbb{R}:\quad \nabla J(\mathbf{x})=\lambda\nabla C(\mathbf{x})\\ &\Rightarrow \text{for } i\geq 2:\quad 2(x_i-a_i)=\lambda\frac{(1-\alpha)x_i}{R_{\mathbf{x}}}\\ &\Rightarrow \frac{x_2-a_2}{x_2}=\frac{x_3-a_3}{x_3}=\cdots=\frac{x_n-a_n}{x_n}\\ &\Rightarrow \exists\,\theta\in\mathbb{R},\quad \text{for } i\geq 2:\quad x_i=\theta\cdot a_i \end{aligned} \tag{26}$$

By using the above results, we get back to the original condition:

$$\begin{aligned} &(1-\alpha)R_{\mathbf{x}}=(1+\alpha)|x_1|\\ &\Rightarrow(1-\alpha)^2\left(x_1^2+\theta^2(a_2^2+\cdots+a_n^2)\right)=(1+\alpha)^2x_1^2\\ &\Rightarrow x_1=\underbrace{\frac{1-\alpha}{1-\hat{\alpha}}\sqrt{\frac{\hat{\alpha}}{\alpha}}}_{\mu}\cdot\theta\cdot a_1 \end{aligned} \tag{27}$$

The only thing left for minimization is to find θ:

$$\begin{aligned} J(\mathbf{x}) &= (\mu\cdot\theta-1)^2a_1^2+(\theta-1)^2(a_2^2+\ldots a_n^2)\\ \frac{\partial}{\partial\theta}J(\mathbf{x}) &= 0\\ &\Rightarrow\quad \theta=\frac{\mu a_1^2+a_2^2+\cdots+a_n^2}{\mu^2a_1^2+a_2^2+\cdots+a_n^2} \end{aligned} \tag{28}$$

Thus, the main minimizer can be briefly stated as:

$$\begin{cases} \hat{\alpha}\triangleq\frac{\sqrt{a_1^2+\cdots+a_n^2}-|a_1|}{\sqrt{a_1^2+\cdots+a_n^2}+|a_1|}\\ \mu\triangleq\frac{1-\alpha}{1-\hat{\alpha}}\sqrt{\frac{\hat{\alpha}}{\alpha}}\\ x_1=\mu\frac{\mu a_1^2+a_2^2+\cdots+a_n^2}{\mu^2a_1^2+a_2^2+\cdots+a_n^2}\cdot a_1\\ x_i=\frac{\mu a_1^2+a_2^2+\cdots+a_n^2}{\mu^2a_1^2+a_2^2+\cdots+a_n^2}\cdot a_i \qquad i\geq 2 \end{cases} \tag{29}$$

Here, we want to present a sample-based version of LHRDM. In other words, in each sample one bit must be embedded. Thus, the block of samples should slide sample by sample over the host signal. That is each block $\hat{x}_k$ should be composed of new host sample and $n-1$ previous watermarked samples. $x_k=\left(x_k,y_{k-1},y_{k-2},\ldots,y_{k-n+1}\right)$. Embedding is performed as before and the value of $f(\mathbf{x})$ should be quantized according to (18). The

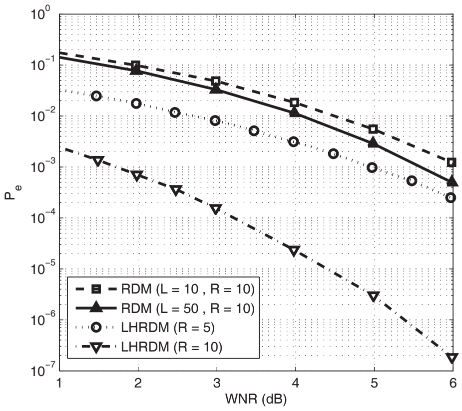

Fig. 1. The comparison of the block based LHRDM with RDM for different values of the block size (R) and memory size (L) (DWR=25dB)

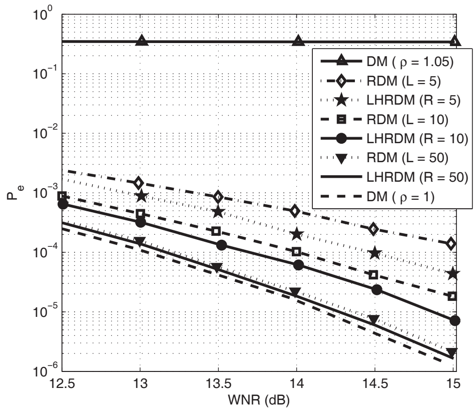

Fig. 2. Empirical values of BER for sample based LHRDM and RDM with different values of R and L (DWR=25dB)

only difference is that in the inverse procedure in order to produce the watermarked block $\hat{\mathbf{x}}_k$, we are just authorized to change the first component of $\mathbf{x}_k$, i.e., x_k and the other samples could not be modified, as they are previous watermarked samples. Consequently, we have, $\hat{\mathbf{x}}_k = \left(\hat{x}_k, y_{k-1}, y_{k-2}, ..., y_{k-n+1}\right)$ and $f(\hat{\mathbf{x}}_k) = y$ which y is the quantized value of $f(\mathbf{x})$. Like the prior problem, by applying these results in the same condition of (25) and using (24), we obtain:

$$y_k = \hat{x}_k = \frac{1-\alpha}{1-\hat{\alpha}}\sqrt{\frac{\hat{\alpha}}{\alpha}}.x_k \tag{30}$$

4. NUMERICAL RESULTS

In this section we show the robustness of the proposed block-based LHRDM against AWGN attack in comparison with RDM [3]. Since the proposed domain acts on blocks of the host signal, to have a fair comparison with RDM acting on single samples, we simulate RDM over all samples of the block (using repetition code) and hard decoding is performed.

Similar to [5], simulation is performed on positive signals. Thus an iid Gaussian signal with a specific mean and the unity variance has been considered. The block size (R) is chosen 10. In order to measure the performance, we evaluate the bit error rate (BER) at a fixed Document to Watermark Ratio (DWR=25 dB) for various Watermark to Noise Ratios (WNRs). The error probability is calculated over several simulations with 5000 bits in each one. To compare the proposed method with RDM, the performance of RDM at the same bit rate, DWR and host signal characteristics with two different memory sizes (L) is depicted. As shown in Fig. 1, the proposed scheme outperforms the RDM scheme. This is expectable, since the embedding domain in the proposed scheme is somehow optimized to be noise insensitive. Besides, increasing the block size (R), better results are achieved. This fact is due to (10) where the sample x_1 is estimated via the variance of the block samples.

In the second experiment, we compare the sample-based version of the LHRDM with DM and RDM algorithm. To this aim, the ideal DM with the gain factor equal to 1 is considered as the reference case. The performance of the DM method in the presence of gain factor equal to 1.05 is also presented. In Fig. 2, the results are depicted for LHRDM and RDM schemes for different values of R and L, respectively. As can be seen, for the equal value of R and L, our method slightly outperforms RDM. Thus, the p-norm function employed in [3] is a good choice for the sample-based methods.

5. CONCLUSION

A general form for the quantization-based data hiding approaches which are robust against gain and noise attacks has been proposed. We show that all the gain invariant functions have some sort of singularity at the origin. Data embedding procedure is performed on the scalar value which is the output of the proposed gain invariant function via quantization. Then the inverse function is applied in such a way that the least distortion is imposed to the host samples in each block. The sample based version of LHRDM is also presented. Experimental results justify the desired performance of the proposed method for the Gaussian host signal. The proposed method outperforms the RDM algorithm with the same memory size L.

6. REFERENCES

[1] B. Chen and G. Wornell, “Quantization Index Modulation: A class of provably good methods for digital watermarking and information embedding,” *IEEE Trans. on Inf. Theory*, vol. 47, pp. 1423-1443, May, 2001.

[2] M. L. Miller, G. J. Doerr, and I. J. Cox, “Applying informed coding and embedding to design robust, high capacity, watermark,” *IEEE Trans. Image Process.*, vol. 13, pp. 792-807, June, 2004.

[3] F. Perz-Gonzalez, C. Mosquera, M. Barni, and A. Abrado, “Rational dither modulation: A high rate data-hiding method invariant to gain attacks,” *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3960-3975, Oct. 2005.

[4] F. Perz-Gonzalez, C. Mosquera, “Quantization-based data hiding robust to linear-time-invariant filtering,” *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 2, pp. 137-152, June 2008.

[5] P. Guccione, M. Scagliola, “Hyperbolic RDM for nonlinear valumetric distortions,” *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 2, pp. 25-35, March 2009.