الخلاصة

اليوم ، اكثر فأكثر العلاقات لقاعدة البيانات ذات الاهمية العالية المستعملة بكثرة والموزعة عبر شبكة الانترنت. ومن هنا، اتت الحاجة الى الملكية لحماية المحتوى الثمين لقاعدة البيانات من النسخ المحظور واعادة التوزيع المحضورة في حالة بيعها او توزيعها الى الاشخاص الغير مؤتمنة.

العلامة المائية هي تقنية فعالة لحماية الحقوق الرقمية ،اخفاء العلامة المائية يتم عن طريق احداث تغير صغير الى المحتوى الاصلي لقاعدة البيانات بدون التأثير بشكل ملحوظ على استخدامها للغرض المقصود.

يوفر هذا المشروع تقنية العلامة المائية بشكل فعال لحماية البيانات العددية العلائقية المهمة والثمينة من النسخ واعادة التوزيع الغير شرعية لهذة البيانات بالاضافة الى ذلك لادعاء الملكية الخاصة ولايقاع التهمة على الخائن المشبوه.

يشمل المشروع ثلاثة مراحل رئسية وهي كالاتي :

المرحلة الاولى وهي اضافة العلامة المائية وطبع الاصابع الى قاعدة البيانات العلائقية التي تضمن بأن بعض مواقع البتات لبعض الحقول (الاعمدة) لبعض القيود (الاسطر) التي تحتوي على قيم معينة، بحيث يتم اختيار قيم القيود والحقول ضمن القيد والبت ضمن الحقل، جميعا تحدد خوارزميا تحت سيطرة مفاتيح سرية معروفه من قبل مالك البيانات فقط بلاضافة الى ذلك تحدد تحت سيطرة خوارزميات MAC(رمز تخويل الرسالة) والتي بدورها تعتمد خوارزمية SHA-1 القياسية ذات الاتجاة الواحد للحصول على 160 بت كقيمة لل Hash وكذلك بأستخدام مولد جف Geffe الذي يبنى من التجميع البسيط من ثلاثة مسجلات خطية LFSRs، بحيث توفر استخدام هذة التقنيات القوة والحماية للنظام.

أن نمط البت المحدد والذي تم اختياره بالصيغة اعلاه يتضمن قيمة العلامة المائية او قيمة طبع الاصابع اعتمادا على قيمة عامل السيطرة المحدد من قبل المالك ، الناتج من هذه المرحلة هي قاعدة بيانات علائقية تحتوي على العلامة المائية .

المرحلة الثانية هي كشف العلامة المائية وطبع الاصابع بنفس المفاتيح السرية التي استعملت في عملية اضافة العلامة المائية وطبع الاصابع الى قاعدة البيانات العلائقية، وكذلك باستخدام مستوى الاهمية(α) التي بدورها تحدد سلوكية النظام مع الاكتشافات الخاطئة .

PDF created with pdfFactory trial version www.pdffactory.com

اكتشاف العلامة المائية وطبعة الاصابع لايتطلبان الوصول الى البيانات الاصلية ولا الى العلامة المائية وطبع الاصابع، كلاهما يمكن ان يُكتشفوا حتى من مجموعة صغيرة لقاعدة البيانات المُعلمة لطالما العينة تحتوي على البعض من اجزاء العلامة المائية.

المرحلة الثالثة هي تحليل النظام المقترح وبين تحليلنا الى النظام بأن التقنية المقترحة تقاوم الاشكال المختلفة من الهجمات الخبيثة وكذلك ضد تحديث البيانات .

اخيرا ، النظام المقترح يوفر تقنية جديدة ناتجة من استخدام تقنيات العلامة المائية وتقنيات طبع الاصابع في نفس الوقت ، لتعريف حقوق الملكية والموزع الغير مشروع لقاعدة البيانات العلائقية .

PDF created with pdfFactory trial version www.pdffactory.com

Abstract

Today, more and more valuable database relations are widely used and distributed over the Internet. Thus, there is a need for the owner to protect valuable content from illicit copying and illegal redistributing when it's to be sold or distributed to potentially untrusted parties.

Watermarking is an effective technology for digital rights protection. A watermark is embedded by introducing small errors to the original content without affecting significantly the usability of it for the intended purpose.

This project provides the effective watermarking technique to protect valuable numeric relational data from illegal duplications and redistributions as well as to claim ownership and suspect traitor. The project consists of three phases, as follows:

The first stage is insertion of the watermark and fingerprint to the relational database that ensures that some bit positions of some of the attributes of some of the tuples contain specific values, the tuples, attributes within a tuple, bit positions in an attribute, and specific bit values are all algorithmically determined under the control of a private keys known only to the owner of the data, as well as by control of various MAC (Message Authenticated Code) functions that depending on the One-Way hash function standard SHA1 algorithms to produces 160 bit hash value , and by using the Geffe's Generator based on simple combination of three LFSR's ,using their techniques provides more robust and protection to the system. This bit pattern constitutes

PDF created with pdfFactory trial version www.pdffactory.com

the watermark or fingerprint value depending on the value of control parameter determined by owner only, the result of this stage is marked relational database.

The second stage is detection of the watermark and fingerprint by the same secret parameters that are used in the watermark and fingerprint insertion and by the significance level α that determines how amenable system is to false hits. Detecting the watermark and fingerprint neither requires access to the original data nor the watermark and fingerprint. Both of them can be detected even in a small subset of a watermarked relation as long as the sample contains some of the marks.

The third stage is the analysis of proposed system, our extensive analysis shows that the proposed technique is robust against various forms of malicious attacks and updates to the data.

Finally, the proposed system provides a new technique that uses watermarking and fingerprinting techniques in the same time to identify the ownership and the illegal distributor of the relational database.

PDF created with pdfFactory trial version www.pdffactory.com