Robust Lossless Watermarking of Relational Databases Based on Circular Histogram Modulation

Javier Franco-Contreras, *Member, IEEE*, Gouenou Coatrieux, *Senior Member, IEEE*,
Fréderic Cuppens, *Member, IEEE*, Nora Cuppens-Boulahia, *Member, IEEE*, and Christian Roux, *Fellow, IEEE*

***Abstract*— In this paper, we adapt the robust reversible watermarking modulation originally proposed by Vleeschouwer *et al.* for images to the protection of relational databases. The resulting scheme modulates the relative angular position of the circular histogram center of mass of one numerical attribute for message embedding. It can be used for verifying database authentication as well as for traceability when identifying database origin after it has been modified. Beyond the application framework, we theoretically evaluate the performance of our scheme in terms of capacity, distortion, and robustness against two common database modifications: 1) addition and 2) removal of tuples. To that end, we model the impact of the embedding process and of database modifications on the probability distribution of the center of mass position. We further verify experimentally these theoretical limits within the framework of a medical database of more than one million of inpatient hospital stay records. We show that under the assumptions imposed by the central limit theorem, experimental results fit the theory. We also compare our approach with two recent and efficient schemes so as to prove its benefits.**

***Index Terms*— Watermarking, relational database, information security.**

I. Introduction

NOWADAYS, relational databases are more and more remotely accessed and shared not only because of their growing economical value but also because of the evolution of data-mining tools which turn them into a fundamental piece in decision making. However, such an access intensifies risks in terms of security: confidentiality, integrity (i.e. proof data have not been modified), authenticity (i.e proof of data origins), traceability as well as of copyright protection concerns. Indeed, outsourced data can be rerouted from their final objectives or modified without permission. Every year, several information leaks are reported, even in domains of activity where data are very sensitive such as healthcare [1].

In such a context, watermarking appears as an interesting security mechanism that completes common encryption based solutions. Basically, it allows the embedding of a message, like some security attributes (e.g. digital signature, authenticity code, ...), in a host document in some multimedia format (image, XML, database...). It encodes the message within host data based on the principle of controlled distortion. By definition, the watermark should be imperceptible to users and is independent of the host data file format storage. Watermarked data can be said *a posteriori* protected as they can be accessed while being protected by embedded security attributes. Since the preliminary work of Agrawal *et al.* in 2002 [2], several database watermarking methods have been proposed [3]–[5]. Most of them focus on copyright or fingerprinting/traitor tracing applications [6], [7] where watermarks are required to be robust so as to survive database modifications, authorized or malevolent. A few of them have been designed fragile and are devoted to database integrity protection. In opposition to robustness, a fragile watermark will not survive data modifications [8]–[10].

Whatever the method, authors assume some data distortion (e.g. modification or modulation of attributes' values as in [3] or variation of tuples' order like in [8]) can be carried out for message insertion without perturbing the interpretation or any *a posteriori* uses of data. In order to better take into account watermark imperceptibility, most recent schemes modify values of attributes under distortion constraints. As example, in [3] the embedding process does not modify numerical attributes for which data quality conditions, expressed in terms of mean square error, are not respected. In [4] and [11] Gross-Amblard and Lafaye *et al.* look at preserving the response to a priori known queries of aggregation, and modulate pairs of tuples in consequence. Shehab *et al.* express distortion constraints on the attribute values and statistics (e.g. mean, standard deviation) so as to adapt watermark distorsion by means of optimization techniques [5]. Another

Manuscript received April 30, 2013; revised September 13, 2013 and November 21, 2013; accepted November 21, 2013. Date of publication December 5, 2013; date of current version January 28, 2014. This work was supported in part by the French National Research Agency-Project ANR ARPEGE PAIRSE, in part by the French Armament Procurement Agency-Project DGA RAPID FRAG&TAG, and in part by the Brittany Region Council. The associate editor coordinating the review of this manuscript and approving it for publication was Prof. C.-C. Jay Kuo.

J. Franco-Contreras, G. Coatrieux, and C. Roux are with the Institut Mines-Telecom, Telecom Bretagne, Inserm U1101 LaTIM, Brest 29238, France, and also with the Université Européenne de Bretagne, Bretagne F29200, France (e-mail: javier.francocontreras@telecom-bretagne.eu; gouenou.coatrieux@telecom-bretagne.eu; christian.roux@telecom-bretagne.eu).

F. Cuppens and N. Cuppens-Boulahia are with the Institut Mines-Telecom, Telecom Bretagne, UMR CNRS 3192 Lab-STICC, Cesson Sévigné 35576, France, and also with the Université Européenne de Bretagne, Bretagne F29200, France (e-mail: frederic.cuppens@telecom-bretagne.eu; nora.cuppens@telecom-bretagne.eu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIFS.2013.2294240

whole set of methods embed data by modulating the order of tuples within a relation [8], [9], [12]. Because these latters do not modify attributes' values, they are said "distortion-free." Nevertheless, such a technique makes the watermark dependent on the database structure and on the way it is stored, limiting its interest to a small number of applications. In their vast majority they are devoted to database integrity verification. One last category of methods refers to reversible or lossless watermarking. The reversibility property allows the recovery of the original data from their watermarked version by inverting watermarking modifications. With such an approach it becomes possible: i) to let access to the watermarked data (if the watermark does not interfere with database post-uses), and; ii) when necessary, to get back to the original data (e.g. database post-process as well as for watermark update).

Up to now, existing reversible approaches have been derived or adapted from lossless image watermarking. This is why they work on numerical attributes rather than on categorical attributes. Notice that the first reversible scheme for categorical attributes has been presented by Coatrieux *et al.* in 2011 [13]. Anyway, most of these schemes are fragile [14] and devoted to database authentication. Robust lossless reversible watermarking has been experimented only recently. In [15], Gupta and Pieprzyk propose a zero-bit watermarking method where a meaningless pattern is embedded into secretly chosen tuples. To do so, a secretly chosen LSB from the integer part of a numerical value is replaced by a pseudo-random generated bit. The original value is then inserted into the space left by right shifting the LSB of the fractional part. The presence of this pattern is checked by the detector, indicating if the database has been watermarked or not. In order to reduce introduced distortion, Farfoura *et al.* [16], [17] suggest watermarking the fractional part of one numerical attribute by means of prediction-error expansion modulation proposed by Alattar in [18]. Although this method is said robust against common database manipulations (e.g. tuple addition or removal), a rounding integer operation may destroy the watermark. More generally, difference expansion modulation has not been designed for being robust to attributes' values modifications (this is the same for images). In this work, in order to overcome the above issues, we propose to exploit the robust lossless watermarking modulation originally proposed for images by De Vleeschouwer *et al.* [19] and integrate it within a common database watermarking scheme. As we will see, this one manipulates circular histograms of data and is less or not at all sensitive to the rounding integer operation or dependent on the existence of attributes with fractional parts. Moreover, our method does not depend on the storing structure of the database, making it robust to tuple reordering in a relation.

The rest of this paper is organized as follows. Section II presents the proposed embedding modulation as well as the main steps of a common chain of database watermarking. We also introduce two watermarking schemes: one is fragile and devoted to database authentication; the second is robust and proposed for database integrity and authenticity control. In Section III, we theoretically evaluate the performance of our schemes in terms of capacity and robustness against common database modifications or attacks: tuple insertion and suppression. We empirically verify these theoretical limits in Section IV by means of experiments conducted on one real medical database of patient stay records. We also compare our approach with two recent and efficients schemes in terms of robustness, distortion and complexity in Section V. Section VI, concludes this paper.

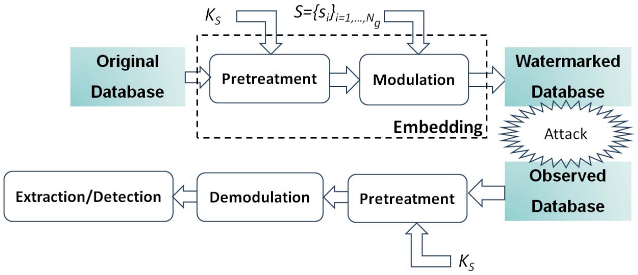


Fig. 1. A common database watermarking chain.

II. Proposed schemes

In this section, we first present a common chain of database watermarking, the way we exploit the modulation of De Vleeschouver *et al.* [19] and, by next, two watermarking schemes.

A. Database Watermarking

By definition, a database DB is composed of a finite set of relations $\{R_i\}_{i=1,\dots,N_R}$. From here on and for sake of simplicity, we will consider one database based on one single relation constituted of N unordered tuples $\{t_u\}_{u=1,\dots,N}$, each of M attributes $\{A_1, A_2, \dots, A_M\}$. The attribute A_n takes its values within an attribute domain and $t_u.A_n$ refers to the value of the n^{th} attribute of the u^{th} tuple. Each tuple is uniquely identified by either one attribute or a set of attributes, we call its primary key $t_u.PK$.

Most database watermarking schemes from the literature follow the procedure depicted in Fig. 1. It comprises two fundamental stages: message embedding and message detection/extraction. As it can be seen, the embedding stage includes a pretreatment, the purpose of which is to make the watermark insertion/reading independent of the database structure or the way this one is stored. To do so, one solution executed before message insertion consists in a "tuple grouping operation" which outputs a set of N_g non-intersecting groups of tuples $\{G^i\}_{i=1,\dots,N_g}$. The most usual strategy to calculate the group index number $n_u \in [0, N_g - 1]$ of the tuple t_u is given in eq.(1) [3], [5]. It relies on a cryptographic hash function applied to the primary key of t_u, i.e. $t_u.PK$, concatenated with a secret watermarking key K_S (in eq.(1) '|' represents the concatenation operator). The use of a cryptographic hash function, such as the Secure Hash Algorithm (SHA), ensures the secure partitioning and the equal distribution of tuples into the groups.

$$n_u = H(K_S|H(K_S|t_u.PK)) mod N_g \tag{1}$$

One bit or symbol of the message is then embedded per group of tuples by modulating or modifying the values of one or several attributes according to the rules of the retained watermarking modulation (e.g. modifying the attribute's statistics as in [3] or the tuple order as in [8]). Thus, with N_g groups, the inserted message corresponds to a sequence of N_g symbols $S = \{s_i\}_{i=1,\dots,N_g}$.

Watermark reading works in a similar way. Tuples are first reorganized in N_g groups. From each group, one message symbol is detected or/and extracted depending on the exploited modulation and the application framework. We come back on these aspects in Section II-C. While tuple primary keys are not modified, the knowledge of the watermarking key ensures synchronization between embedding and reading stages.

B. Circular Histogram Based Modulation

In [19], De Vleeschouwer *et al.* present two different modulations, one robust and one fragile, both based on a circular interpretation of bijective transformations. In the robust case, we focus on here, they propose to divide a grayscale image into N_b blocks of pixels. Each block is equally divided into two sub-blocks whose histograms are mapped onto a circle. In order to embed one bit in a block, the relative angle between both circular histograms' center of mass is modulated. Depending on the bit value to embed in a block, this operation consists in shifting of $\pm\Delta$ the pixel gray values of one pixel sub-block and of $\mp\Delta$ those of the other sub-block. In this work, we apply this robust modulation in order to embed one symbol s_i of the watermark (or equivalently of the message) in each group of tuples, i.e. $\{G^i\}_{i=1,\dots,N_g}$.

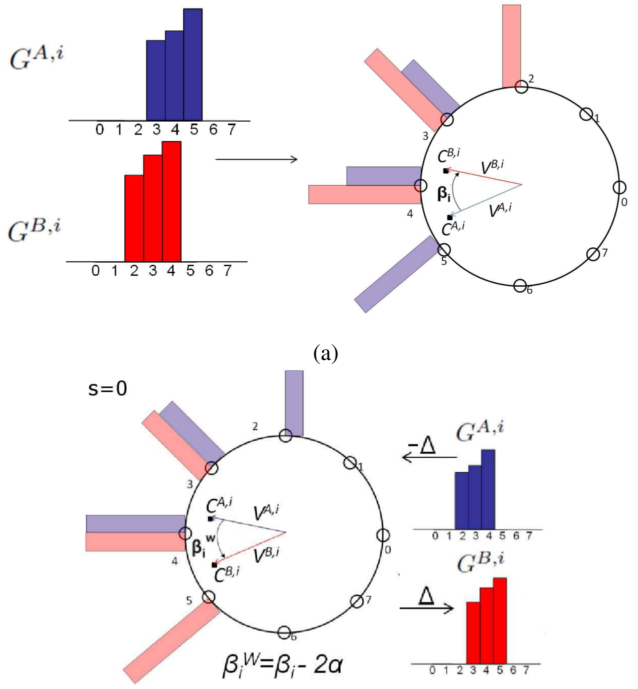
Let us consider one group of tuples G^i and A_n be the numerical attribute retained for embedding. The group is equally divided in two sub-groups of tuples $G^{A,i}$ and $G^{B,i}$, following the same principles of tuple grouping described in section II-A. The subgroup membership $n_{u_{sg}}$ of one tuple is given by:

$$n_{u_{sg}} = \begin{cases} G^{A,i} & if H(K_S|t_u.PK)mod2 = 0 \\ G^{B,i} & if H(K_S|t_u.PK)mod2 = 1 \end{cases} \quad (2)$$

By next, the histograms of the attribute A_n in each subgroup $G^{A,i}$ and $G^{B,i}$ are calculated and mapped onto a circle. Then, and as illustrated in Fig. 2(a), the histogram center of mass $C^{A,i}$ (resp. $C^{B,i}$) of the sub-group $G^{A,i}$ (resp. $G^{B,i}$) and its associated vector $V^{A,i}$ (resp. $V^{B,i}$) are calculated. To do so, let us assume the attribute domain of A_n corresponds to the integer range [0,L-1]. Notice that if A_n is a numerical attribute encoded on a fixed number of bits b, then it can take 2^b distinct values. The module and phase of $V^{A,i}$ (resp. $V^{B,i}$) can be calculated from its Cartesian coordinates given by [19]:

$$X = \frac{1}{M}\sum_{l=0}^{L-1} n_l cos\left(\frac{2\pi l}{L}\right)$$
$$Y = \frac{1}{M}\sum_{l=0}^{L-1} n_l sin\left(\frac{2\pi l}{L}\right)$$
$$M = \sum_{l=0}^{L-1} n_l \quad (3)$$

where n_l is the cardinality of the circular histogram class l of $G^{A,i}$ (i.e. when A_n takes the value l). From that standpoint, the module of $V^{A,i}$ equals $R = \sqrt{X^2+Y^2}$ and its phase, we also call mean direction μ, is given by:



(a)

(b)

Fig. 2. (a) Histogram mapping of each sub-group G^A and G^B onto a circle. The angle between the vectors pointing the centers of mass is modulated in order to embed one symbol of the message. (b) Embedding of a symbol s = 0, corresponding to a rotation of the circular histograms of $G^{A,i}$ and $G^{B,i}$ in opposite directions with an angle step α in order to modify the sign of β_i. This is equivalent to the addition of Δ to the attribute values in $G^{B,i}$ and $-\Delta$ to those of $G^{A,i}$.

$$\mu = \begin{cases} \arctan(Y/X) \ if \ \ X > 0 \\ \frac{\pi}{2} \ if \ \ X = 0, Y > 0 \\ -\frac{\pi}{2} \ if \ \ X = 0, Y < 0 \\ \pi + \arctan(Y/X) \ else \end{cases} \quad (4)$$

Let us now consider the embedding of a sequence of bits into the database, or more precisely the insertion of the symbol $s = 0/1$ into G^i. As in [19], we modulate the relative angle $\beta_i = (\widehat{V^{A,i}, V^{B,i}}) \simeq 0$ between $V^{A,i}$ and $V^{B,i}$. Depending if we want to insert $s = 0$ or $s = 1$, we change it into its watermarked version β_i^W by rotating the circular histograms of $G^{A,i}$ and $G^{B,i}$ in opposite directions with an angle step α as follows [see Fig. 2(b)]:

$$\beta_i^W = \beta_i - 2\alpha \ if \ s = 0 \ (\beta_i^W < 0)$$
$$\beta_i^W = \beta_i + 2\alpha \ if \ s = 1 \ (\beta_i^W > 0) \quad (5)$$

The angle step α is given by:

$$\alpha = \left|\frac{2\pi\Delta}{L}\right| \quad (6)$$

where Δ corresponds to the shift amplitude of the histogram [see Fig. 2(b)]. More precisely, modifying the angle β_i of $2\alpha(2s-1)$ results in adding $(2s-1)\Delta$ to the attributes of $G^{A,i}$ and $(1-2s)\Delta$ to those of $G^{B,i}$.

At the reading stage, the sign of β_i^W indicates the embedded symbol as well as the direction of rotation to follow so as to invert the insertion process and recover the original value of β_i.

However, at this point, not all of the groups of tuples can convey one symbol of message. In fact and from a more general point of view, we propose to distinguish three classes of groups. In the case $|\beta_i| < 2\alpha$ one can insert $s = 0$ or $s = 1$, as it is possible to swap the position of $V^{A,i}$ and $V^{B,i}$. We refer groups fulfilling this condition as "carrier-groups," due to the fact they can convey one symbol of the watermark. We identify two other kind of groups: "non-carrier groups" and "overflowed groups." They have to be considered separately and handled specifically so as to make the scheme fully reversible. Non-carrier groups are those for which the angle distortion α is not big enough to make change the sign of β_i [see Fig. 3(a)]. In order not confusing such non-carriers with carriers at the reading stage, they are modified in the following way [see Fig. 3(a)]:

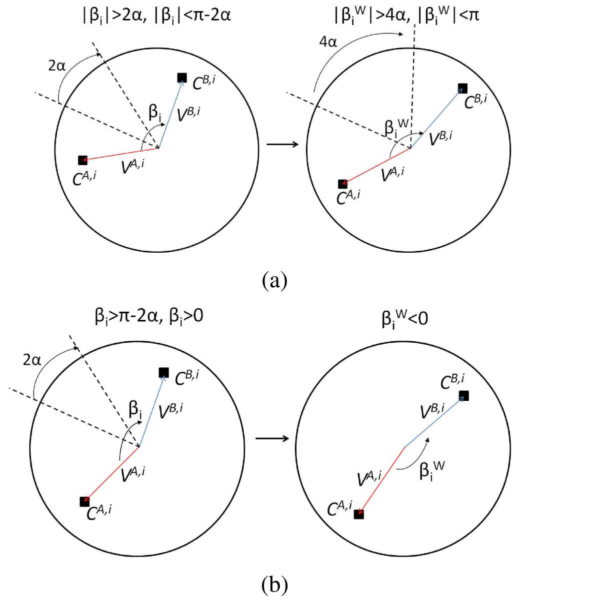
$$\begin{aligned} \beta_i^W &= \beta_i + 2\alpha \; if \; \beta_i > 0 \\ \beta_i^W &= \beta_i - 2\alpha \; if \; \beta_i < 0 \end{aligned} \tag{7}$$

In fact, this process results in increasing the angle $\widehat{V^{A,i}, V^{B,i}}$. At the reading stage, these watermarked non-carrier groups are those such as $|\beta_i^W| > 4\alpha$ and can consequently be easily retrieved and differentiated from the watermarked carriers, which belong to the range $[-4\alpha, 4\alpha]$. Thus the reader just has to add or subtract α based on eq.(7) so as to restore these watermarked non-carrier groups.

The last situation corresponds to groups of tuples we refer as "overflow-groups". This means groups for which an "angle overflow" may occur if modified. Basically and as exposed in Fig. 3(b), one overflow-group is a non-carrier group which angle $|\beta_i|$ exceeds $\pi - 2\alpha$. If modified according to rules given in eq. (7), signs of β_i and β_i^W will be different and the watermark reader will not restore properly the original angle β_i based on eq.(7). For instance, if $\beta_i > \pi - 2\alpha$ and $\beta_i > 0$ [see Fig. 3(b)] then adding 2α will lead to $\beta_i^W < 0$. On its side the reader will thus restore the group subtracting 2α instead of -2α. The solution we adopt so as to manage these problematic groups and to make the modulation fully reversible is the following one. At the embedding stage, these groups are left unchanged (i.e. not modified). We inform the reader about the existence of such groups by means of some extra data (a message overhead) inserted along with the message. By doing so, our scheme is blind. Basically, this message overhead avoids the reader confusing overflow groups with non-carriers. It corresponds to a vector O_v of bits stating that watermarked groups such as $\beta_i^W > \pi - 2\alpha$ or $\beta_i^W < -(\pi - 2\alpha)$ are overflow-groups (unmodified) or non-carrier groups (which angle has been shifted based on eq.(7)). For instance, if $O_v(k) = 1$ then the k^{th} group such as $\beta_i^W > \pi - 2\alpha$ or $\beta_i^W < -(\pi - 2\alpha)$ is a non-carrier group; otherwise it is an overflow-group.

C. Fragile and Robust Database Watermarking Schemes

Database watermark robustness (resp. fragility) is defined as the ability (resp. inability) to extract/detect the embedded message after an attack such as tuple insertion, tuple deletion or attribute modification. In our approach, if we look at one watermarked group of tuples, this one will be said robust to an attack if it remains in the same class (carrier, non-carrier) while encoding the same symbol. In practice, this unlikely happens and three different situations can occur: i) a symbol error, when the symbol embedded into a carrier group changes of value; ii) a carrier loss, when a carrier group becomes a non-carrier one; iii) a carrier injection, when a non-carrier group becomes a carrier. The most harmful scenarios result from carrier injections and deletions. They lead to a loss of synchronization between the embedder and the reader. As example, in the case of a carrier injection, the reader will extract a longer sequence of symbols and, consequently, will face difficulties for interpreting the message. This is the reason why we propose two different reversible schemes. The first one is fragile while the second has been designed so as to be robust to different kinds of attacks.



(a)

(b)

Fig. 3. Problematic groups: Non-carrier groups and overflow groups (black squares represent circular histogram centers of mass). (a) Non-carrier groups are such $|\beta_i| > 2\alpha$ (*on the left*); they are watermarked applying eq. (7) (*on the right*). (b) Overflow groups are such as $|\beta_i^W| > \pi - 2\alpha$. In the given example $\beta_i^W > \pi - 2\alpha$ (*on the left*); if modified the reader will identify $\beta_i^W < 0$ and will not properly invert eq.(7); it will subtract 2α to β_i^W instead of -2α (*on the right*).

Our fragile scheme consists in the embedding of a sequence of bits such as $S = \{s_i\}_{i=1,\ldots,N_c}$, $s_i \in \{0, 1\}$, where N_c is the number of available carriers. This sequence includes the message m_s the user wants to insert along with the overhead O_v if necessary (see Section II-B). At the detection, the sequence of bits S is extracted directly from the carrier groups. In an applicative context, m_s may correspond to the digital signature of the database [8], [14]. At the reception, the recipient just has to compare the extracted signature to the one recomputed from the restored database so as to decide about the database integrity.

The main problem to solve in building a robust reversible watermarking scheme is to counteract synchronization issues

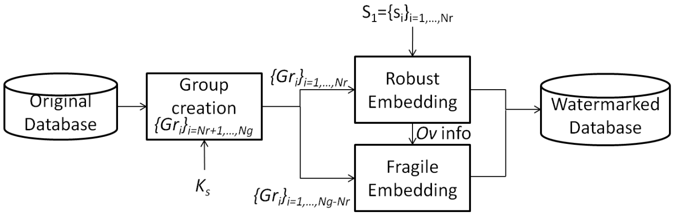


Fig. 4. Proposed robust scheme. The sequence S^1 is robustly embedded in the first N_r groups while the reconstruction information fills the $N_g - N_r$ remaining groups.

due to carrier injections or erasures. Notice that when De Vleeschouwer *et al.* introduce their robust modulation in [19], they do not specify how to manage such a situation. The solution we adopted to overcome these synchronization problems is based on the insertion of two watermark messages S^1 and S^2 of different nature. S^1 is made robust by means of a correlation based detection at the reading stage [20]. S^2 is fragile and contains at least the information required so as to ensure the reversibility of the scheme (i.e. it contains the overhead - see Section II-B). To make more clear our proposal, let us describe in details how message embedding is conducted. As illustrated in Fig. 4, S^1 corresponds to a fixed length pseudo-random sequence of N_r symbols such as: $S^1 = \{s^1_j\}_{j=1,...,N_r}$, with $s^1_j \in \{-1, +1\}$. S^1 is inserted into the N_r first groups of tuples (i.e. $\{G^j\}_{j=1...N_r}$) considering the previous modulation with s=-1/+1 in eq.(5). Notice that because all first N_r groups of tuples may not be carriers only (see Section II-B), it is possible S^1 differs from its embedded version $\hat{S}^1$ (even without modifications of the database). Indeed, $\hat{s}^1_j$ will be equal to +1/-1 if the corresponding group G^j is a carrier-group or equal to "null" if it is a non-carrier or overflow group. As stated before, S^1 is detected by means of a correlation measure $C_{S_1} =< \hat{S}^1, S^1 >$, where $\hat{S}^1$ is the sequence of symbols extracted from the N_r first watermarked groups. If C_{S^1} is greater than a decision threshold Tr_{S^1}, S^1 is said present in the database. Extracted null values as well as their corresponding symbols in S^1 are not considered in the correlation measurement (i.e. in C_{S^1}). The second sequence S^2 is inserted like in the previous fragile scheme into the other $N_g - N_r$ groups of tuples. It contains a sequence of bits which encodes the overhead $O_{v_{info}}$ required for reconstructing the whole database ($O_{v_{info}}$ indicates also overflow-groups into the first N_r groups).

As exposed, the robustness of this scheme stands on the fixed length of S^1 which is detected by means of correlation. By doing so, any carrier injections or erasures can simply be considered as a symbol error. However, S^1 needs to be known for the detection process. This solution is rather simple and more complex ones based on error correction codes can be drawn [3].

From a more applicative point of view, such a robust-fragile scheme may help to identify the database origin or ownership as well as the recipient with traitor tracing objective. Beyond, if the fragile capacity is large enough, S^2 may convey not only the overhead information $O_{v_{info}}$ but also a message m_s, like a digital signature of the database. To summarize the way this robust-fragile system works, let us consider the process its watermark reader follows:

1) Based on the watermarking key K_s and primary keys, tuples are reorganized into N_g groups.
2) $\hat{S}^1$ is extracted from the N_r first groups. C_{S^1} is computed and if it is greater than Tr_{S^1} the database origins are confirmed.
3) $\hat{S}^2$ is extracted from the carriers of the other $N_g - N_r$ groups. If the database has not been modified, then m_s and O_v are error-free extracted, making it possible to restore the database and then verify its integrity in the case m_s contains the database digital signature. On the contrary, m_s and O_v will be extracted with errors and will inform the user about database integrity loss.

Performance in terms of capacity of the above schemes depend on the number of carrier-groups and overflow-groups. On the other hand, as previously exposed robustness is established based on the probability of symbol error, carrier injection and carrier deletion. We will see in Sect. III that these probabilities rely in part on the number of tuples per group and also on the properties of the numerical attribute retained for message embedding.

III. Theoretical Performance

In this section we theoretically evaluate above schemes' performance in terms of capacity and robustness against two most common database attacks. Both depend on the statistical distribution of β_i and on the impacts of database modifications on this random variable.

A. Capacity Performance

As stated, capacity directly depends on the number of carrier groups, i.e. those for which $|\beta_i| < 2\alpha$ (see section II-B). Capacity can be established once the probability density function (p.d.f) of β_i over the database is known. To do so, let us first recall that β_i is associated to the group of tuples G^i and corresponds to the angle between the centers of mass of two circular histograms of the same attribute A_n considering two subgroups of tuples $G^{A,i}$ and $G^{B,i}$. Because each histogram represents the distribution of the attribute A_n, we can refer to some results issued from circular statistics, a sub-discipline of statistics that deals with data measured by angles or vectors, so as to get the p.d.f of β_i (see books [21] and [22] as main references).

As a preliminary statement, let us consider the circular data distribution of one attribute θ (i.e. its histogram mapped onto a circle). This can be seen as the p.d.f $f(\theta)$ of a discrete random variable θ which takes L values around the circle, i.e. in the finite set $\{\frac{2\pi l}{L}\}_{l=0,...,L-1}$. The mean direction μ of θ (or equivalently the phase of the vector associated to the center of mass of θ circular histogram) can be estimated based on a finite number of θ samples. Based on the Law of large numbers, it was shown by Fisher and Lewis [23] that for any circular data distribution $f(\theta)$ the difference between the real mean direction and its estimated value tends to zero as the number of samples used in the estimation tends to ∞. With the help of the central limit theorem, they also proved

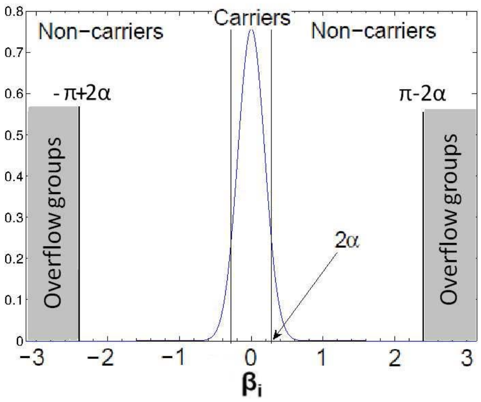


Fig. 5. β_i distribution.

that the distribution of the mean direction estimator approaches a normal distribution centered on the real mean direction of the circular data distribution.

Let us come back now to our problem. By modulating β_i we in fact modulate the angle between two mean directions $\mu^{A,i}$ and $\mu^{B,i}$ of two circular histograms attached to the same attribute A_n within two sub-groups of tuples $G^{A,i}$ and $G^{B,i}$ respectively (see section II-B). $\mu^{A,i}$ (resp. $\mu^{B,i}$) calculated on the sub-group $G^{A,i}$ (resp. $G^{B,i}$) can be seen as the estimator of the mean direction of the attribute A_n (i.e. $\theta = A_n$ in the above) using a number of samples or tuples $\frac{N}{2N_g}$, where (N and N_g are the number of tuples in the database and the number of groups respectively).

Thus, from the above we can easily state that both $\mu^{A,i}$ and $\mu^{B,i}$ follow a normal distribution. Based on the fact the difference between two normally distributed random variables is also a normally distributed random variable, then $\beta_i = \mu^{A,i} - \mu^{B,i}$ follows a centered normal distribution $\mathcal{N}(0, \sigma^2_{\beta_i})$ where $\sigma^2_{\beta_i}$ corresponds to its variance.

From this standpoint, based on the p.d.f of β_i (see Fig. 5) and for a given angle shift α, the probability a group of tuples is a carrier-group (see section II-B) and is defined as:

$$\mathbb{P}_{carrier} = \Phi\left(\frac{2\alpha}{\sigma_{\beta_i}}\right) - \Phi\left(-\frac{2\alpha}{\sigma_{\beta_i}}\right) \tag{8}$$

where Φ is the cumulative distribution function for a normal distribution, calculated as:

$$\Phi\left(\frac{2\alpha}{\sigma_{\beta_i}}\right) = \frac{1}{\sigma_{\beta_i}\sqrt{2\pi}} \int_{-\infty}^{2\alpha} e^{\frac{-t^2}{2\sigma^2_{\beta_i}}}\, dt \tag{9}$$

being t an auxiliary random variable. As common convention, we take $\Phi(-\infty) = 0$ and $\Phi(\infty) = 1$.

In practice, considering one numerical attribute, a database of N tuples and N_g groups, one just has to estimate $\sigma^2_{\beta_i}$ to find out the capacity limit of our fragile scheme. To do so, let us first estimate the variance of the mean directions as in [24]

$$\sigma^2_{\mu^{A,i}} = \sigma^2_{\mu^{B,i}} = \frac{\sigma_s^2}{\frac{N}{2N_g}R^2} \tag{10}$$

where: R corresponds to the module of center of mass vector (i.e. $V^{A,i}$, see Section II-B) and σ_s^2 is defined as [24]:

$$\sigma_s^2 = \sum_{l=0}^{L-1} sin^2(\frac{2\pi l}{L}) f(\frac{2\pi l}{L}) \tag{11}$$

The values $\{\frac{2\pi l}{L}\}_{l=0,\dots,L-1}$ are the bins of the circular histogram attached to the attribute A_n and $f(\frac{2\pi l}{L})$ their corresponding probabilities. Finally, due to the fact β_i results from the difference of two normally distributed random variables $\mu_{A,i}$ and $\mu_{B,i}$, its variance is:

$$\sigma^2_{\beta_i} = \frac{2\sigma_s^2}{\frac{N}{2N_g}R^2} \tag{12}$$

Notice that the above normal distribution assumption of β_i is verified in the cases when $\frac{N}{2N_g} \geq 30$ (see [25] for further details).

The carrier probability can then be derived from eq. (8), and the total amount of bits C_T one may expect to insert into the database is given by

$$C_T = N_g \cdot \mathbb{P}_{carrier} \tag{13}$$

In order to get the real capacity, one must subtract to C_T the number of bits used for encoding of the overhead, i.e. $|O_v|$ bits. This number of bits is directly linked to the probability β_i belongs to the range $[-\pi, -\pi + 4\alpha] \bigcup [\pi - 4\alpha, \pi]$. We recall that the overhead is a vector which components indicate by '0' or '1' whether a watermarked angle β_i^w the reader sees in the range $[-\pi, -\pi + 2\alpha] \bigcup [\pi - 2\alpha, \pi]$ has been shifted or not (see end of Section II-B).

$$|O_v| \leq N_g.\mathbb{P}_{[-\pi,-\pi+4\alpha]\bigcup[\pi-4\alpha,\pi]} \tag{14}$$

Where

$$\mathbb{P}_{[-\pi,-\pi+4\alpha]\bigcup[\pi-4\alpha,\pi]} = \left[\Phi\left(\frac{\pi}{\sigma_{\beta_i}}\right) - \Phi\left(\frac{\pi-4\alpha}{\sigma_{\beta_i}}\right)\right] + \left[\Phi\left(-\frac{(\pi-4\alpha)}{\sigma_{\beta_i}}\right) - \Phi\left(-\frac{\pi}{\sigma_{\beta_i}}\right)\right] \tag{15}$$

Finally, the length of the message one may expect to embed is upper bounded such as: $C \leq C_T - |O_v|$

From these results, we can conclude that, for a fixed value of α, the embedding capacity directly depends on the attribute's statistics. By extension, an uniformly distributed attribute will not be watermarkable as $\sigma^2_{\beta_i}$ will tend to ∞ (see eq.(12)) and the capacity to 0 (see eq.(8)).

B. Robustness Performance

Let us consider the watermarking of one database of β_i distribution given in Fig. 5, with a fixed angle shift amplitude α and a message constituted of a sequence S of uniformly distributed symbols $s_i \in \{-1, +1\}$ (i.e. like S^1 in section II-C). The resulting distribution of the watermarked angles, i.e. of the random variable β_i^W, over the whole database is given in Fig. 6, where we retrieve the different classes of angles (or equivalently of groups of tuples): non-carriers and carriers (see the modulation rules in section II-B). In such a framework, performance in terms of robustness depend on the probability a group of tuples changes of class (carrier or non-carrier) or of embedded symbol (in case the group is a carrier) after a database attack occurred. We propose to compute these probabilities considering two common database attacks or modifications: tuple addition or tuple removal. To do so, we need to express the impact of such an attack on the p.d.f of β_i^W; p.d.f we need to establish at first.

P.d.f of β_i^W classes: As depicted in Fig. 6, we propose to distinguish four classes depending if β_i^W is a carrier or a non-carrier and if it has been shifted by $+2\alpha$ or -2α. Notice that from here on, β_i overflow-angles (or equivalently overflow-groups of tuples, see section II-B) are considered as non-carriers; they do not influence message robustness. The p.d.f of each class can be modeled by one truncated normal distribution functions (see Appendix VI), where ϕ is the probability density function of the standard normal distribution:

- β_i^W Carriers - β_i shifted of 2α ($c+$ in Fig. 6).

$$f_{c+}(\beta_i^W) = \frac{\frac{1}{\sigma_{\beta_i}} \cdot \phi\left(\frac{\beta_i^W - 2\alpha}{\sigma_{\beta_i}}\right)}{\Phi\left(\frac{2\alpha}{\sigma_{\beta_i}}\right) - \Phi\left(-\frac{2\alpha}{\sigma_{\beta_i}}\right)}, \ \beta_i^W \in (0, 4\alpha)$$

- β_i^W Carriers - β_i shifted of -2α ($c-$ in Fig. 6).

$$f_{c-}(\beta_i^W) = \frac{\frac{1}{\sigma_{\beta_i}} \cdot \phi\left(\frac{\beta_i^W + 2\alpha}{\sigma_{\beta_i}}\right)}{\Phi\left(\frac{2\alpha}{\sigma_{\beta_i}}\right) - \Phi\left(-\frac{2\alpha}{\sigma_{\beta_i}}\right)}, \ \beta_i^W \in (-4\alpha, 0)$$

- β_i^W Non-carriers - β_i shifted of 2α ($nc+$ in Fig. 6).

$$f_{nc+}(\beta_i^W) = \frac{\frac{1}{\sigma_{\beta_i}} \cdot \phi\left(\frac{\beta_i^W - 2\alpha}{\sigma_{\beta_i}}\right)}{1 - \Phi\left(\frac{2\alpha}{\sigma_{\beta_i}}\right)}, \ \beta_i^W \in (4\alpha, \pi)$$

- β_i^W Non-carriers - β_i shifted of -2α ($nc-$ in Fig. 6).

$$f_{nc-}(\beta_i^W) = \frac{\frac{1}{\sigma_{\beta_i}} \cdot \phi\left(\frac{\beta_i^W + 2\alpha}{\sigma_{\beta_i}}\right)}{\Phi\left(\frac{-2\alpha}{\sigma_{\beta_i}}\right)}, \ \beta_i^W \in (-\pi, -4\alpha)$$

Deletion Attack: Let us consider the attacker randomly eliminates N_d tuples in a way such that each group G_i loses in average $\frac{N_d}{N_g}$ tuples. In G^i, reducing the number of tuples influences the accuracy of $\mu^{A,i}$ and $\mu^{B,i}$ which are by definition estimators of the mean direction of $G^{A,i}$ and $G^{B,i}$ circular histograms respectively. Considering the whole database, this does not modify the original nature of the p.d.f of $\mu^{A,i}$ and $\mu^{B,i}$ but increase their variance as well as by extension the one of β_i^W. From our knowledge, such a variance increase can be modeled by adding to β_i^w a centered normally distributed random variable ϵ_i such as $\epsilon_i \sim \mathcal{N}(0, \sigma_{\epsilon_i})$. As a consequence the p.d.f of the random variable associated to the attacked watermarked angles β_i^{del}, i.e. $\beta_i^{del} = \beta_i^w + \epsilon$, is obtained after the convolution of each p.d.f of the previous classes with the p.d.f of ϵ_i (see appendix VI) leading to:

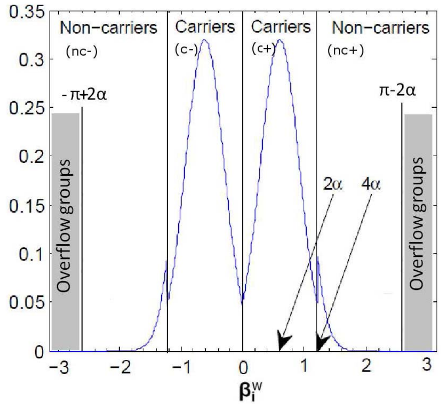


Fig. 6. β_i^W distribution after the embedding process. We retrieve carrier and non-carrier classes.

$$f_{c+}(\beta_i^{del}) = \frac{\frac{1}{\sigma_{\beta_i^{del}}}\phi\left(\frac{\beta_i^{del}-2\alpha}{\sigma_{\beta_i^{del}}}\right)\left[\Phi\left(\frac{\beta_i^{del}-4\alpha-\kappa_+}{\chi}\right)-\Phi\left(\frac{\beta_i^{del}-\kappa_+}{\chi}\right)\right]}{\Phi\left(\frac{2\alpha}{\sigma_{\beta_i}}\right) - \Phi\left(-\frac{2\alpha}{\sigma_{\beta_i}}\right)}$$

$$f_{c-}(\beta_i^{del}) = \frac{\frac{1}{\sigma_{\beta_i^{del}}}\phi\left(\frac{\beta_i^{del}+2\alpha}{\sigma_{\beta_i^{del}}}\right)\left[\Phi\left(\frac{\beta_i^{del}-\kappa_-}{\chi}\right)-\Phi\left(\frac{\beta_i^{del}+4\alpha-\kappa_-}{\chi}\right)\right]}{\Phi\left(\frac{2\alpha}{\sigma_{\beta_i}}\right) - \Phi\left(-\frac{2\alpha}{\sigma_{\beta_i}}\right)}$$

$$f_{nc+}(\beta_i^{del}) = \frac{\frac{1}{\sigma_{\beta_i^{del}}}\phi\left(\frac{\beta_i^{del}-2\alpha}{\sigma_{\beta_i^{del}}}\right)\left[1-\Phi\left(\frac{\beta_i^{del}-4\alpha-\kappa_+}{\chi}\right)\right]}{1 - \Phi\left(\frac{2\alpha}{\sigma_{\beta_i}}\right)}$$

$$f_{nc-}(\beta_i^{del}) = \frac{\frac{1}{\sigma_{\beta_i^{del}}}\phi\left(\frac{\beta_i^{del}+2\alpha}{\sigma_{\beta_i^{del}}}\right)\left[\Phi\left(\frac{\beta_i^{del}+4\alpha-\kappa_-}{\chi}\right)\right]}{\Phi\left(\frac{-2\alpha}{\sigma_{\beta_i}}\right)} \quad (16)$$

with $\kappa_+ = \frac{\sigma_{\epsilon_i}^2(\beta_i^{del}-2\alpha)}{\sigma_{\epsilon_i}^2+\sigma_{\beta_i}^2}$, $\kappa_- = \frac{\sigma_{\epsilon_i}^2(\beta_i^{del}+2\alpha)}{\sigma_{\epsilon_i}^2+\sigma_{\beta_i}^2}$ and $\chi = \frac{\sigma_{\epsilon_i}\sigma_{\beta_i}}{\sqrt{\sigma_{\epsilon_i}^2+\sigma_{\beta_i}^2}}$.

Considering one real database, the value of $\sigma_{\beta_i^{del}}$ can be derived from eq. (12) substituting the sub-group number of tuples $\frac{N}{2N_g}$ by $\frac{(N-N_d)}{2N_g}$ which takes into account the reduction of tuples. Consequently, the value of $\sigma_{\beta_i^{del}}$ is:

$$\sigma_{\beta_i^{del}}^2 = \frac{2\sigma_s^2}{R^2 \frac{N-N_d}{2N_g}} \quad (17)$$

In order to compute the p.d.f $f(\beta_i^{del})$ and by next evaluate the robustness, we also need $\sigma_{\epsilon_i}^2$. Given that the variance of the sum of two independent random variables is the sum of their respective variances, we obtain:

$$\sigma_{\epsilon_i}^2 = \sigma_{\beta_i^{del}}^2 - \sigma_{\beta_i}^2 = \frac{2\sigma_s^2}{R^2 \frac{N-N_d}{2N_g}} - \sigma_{\beta_i}^2 \quad (18)$$

Insertion Attack: Let us consider the attacker inserts N_i tuples and assume the corresponding added attribute values follow the same distribution as the original un-watermarked attribute A_n. Because of the cryptographic hash function used for distributing tuples into groups G^i (see eq.(1) in

Section II-A), we can consider new tuples are uniformly distributed among the groups $\{G^i\}_{i=1,...,N_g}$ as well as in sub-groups $G^{A,i}$ and $G^{B,i}$. In the sequel, we suppose the number of tuples added in each sub-group is high enough so as to respect central limit theorem conditions (see [25]). As described, such an attack can be modeled by a mixture of two populations: the watermarked tuples and the added un-watermarked tuples with mixture proportions parameters p_1 and p_2 such as $p_2 = 1 - p_1$ with $p_1 = \frac{N}{N+N_i}$.

Furthermore, under the central limit theorem conditions and from the work of Fisher and Lewis [23], the p.d.f of the resulting random variable β_i^{ins} (i.e. the p.d.f of β_i after watermarking and modification) remains normal. The variance and the mean of β_i^{ins} are however proportional to those of the angles β_i^W and angles β_{add} (angles related to the inserted tuples). The mean of β_i^{ins}, obtained with the expected value operator, is then such as

$$\begin{aligned} \mathrm{E}[\beta_i^{ins}] &= p_1\,\mathrm{E}[\beta_i^W] + p_2\,\mathrm{E}[\beta_{add}] \\ &= p_1\,\mathrm{E}[\beta_i^W]\,(as\,\mathrm{E}[\beta_{add}] = 0) \end{aligned} \tag{19}$$

while its variance is given by (see Apendix C):

$$\begin{aligned} \sigma^2_{\beta_i^{ins}} &= p_1^2(\sigma^2_{\beta_i^W} + (\mathrm{E}[\beta_i^W])^2) \\ &\quad + p_2^2(\sigma^2_{\beta_{add}} + (\mathrm{E}[\beta_{add}])^2) - (\mathrm{E}[\beta_i^{ins}])^2 \end{aligned} \tag{20}$$

Values of $\mathrm{E}[\beta_i^W]$ and $\sigma^2_{\beta_i^W}$ depend on the previously defined classes (i.e. *c*+, *c*-, *nc*+, *nc*-) leading to four mean values $\mathrm{E}[\beta_{i,c+}^{ins}]$, $\mathrm{E}[\beta_{i,c-}^{ins}]$, $\mathrm{E}[\beta_{i,nc+}^{ins}]$ and $\mathrm{E}[\beta_{i,nc-}^{ins}]$ and four different variance values $\sigma^2_{\beta_{i,c+}^{ins}}$, $\sigma^2_{\beta_{i,c-}^{ins}}$, $\sigma^2_{\beta_{i,nc+}^{ins}}$ and $\sigma^2_{\beta_{i,nc-}^{ins}}$ which can be obtained with the help of appendix A. As a consequence, the p.d.f of β_{ins} is given per class as follow:

$$\begin{aligned} f_{c+}(\beta_i^{ins}) &= \phi\left(\frac{\beta_i^{ins} - \mathrm{E}[\beta_{i,c+}^{ins}]}{\sigma^2_{\beta_{i,c+}^{ins}}}\right) \\ f_{c-}(\beta_i^{ins}) &= \phi\left(\frac{\beta_i^{ins} - \mathrm{E}[\beta_{i,c-}^{ins}]}{\sigma^2_{\beta_{i,c-}^{ins}}}\right) \\ f_{nc+}(\beta_i^{ins}) &= \phi\left(\frac{\beta_i^{ins} - \mathrm{E}[\beta_{i,nc+}^{ins}]}{\sigma^2_{\beta_{i,nc+}^{ins}}}\right) \\ f_{nc-}(\beta_i^{ins}) &= \phi\left(\frac{\beta_i^{ins} - \mathrm{E}[\beta_{i,nc-}^{ins}]}{\sigma^2_{\beta_{i,nc-}^{ins}}}\right) \end{aligned} \tag{21}$$

In the case N_i tuples are added to the whole database, one can determine the standard deviation σ_{add} of β_{add} similarly as before:

$$\sigma^2_{\beta_{add}} = \frac{\sigma_s^2}{(N_i/2N_g)R^2} \tag{22}$$

Robustness Performance - Probabilities of "Error": The robustness of our scheme is characterized by three situations after an attack occurred:

- "Symbol error," of probability $\mathbb{P}_e$. It concerns carrier groups for which embedded symbols have been changed.
- "Carrier loss," of probability $\mathbb{P}_l$. Such a situation occurs when a carrier-group becomes a non-carrier group, it can be seen as a symbol erasure or deletion.
- "Carrier injection," of probability $\mathbb{P}_i$. This happens when a non-carrier-group turns into a carrier-group, it can also be viewed as a symbol injection.

$\mathbb{P}_e$, $\mathbb{P}_l$ and $\mathbb{P}_i$ can be derived from a hypothesis testing problem with the following set of four hypothesis:

- H_0 corresponds to the case $s_i = -1$, i.e. $\beta_i^W \in c-$.
- H_1 corresponds to the case $s_i = 1$, i.e. $\beta_i^W \in c+$.
- H_2 represents "negative" non-carriers, i.e. $\beta_i^W \in nc-$.
- H_3 represents "positive" non-carriers, i.e. $\beta_i^W \in nc+$.

The probability the watermark reader returns the wrong symbol value while the group remains a carrier-group, i.e. $\mathbb{P}_e$, corresponds to cases where only H_0 and H_1 hypothesis are considered with errors, i.e. with the acceptance of H_0 (resp. H_1) when the correct hypothesis is H_1 (resp. H_0). Thus $\mathbb{P}_e$ is expressed as:

$$\mathbb{P}_e = \frac{1}{2}Pr(H_1|H_0) + \frac{1}{2}Pr(H_0|H_1) \tag{23}$$

Depending on the attack, i.e tuple insertion or removal, P_e can be refined. As example, if the deletion attack is considered then

$$\begin{aligned} \mathbb{P}_e &= \frac{Pr(4\alpha > \beta_i^{del} > 0|H_0) + Pr(-4\alpha < \beta_i^{del} < 0|H_1)}{2} \\ &= \frac{\int_0^{4\alpha} f_{c_-}(\beta_i^{del})d\beta_i^{del} + \int_{-4\alpha}^{0} f_{c_+}(\beta_i^{del})d\beta_i^{del}}{2} \end{aligned} \tag{24}$$

The probability of carrier loss, i.e. $\mathbb{P}_l$, can be similarly derived and is calculated as:

$$\begin{aligned} \mathbb{P}_l &= \frac{1}{2}Pr(H_2|H_0) + \frac{1}{2}Pr(H_3|H_1) \\ &= \frac{Pr(\beta_i^{del} < -4\alpha|H_0) + Pr(\beta_i^{del} > 4\alpha|H_1)}{2} \\ &= \frac{\int_{-\pi}^{-4\alpha} f_{c_-}(\beta_i^{del})d\beta_i^{del} + \int_{4\alpha}^{\pi} f_{c_+}(\beta_i^{del})d\beta_i^{del}}{2} \end{aligned} \tag{25}$$

$\mathbb{P}_i$, i.e. the probability of a carrier injection, is obtained on its side as follows:

$$\begin{aligned} \mathbb{P}_i &= Pr(H_0|H_2) + Pr(H_1|H_3) \\ &= Pr(\beta_i^{del} > -4\alpha|H_2) + Pr(\beta_i^{del} < 4\alpha|H_3) \\ &= \int_{-4\alpha}^{0} f_{nc-}(\beta_i^{del})d\beta_i^{del} + \int_{0}^{4\alpha} f_{nc+}(\beta_i^{del})d\beta_i^{del} \end{aligned} \tag{26}$$

In order to get these probabilities in the case of the tuple insertion attack, one just has to use β_{ins} instead of β_{del} in eq. (24), (25), (26).

IV. Experimental Results

The purpose of this section is to verify the theoretical performance of our system in terms of capacity and robustness in the framework of one real database.

A. Dataset & Watermarking Scheme Parameterization

The database we use is constituted of one relation of about two million tuples issued from one real medical database containing pieces of information related to inpatient stays in French hospitals. Only one million are watermarked. The others will for example serve the tuple insertion attack.

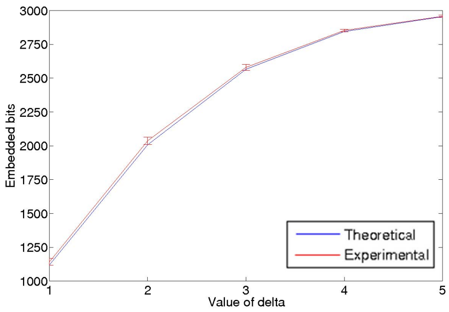


Fig. 7. Capacity depending on the shift amplitude Δ for *Age* attribute taking 3000 groups.

In this table, each tuple is represented by fifteen attributes like the hospital identifier (*id_hospital*), the patient stay identifier (*id_stay*), the patient age (*age*), the stay duration (*dur_stay*) and several other data useful for statistical analysis of hospital activities. In the upcoming experiments, the attributes *id_hospital* and *id_stay* were concatenated and considered as the primary key used by next for tuple groups and subgroups constitution (see Section II). Two numerical attributes were considered for the tests and watermarked independently: patient age (*age*) and stay duration (*dur_stay*). The domain of definition of the attribute *age* is the integer range $[0, 110]$ with a mean value of 49.5 and the one of the attribute *dur_stay* $[0, 248]$ with a mean value of 3.9. Notice that both attributes have distinct β_i variances. For instance, in the case of $N_g = 3000$ groups and using eq.(12), we have $\sigma^2_{\beta_i} = 0.0456$ for the *age* attribute whereas it is $\sigma^2_{\beta_i} = 3.1188E - 5$ for *dur_stay*. For robustness experiments, the message we embed is a random sequence of two symbols '-1'/'+1' uniformly distributed. Furthermore, results are given in average after 30 random simulations with the same parameterization but with different tuples.

B. Capacity Results

In a first time, let us consider the attribute *age* (N occurrences) with a fixed number of groups $N_g = 3000$ and an attribute shift amplitude Δ varying in the range $[1, 5]$. We recall that the angle shift α of β_i depends on Δ (see eq. (6)). As it can be seen in Fig. 7, capacity increases along with Δ and verifies the theoretical limit we define in Section II-A. Obviously, one must also consider that the attribute distortion increases along with the capacity. In the case the whole attribute *age* set is watermarked, all values are modified of $\pm\Delta$, leading to a mean square error (MSE) of Δ^2. If there exist some overflow-groups of tuples then the MSE will be smaller.

In a second experiment, *age* and *dur_stay* were watermarked with $\Delta = 3$ and $\Delta = 1$ respectively while considering varying number of groups such as $N_g \in 500, 700, 1500, 3000$. Notice that the more important the number of groups, the smaller is the number of tuples per groups. As depicted in Fig. 8 for both attributes, obtained capacities fit the theoretical limit we establish in section III-A. Given results confirm that the capacity depends on the properties of the attributes considered for embedding and especially of its standard deviation (see section III-A). Indeed, we can insert more data within the attribute *dur_stay* which is of smaller variance.

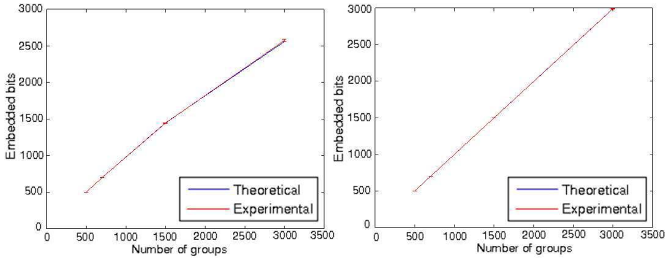


Fig. 8. Capacity results for each considered attribute. Left: *Age* attribute. Right: *dur_stay* attribute.

C. Robustness Results

Experimental and theoretical results are presented together in Tables I to III. These tables give the probabilities of error of symbol $\mathbb{P}_e$ (Table I), of carrier loss $\mathbb{P}_l$ (Table II) and of carrier injection $\mathbb{P}_i$ (Table III) considering two attacks, tuples insertion and removal, of various extent. More clearly, considering a database of $N = 10^6$ tuples, between 10% to 50% of tuples were removed or added. Indicated experimental results are given in average accompanied with their standard deviation.

Regarding the probability or error of symbol $\mathbb{P}_e$, it can be seen from Table I, that experimental results are very closed to the theoretical ones we established in Section II-A whatever the attribute and the attack. This is also the same for $\mathbb{P}_l$, the probability of carrier loss, in the case of the tuple deletion attack (see Table II). However if we look at the injection attack, obtained results for $\mathbb{P}_l$ are slightly different. This may be explained by the fact that, for small number of injected tuples, experiments do not verify the central limit theorem, an hypothesis we made in section III-B when establishing $\mathbb{P}_l$. However, when the number of added tuples per group increases, experimental results tend to fit theoretical ones whatever the attack and attribute. If now we look at the carrier injection probability (or equivalently of symbol injection), $\mathbb{P}_i$, experimental results are again very close to the theory.

From a more general point of view, whatever the attack $\mathbb{P}_l$, $\mathbb{P}_e$ and $\mathbb{P}_i$ increase along with the number of groups as well as with the standard deviation of the attribute. One can also remark that in the case of the insertion attack, $\mathbb{P}_l$ and $\mathbb{P}_i$ decrease and increase respectively when the number of injected tuples rises up. Nevertheless, from all the above comments, it appears that once the statistical properties of the attribute we want to watermark are known, we are able to estimate the performance of our scheme in terms of capacity and also in terms of robustness for a given attack extent.

V. Comparison With Recent Robust Lossless Watermarking Methods

Herein, we compare our approach with [15] and [16], two recent and efficient robust lossless methods, in terms of distortion, robustness and complexity. For fair comparison,

TABLE I

Number of Symbol Errors (i.e., $\mathbb{P}_e \cdot C_T$) for Both Attributes *Age* and *Dur_Stay*. The Table Contains Theoretical (*Th.*) and Experimental Results, the Latter Are Given in Average (*Avg.*) Along With Their Corresponding Standard Deviation (*Std*) for Different Size of Group and After 30 Simulations. The Database Contains $N = 1048575$ Tuples

		Symbol Errors											
	Attack	Attribute *age* with $\Delta = 3$											
		Nb. groups											
		500			700			1500			3000		
		Th.	Avg.	std	Th.	Avg.	std	Th.	Avg.	std	Th.	Avg.	std
Deletion	$N_d = 10\%N$	0.1074	0.0667	0.2537	0.7052	0.6000	0.9322	13.5118	14.0333	3.056	70.9538	71.6000	9.3314
	$N_d = 20\%N$	0.2724	0.3000	0.5350	1.5739	1.4333	1.0063	24.9977	25.9000	5.5606	119.3641	118.6000	10.5947
	$N_d = 30\%N$	0.5870	0.3667	0.7184	2.9635	3.0000	1.9827	38.9857	38.9000	6.4077	170.2662	165.3000	11.3385
	$N_d = 50\%N$	2.4157	2.4667	1.5025	9.0949	8.7667	2.9441	80.2505	82.7333	6.4001	292.8295	291.6000	13.2836
Insertion	$N_i = 10\%N$	0.1458	0.0667	0.2537	1.0809	0.7000	0.8367	19.4604	13.8333	3.3330	84.2269	64.7667	7.2668
	$N_i = 20\%N$	0.2432	0.2000	0.4068	1.6012	1.0667	1.0483	25.5356	22.9667	4.7596	110.9885	99.3667	9.8628
	$N_i = 30\%N$	0.3770	0.3333	0.5467	2.2404	1.7333	1.5071	32.0431	29.9333	6.0168	137.6633	129.5333	8.3655
	$N_i = 50\%N$	0.7679	0.5667	0.8172	3.8630	3.9000	1.7489	45.8714	47.5000	8.4761	188.8682	186.4667	13.8009
	Attack	Attribute *dur_stay* with $\Delta = 1$											
Deletion	$N_d = 10\%N$	0	0	0	0	0	0	0.0197	0.0333	0.1826	3.0148	3.9667	1.7905
	$N_d = 20\%N$	0	0	0	0	0	0	0.0636	0.1333	0.3457	6.7667	8.4333	3.8118
	$N_d = 30\%N$	0	0	0	0	0	0	0.1771	0.1667	0.3790	12.7618	14.3333	3.7539
	$N_d = 50\%N$	0	0	0	0.0021	0	0	1.2637	1.7667	1.4547	39.1717	42.6333	5.7445
Insertion	$N_i = 10\%N$	0	0	0	0	0	0	0.0251	0	0	4.8504	3.4667	1.9605
	$N_i = 20\%N$	0	0	0	0	0	0	0.0518	0.0333	0.1826	7.1523	5.5000	2.5563
	$N_i = 30\%N$	0	0	0	0	0	0	0.0962	0.1333	0.3457	9.9673	9.7000	3.1200
	$N_i = 50\%N$	0	0	0	0.0001	0	0	0.2624	0.2667	0.5208	17.0723	16.7667	4.3286

TABLE II

Number of Lost Carriers (i.e., $\mathbb{P}_l \cdot C_T$) for Both Attributes *Age* and *Dur_Stay*. The Table Contains Theoretical (*Th.*) and Experimental Results, the Latter Are Given in Average (*Avg.*) Along With Their Corresponding Standard Deviation (*Std*) for Different Size of Group and After 30 Simulations. The Database Contains $N = 1048575$ Tuples

		Lost Carriers											
	Attack	Attribute *age* with $\Delta = 3$											
		Nb. groups											
		500			700			1500			3000		
		Th.	Avg.	std	Th.	Avg.	std	Th.	Avg.	std	Th.	Avg.	std
Deletion	$N_d = 10\%N$	0.1075	0	0	0.7061	0.8000	0.7611	13.5237	15.4000	3.4998	70.9954	71.8667	7.2812
	$N_d = 20\%N$	0.2727	0.1333	0.3457	1.5755	1.4000	1.1017	25.0130	25.2667	4.9684	119.4118	117.3333	10.6491
	$N_d = 30\%N$	0.5876	0.4667	0.6814	2.9659	3.0000	1.9298	39.0044	39.1333	6.1293	170.3189	170.1333	9.1189
	$N_d = 50\%N$	2.4175	1.9333	1.1725	9.1001	10.1333	3.4614	80.2766	82.6667	9.5424	293.2363	290.5000	16.0490
Insertion	$N_i = 10\%N$	0.0106	0	0	0.1496	0	0	6.0895	1.4667	1.2521	36.4724	16.3000	4.6174
	$N_i = 20\%N$	0.0013	0	0	0.0315	0	0	2.6339	0.5000	0.8200	23.0069	12.0667	3.0618
	$N_i = 30\%N$	0.0002	0	0	0.0064	0	0	1.1334	0.2333	0.5040	14.6099	7.2667	2.8999
	$N_i = 50\%N$	0	0	0	0.0002	0	0	0.2078	0.0333	0.1826	5.9800	3.1333	1.6554
	Attack	Attribute *dur_stay* with $\Delta = 1$											
Deletion	$N_d = 10\%N$	0	0	0	0	0	0	0.0232	0.0667	0.2537	3.3431	4.1333	2.2242
	$N_d = 20\%N$	0	0	0	0	0	0	0.0723	0.1333	0.3457	7.2946	7.7333	3.0954
	$N_d = 30\%N$	0	0	0	0.0001	0	0	0.1973	0.3000	0.6513	13.5643	14.7000	3.4256
	$N_d = 50\%N$	0	0	0	0.0025	0	0	1.3674	1.7333	1.5071	40.8842	44.5333	7.0257
Insertion	$N_i = 10\%N$	0	0	0	0	0	0	0.0007	0	0	0.7490	0.1333	0.3457
	$N_i = 20\%N$	0	0	0	0	0	0	0	0	0	0.1624	0	0
	$N_i = 30\%N$	0	0	0	0	0	0	0	0	0	0.0340	0	0
	$N_i = 50\%N$	0	0	0	0	0	0	0	0	0	0.0014	0	0

we have considered their experimental framework in which tuples with real-valued numerical attributes are randomly generated. However, for question of simplicity, only one attribute was considered for embedding. At the same time, [15] and [16] were slightly modified, without changing intrinsically the strategy they follow, so as to adapt them to a correlation based watermark detection like our robust scheme does while considering a watermark S_1 of 64 bit long (see Sect. II-B).

TABLE III

Number of Injected Carriers (i.e., $\mathbb{P}_i \cdot (N_g - C_T)$) for Both Attributes *Age* and *Dur_Stay*. The Table Contains Theoretical (*Th.*) and Experimental Results, the Latter Are Given in Average (*Avg.*) Along With Their Corresponding Standard Deviation (*Std*) for Different Size of Group and After 30 Simulations. The Database Contains $N = 1048575$ Tuples

		Injected Carriers $\mathbb{P}_i$											
	Attack	Attribute *age* with $\Delta = 3$											
		Nb. groups											
		500			700			1500			3000		
		Th.	Avg.	std	Th.	Avg.	std	Th.	Avg.	std	Th.	Avg.	std
Deletion	$N_d = 10\%N$	0.0491	0.0333	0	0.4073	0.5333	0.7611	11.7440	12.5333	3.4998	79.8401	78.9667	7.2812
	$N_d = 20\%N$	0.0590	0.0667	0.3457	0.4974	0.7000	1.1017	14.8796	16.4000	4.9684	104.2907	103.0667	10.6491
	$N_d = 30\%N$	0.0649	0.0333	0.6814	0.5525	0.7333	1.9298	16.9244	17.7667	6.1293	121.1165	119.7333	9.1189
	$N_d = 50\%N$	0.0725	0	1.1725	0.6252	0.9667	3.4614	19.7847	20.5000	9.5424	145.8862	141.0000	16.0490
Insertion	$N_i = 10\%N$	0.1429	0.3333	0.5467	1.1838	0.9667	0.9643	28.2523	31.4333	6.3933	161.8367	172.4667	13.9846
	$N_i = 20\%N$	0.1621	0.3000	0.4661	1.4665	1.3667	1.1885	41.7108	45.1333	6.9219	252.4141	258.1333	10.6179
	$N_i = 30\%N$	0.1638	0.3333	0.5467	1.5179	1.4000	1.1626	48.0390	50.2333	7.2048	316.9128	313.1667	15.8921
	$N_i = 50\%N$	0.1640	0.3333	0.5467	1.5278	1.4000	1.1626	51.9391	54.7000	7.0572	388.6094	376.0667	16.0085
	Attack	Attribute *dur_stay* with $\Delta = 1$											
Deletion	$N_d = 10\%N$	0	0	0	0	0	0	0.0061	0	0	1.7001	1.7333	1.2847
	$N_d = 20\%N$	0	0	0	0	0	0	0.0073	0	0	2.1196	2.7333	1.5960
	$N_d = 30\%N$	0	0	0	0	0	0	0.0081	0	0	2.3764	2.8667	1.6761
	$N_d = 50\%N$	0	0	0	0	0	0	0.0090	0	0	2.7163	3.7000	2.1197
Insertion	$N_i = 10\%N$	0	0	0	0	0	0	0.0210	0.0333	0.1826	5.3529	6.7333	2.4202
	$N_i = 20\%N$	0	0	0	0	0	0	0.0221	0.0333	0.1826	6.7545	7.8333	2.7926
	$N_i = 30\%N$	0	0	0	0	0	0	0.0222	0.0333	0.1826	7.0229	8.3667	2.5255
	$N_i = 50\%N$	0	0	0	0	0	0	0.0222	0.0333	0.1826	7.0774	8.5667	2.6088

Let us consider the method of Gupta and Pieprzyk [15]. It works at the tuple level and not on groups of tuples. In order to make their scheme secure, one out of γ tuples are secretly watermarked. This methods replaces one of the LSBs of the integer part of one attribute $t_u.A_n$ by a secretly pseudo-random generated bit. The original bit is inserted into the fractional part of $t_u.A_n$ by means of reversible difference expansion modulation [18]. In order to adapt this scheme, instead of inserting a random sequence of bits, we embed a 64 bit long watermark and repeat it as long as tuples are available. A majority vote mechanism is used to extract the watermark which is then compared with the original one by means of correlation.

We implemented the method of Farfoura *et al* with no modifications. Like [15], it works at the tuple level. To sum it up roughly, considering one attribute value $t_u.A_n$, this method computes the difference between the fractional part of $t_u.A_n$ with a value derived from the hash of its primary key $t_u.P_k$. Then, one bit of the message is concatenated to the binary representation of this difference (expanding it). The result is then converted into an integer value used as watermarked fractional part. In this scheme, the watermark bits are repeated as long as tuples are available and its detection is done by correlation, as in the extension of [15] we proposed. One possible disadvantage of [16] is that it introduces new values in the attribute domain. More clearly, if the fractional part of an attribute is encoded on a fixed number of p bits, then its values will belong to the range $[0, \frac{1}{2^p}]$. By expanding the difference, we have no guarantee the resulting values belong to the attribute domain. This is the case for example for an attribute "number of weeks" measured with a daily precision, its fractional part varies in discrete multiples of $\frac{1}{7}$ (encoded on $p = 3$ bits). Furthermore, adding new attribute values can be easily identified. [16] does not specify how to deal with such a situation.

In our experiments, 80000 tuples of one attribute with values following a normal distribution of mean 135 and standard deviation 28.787 were generated. As in the previous section, results are given in average after 30 random simulations. Both [15] and [16] were parameterized with $\gamma = 7$, i.e. one out of seven tuples is watermarked, while our scheme makes use of all tuples with a shift amplitude $\Delta = 2$. This parametrization was chosen so as to enure a similar distortion for all algorithms; distortion we evaluate through the variations of the attribute's mean and variance after the insertion process like in [15] and [16]. Distortion results are given in Table IV. It can be seen that these three methods provide closed performance and tend to preserve the attribute's mean and variance.

By next, with the same parameterization, three attacks were considered in order to evaluate algorithms' robustness: insertion and suppression of tuples and attribute modification. Insertion and suppression attacks were performed with a percentage of suppressed/added tuples in the range $12.5\% - 87.5\%$. Attribute modification was conducted in two different manners: i) Gaussian noise addition; ii) rounding operation. As depicted in Fig. 9, the three methods have a similar behavior under a tuple insertion attack. They perform well even when the percentage of new tuples is near 90%. In the case of a tuple deletion attack, our method performs worse under strong attack conditions, i.e. when more than

TABLE IV
INTRODUCED DISTORTION BY COMPARED METHODS IN TERMS OF THE MEAN AND THE VARIANCE

Method	Mean		Variance	
	Original	Modified	Original	Modified
Farfoura *et al.* [16]	134.9844	134.9969	828.966	829.3225
Gupta and Pieprzyk [15]	134.9838	134.9842	828.059	831.8388
Proposed Method	135.0079	135.0048	828.592	832.5181

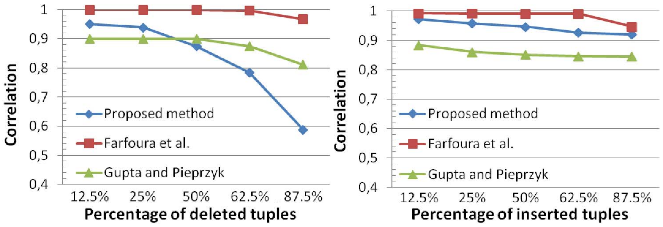


Fig. 9. Methods' Correlation values in the case of the tuple deletion attack (Left) and the tuple insertion attack (Right) with various intensities.

50% of tuples are removed. Nevertheless, it provides better performance than [15] for smaller percentage of tuple removal.

The first attribute modification attack we applied consists in adding a centered Gaussian noise of standard deviation $\sigma = 0.1$ to all watermarked tuples. Herein, our method performs quite well with correlation values greater than 0.97, compared to [15] which gets values above 0.87. On its side, [16] did not achieve a correlation greater than 0.53. Under the rounding attack, where values are rounded to the nearest integer, the method of [16] is inefficient due to the fact it embeds data into the attribute fractional part. That is not case of our scheme and of the one of Gupta and Pieprzyk [15]. They show similar behaviors with correlation values greater than 0.96.

Computation time is used so as to evaluate the complexity of these approaches. [15] and [16] show similar performance with an embedding/detection process conducted in about 60s. This is quite normal due to the fact they follow a similar strategy. Our method is nearly twice slower. The reason may stand in the histogram calculation for each sub-group of tuples.

To sum up, our approach provides better robustness performance than the scheme of Gupta and Pieprzyk [15] (except for strong deletion attacks), but it is twice slower. The method of Farfoura *et al.* better resists to tuple addition and removal but not to attribute modification attacks. It also introduces new values in the attribute domain. This may limit its application. That is not the case of our scheme and of the method of Gupta and Pieprzyk [15].

VI. CONCLUSION

In this paper, we have proposed a robust lossless relational database watermarking scheme which makes use of circular histogram modulation. It can be used for verifying the integrity of the database and also for verifying its authenticity even if the database has been modified. In addition, we have theoretically established and verified experimentally the performance of our method in terms of capacity and robustness against two common attacks: tuple deletion and tuple insertion. The proposed results allow the user to correctly select our scheme parameters under constraints of capacity, robustness and also distortion. We also have shown the performance gain our scheme can provide, as well as its disadvantages, compared with two recent and efficient schemes.

APPENDIX A
TRUNCATED NORMAL DISTRIBUTION

The p.d.f of a normally distributed random variable whose values are bounded can be represented by a truncated normal distribution. Let us consider $\gamma \sim \mathcal{N}(\mu,\sigma)$ which lies in the interval $\gamma \in [a,b]$, the truncated density function is:

$$f(\gamma;\mu,\sigma,a,b) = \begin{cases} \dfrac{\frac{1}{\sigma}\phi\left(\frac{\gamma-\mu}{\sigma}\right)}{\Phi\left(\frac{b-\mu}{\sigma}\right)-\Phi\left(\frac{a-\mu}{\sigma}\right)}, & \text{if } a \leq \gamma \leq b \\ 0, & \text{elsewhere} \end{cases}$$

The moments of this distribution are given by [26]:

$$\mathrm{E}[\gamma \mid a < \gamma < b] = \mu + \frac{\phi\left(\frac{a-\mu}{\sigma}\right) - \phi\left(\frac{b-\mu}{\sigma}\right)}{\Phi\left(\frac{b-\mu}{\sigma}\right) - \Phi\left(\frac{a-\mu}{\sigma}\right)}\sigma$$

$$\sigma^2_{(\gamma \mid a<\gamma<b)} = \sigma^2 \left[1 + \frac{\frac{a-\mu}{\sigma}\phi\left(\frac{a-\mu}{\sigma}\right) - \frac{b-\mu}{\sigma}\phi\left(\frac{b-\mu}{\sigma}\right)}{\Phi\left(\frac{b-\mu}{\sigma}\right) - \Phi\left(\frac{a-\mu}{\sigma}\right)} - \left(\frac{\phi\left(\frac{a-\mu}{\sigma}\right) - \phi\left(\frac{b-\mu}{\sigma}\right)}{\Phi\left(\frac{b-\mu}{\sigma}\right) - \Phi\left(\frac{a-\mu}{\sigma}\right)} \right)^2 \right]$$

APPENDIX B
SUM OF A TRUNCATED NORMAL AND A CENTERED NORMAL VARIABLE

It has been demonstrated by Turban in [27] that:

Proposition 1: Let $O \sim \mathcal{N}(0,\sigma_O)$ and $P \sim \mathcal{TN}(\mu_P, \sigma_P, a, b)$ be a normal and a truncated normal independent random variables. Then, $Q = O + P$ is distributed according to the density:

$$f(q) = \lambda e^{\frac{-(q-\mu_P)^2}{2(\sigma_O^2+\sigma_P^2)}} \left[\Phi\left(\frac{q-b-\kappa}{\chi}\right) - \Phi\left(\frac{q-a-\kappa}{\chi}\right) \right]$$

where

- $\kappa = \frac{\sigma_O^2(q-\mu_P)}{\sigma_O^2+\sigma_P^2}$, $\chi^2 = \frac{\sigma_O^2\sigma_P^2}{\sigma_O^2+\sigma_P^2}$
- $\lambda = \frac{\sqrt{2\pi}\chi}{2\pi\sigma_O\sigma_P(\Phi(d)-\Phi(c))}$
- $c = \frac{\mu_P-a}{\sigma_P}$ and $d = \frac{\mu_P-b}{\sigma_P}$.

APPENDIX C
VARIANCE OF THE MEAN OF A MIXTURE OF TWO RANDOM VARIABLES

Let Q be a random variable resulting from the mixture of two random variables O and P such as $Q = \pi_1 O + \pi_2 P$, with π_1 and π_2 the mixture proportions. The mean value of Q is:

$$\mathrm{E}[Q] = \pi_1 \mathrm{E}[O] + \pi_2 \mathrm{E}[P]$$

The variance of $\mathrm{E}[Q]$ is given by:

$$\begin{aligned}\mathrm{var}(\mathrm{E}[Q]) &= \mathrm{E}[(\pi_1\,\mathrm{E}[O]+\pi_2\,\mathrm{E}[P])^2]-(\mathrm{E}[Q])^2\\ &= \pi_1^2\,\mathrm{E}[(\mathrm{E}[O])^2]+\pi_2^2\,\mathrm{E}[(\mathrm{E}[P])^2]\\ &\quad +2\pi_1\pi_2\,\mathrm{E}[O]\,\mathrm{E}[P]-(\mathrm{E}[Q])^2\\ &= \pi_1^2(\sigma_O^2+(\mathrm{E}[O])^2)+\pi_2^2(\sigma_P^2+(\mathrm{E}[P])^2)\\ &\quad +2\pi_1\pi_2\,\mathrm{E}[O]\,\mathrm{E}[P]-(\mathrm{E}[Q])^2\end{aligned}$$

REFERENCES

[1] M. McNickle. (2013, Apr. 17). *Top 10 Data Security Breaches in 2012* [Online]. Available: http://www.healthcarefinancenews.com/news/top-10-data-security-breaches-2012

[2] R. Agrawal and J. Kiernan, "Watermarking relational databases," in *Proc. 28th Int. Conf. VLDB*, Jul. 2002, pp. 155–166.

[3] R. Sion, M. Atallah, and S. Prabhakar, "Rights protection for relational data," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 12, pp. 1509–1525, Dec. 2004.

[4] D. Gross-AMBLARD, "Query-preserving watermarking of relational databases and XML documents," *ACM Trans. Database Syst.*, vol. 36, pp. 1–24, Mar. 2011.

[5] M. Shehab, E. Bertino, and A. Ghafoor, "Watermarking relational databases using optimization-based techniques," *IEEE Trans. Knowl. Data Eng.*, vol. 20, no. 1, pp. 116–129, Jan. 2008.

[6] Y. Li, V. Swarup, and S. Jajodia, "Fingerprinting relational databases: Schemes and specialties," *IEEE Trans. Dependable Secure Comput.*, vol. 2, no. 1, pp. 34–45, Jan./Mar. 2005.

[7] F. Guo, J. Wang, and D. Li, "Fingerprinting relational databases," in *Proc. ACM SAC*, 2006, pp. 487–492.

[8] Y. Li, H. Guo, and S. Jajodia, "Tamper detection and localization for categorical data using fragile watermarks," in *Proc. 4th ACM Workshop DRM*, Oct. 2004, pp. 73–82.

[9] I. Kamel and K. Kamel, "Toward protecting the integrity of relational databases," in *Proc. IEEE World Cong. Internet Sec.*, Feb. 2011, pp. 258–261.

[10] J. Guo, "Fragile watermarking scheme for tamper detection of relational database," in *Proc. CAMAN*, May 2011, pp. 1–4.

[11] J. Lafaye, D. Gross-Amblard, C. Constantin, and M. Guerrouani, "Watermill: An optimized fingerprinting system for databases under constraints," *IEEE Trans. Knowl. Data Eng.*, vol. 20, no. 4, pp. 532–546, Apr. 2008.

[12] S. Bhattacharya and A. Cortesi, "A distortion free watermark framework for relational databases," in *Proc. 4th Int. Conf. Softw. Data Technol.*, vol. 2. Dec. 2009, pp. 229–234.

[13] G. Coatrieux, E. Chazard, R. Beuscart, and C. Roux, "Lossless watermarking of categorical attributes for verifying medical data base integrity," in *Proc. IEEE Annu. Int. Conf. EMBS, EMBC*, Sep. 2011, pp. 8195–8198.

[14] Y. Zhang, X. Niu, and B. Yang, "Reversible watermarking for relational database authentication," *J. Comput.*, vol. 17, no. 2, pp. 59–66, Jul. 2006.

[15] G. Gupta and J. Pieprzyk, "Database relation watermarking resilient against secondary watermarking attacks," in *Proc. ICISS* (Lecture Notes in Computer Science), A. Prakash and I. Gupta, Eds. New York, NY, USA: Springer-Verlag, 2009, pp. 222–236.

[16] M. E. Farfoura, S.-J. Horng, J.-L. Lai, R.-S. Run, R.-J. Chen, and M. K. Khan, "A blind reversible method for watermarking relational databases based on a time-stamping protocol," *Expert Syst. Appl.*, vol. 39, no. 3, pp. 3185–3196, Feb. 2012.

[17] M. E. Farfoura, S.-J. Horng, and X. Wang, "A novel blind reversible method for watermarking relational databases," *J. Chin. Inst. Eng.*, vol. 36, no. 1, pp. 87–97, 2013.

[18] A. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Trans. Image Process.*, vol. 13, no. 8, pp. 1147–1156, Aug. 2004.

[19] C. De Vleeschouwer, J.-F. Delaigle, and B. Macq, "Circular interpretation of bijective transformations in lossless watermarking for media asset management," *IEEE Trans. Multimedia*, vol. 5, no. 1, pp. 97–105, Mar. 2003.

[20] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*, 2nd ed. San Mateo, CA, USA: Morgan Kaufmann, 2008.

[21] K. V. Mardia and P. E. Jupp, *Directional Statistics* (Probability and Statistics). Chichester, U.K.: Wiley, 1999.

[22] N. I. Fisher, *Statistical Analysis of Circular Data*. Cambridge, U.K.: Cambridge Univ. Press, 1993.

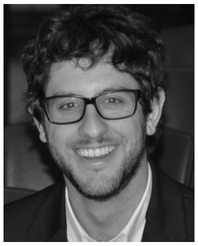
[23] N. I. Fisher and T. Lewis, "Estimating the common mean direction of several circular or spherical distributions with differing dispersions," *Biometrika*, vol. 70, no. 2, pp. 333–341, Aug. 1983.

[24] R. G. McKilliam, "Lattice theory, circular statistics and polynomial phase signals," Ph.D. dissertation, Inf. Comput. Sci., Univ. Queensland, Brisbane, Australia, Dec. 2010.

[25] M. Berenson, T. Krehbiel, and D. Levine, *Basic Business Statistics: Concepts and Applications*. Upper Saddle River, NJ, USA: Prentice-Hall, 2012.

[26] N. L. Johnson, S. Kotz, and N. Balakrishnan, *Continuous Univariate Distributions* (Probability and Statistics), vol. 1. Hoboken, NJ, USA: Wiley, May 1995.

[27] S. Turban. (2013, Apr. 17). *Convolution of a Truncated Normal and a Centered Normal Variable* [Online]. Available: http://www.columbia.edu/~st2511/notes.html



Javier Franco-Contreras (M'11) received the B.E. degree from Universidad de Valladolid and the M.Sc. degree from TELECOM Bretagne in 2011. Since 2011, he has been pursuing the Ph.D. degree with the Department of Information and Image Processing, TELECOM Bretagne and Laboratory of Medical Information Processing, INSERM U1101, Brest, France, focusing on medical database protection based on watermarking. His main areas of research interest are medical information security and watermarking.

Gouenou Coatrieux (M'06–SM'13) received the Ph.D. degree in signal processing and telecommunication from the University of Rennes I, Rennes, France, in collaboration with the Institute Mines-Telecom, Telecom Paris-Tech, Paris, France, in 2002, in the field of watermarking in medical imaging.

He is currently an Associate Professor with the Department of Information and Image Processing, Institute Mines-Telecom, Telecom Bretagne, Brest, France. He conducts his research in the Laboratory of Medical Information Processing, Institut National de la Santé et de la Recherche Médicale, Brest. His primary research interests concern medical information system security and medical data (images, databases, electronic patient records) protection by means of watermarking and encryption.

Dr. Coatrieux is an Associate Editor of the IEEE JOURNAL ON BIOMEDICAL AND HEALTH INFORMATICS, *Digital Signal Processing*, and *Innovation and Research in BioMedical Engineering*. He is a member of the International Federation for Medical and Biological Engineering "Global Citizen Safety and Security Working Group" and the European Federation for Medical Informatics "Security, Safety, and Ethics Working Group," and has contributed to the Technical Committee of "Information Technology for Health" of the IEEE Engineering in Medicine and Biology Society.

Fréderic Cuppens (M'11) is a Full Professor with TELECOM Bretagne of Institut Mines-Telecom and is co-responsible for SFIIS (security, reliability, and integrity of systems' information), one of the CNRS LabSTICC teams. He received the Engineering degree in computer science and the Ph.D. degree and the HDR (Habilitation to supervise research). He has been working for more than 20 years on various topics of computer security, including definition of formal models of security policies, access control to network and information systems, intrusion detection, reaction and countermeasures, and formal techniques to refine security policies and prove security properties. He has published more than 150 technical papers in refereed journals and conference proceedings. He served on several conference program committees as a member or General Chair. He was the Program Committee Chair of several conferences, including ESORICS 2000, IFIP SEC 2004, SAR-SSI 2006, SETOP 2008, CRISIS 2011, PST 2011, and DBSEC 2012.

Nora Cuppens-Boulahia (M'11) is an Associate Researcher with TELECOM Bretagne of Institut Mines-Telecom. She received the Engineering degree in computer science and the Ph.D. degree from ENSAE (National Higher School of Aeronautics and Space), and the HDR degree from University Rennes 1. Her research interests include formalization of security properties and policies, cryptographic protocol analysis, formal validation of security properties, and threat and reaction risk assessment. Her current research topics include *a posteriori* access and usage control and traceability, privacy preserving by query rewriting, data fragmentation, and security of web services. She has published more than 80 technical papers in refereed journals and conference proceedings. She has been a member of several international program committees in information security system domain and the Program Committee Chair of SETOP 2008, SETOP 2009, SAR-SSI 2009, CRiSIS 2010, DPM 2011, SECOTS 2012, DBSEC 2012, PST 2012, and the Co-General Chair of ESORICS 2009. She is the French representative of IFIP TC11 "Information Security" and she is co-responsible for the information system security axis of the French learned society SEE.

Christian Roux (F'05) received the Aggregation degree in physics from Ecole Normale Supérieure, Cachan, France, in 1978, and the Ph.D. degree from Institut National Polytechnique, Grenoble, France, in 1980. In 1982, he joined Institut Mines-Telecom, Telecom Bretagne, Brest, France, where he became an Associate Professor in 1987 and has been a Professor since 1987. He was a Visiting Professor with the Medical Image Processing Group, Department of Radiology, University of Pennsylvania, from 1992 to 1993, and a Distinguished International Research Fellow with the Department of Electrical Engineering, University of Calgary, Canada, in 1996 and 2003. He is the Founding Director of the Laboratoire de Traitement degree l'Information Médicale, INSERM U1101, Telecom Bretagne-Université de Bretagne Occidentale. His research interests concern advanced medical information processing, and spatial, temporal, and functional information modeling and analysis in medical images, with applications in various medical domains, including orthopedics, gastroenterology, ophthalmology, cardiology, and nuclear medicine. He has published over 160 papers and holds nine patents.

Dr. Roux was an Associate Editor of the IEEE TRANSACTIONS ON MEDICAL IMAGING from 1993 to 2000, is a member of the editorial board of the IEEE TRANSACTIONS ON INFORMATION TECHNOLOGY and the PROCEEDINGS OF THE IEEE, and a Chair of the GRETSI Program Committee. He served as the President of the IEEE Engineering in Medicine and Biology Society in 2001. He is the Founding Co-Chairman of the IEEE EMBS International Summer School, Berder Island, France. He received the IEEE EMBS Award in 2003 and the INSERM Award for basic research in 2006.