Reversible Watermarking for Relational Database Authentication

Yong Zhang[1,2,*], Bian Yang[3], and Xia-Mu Niu[1,2,3]

[1] Shenzhen Graduate School at Harbin Institute of Technology
Shenzhen 518055, P.R. China
xiamu.niu@isec.hitsz.edu.cn

[2] Shenzhen Innovation International
Shenzhen 518057, P.R. China
zhangyong076@gmail.com, xiamu.niu@hit.edu.cn

[3] School of Computer Science and Technology at Harbin Institute of Technology
Harbin 150001, P.R.China
bian@ict.hit.edu.cn, xiamu.niu@hit.edu.cn

Received 5 May 2006; Revised 12 June 2006 ; Accepted 15 June 2006

Abstract. A reversible watermarking scheme for relational databases is proposed in this paper to achieve lossless and exact authentication of relational databases via expansion on data error histogram. This reversible watermarking scheme possesses the ability of perfect restoration of the original attribute data from the untampered watermarked relational databases, thus guaranteeing a "clear and exact" tampered-or-not authentication without worry about causing any permanent distortion to the database. In this scenario, only the secret key owner possesses the capability to exactly restore the database's original state. Simulations demonstrate the scheme's security and feasibility for low-correlated data in typical databases.

Keywords: reversible watermark, digital watermarking, relational databases

1 Introduction

Security is of increasing concern with databases for database's high added values and extensive installation in modern information systems. In addition to encryption, watermarking techniques is practically proven as another possible solution to enhance databases' content security especially for copyright protection [1-6] and data tampering detection [7]. Unlike encryption or hash description, typical watermarking techniques modify original data as a modulation of the watermark information, and inevitably cause permanent distortion to the original data, and therefore cannot meet the integrity requirement of the data in some applications. This underlying defect can be relieved by reversible watermarking techniques [8-22] by their reversibility in both robust watermarking [8,9] and fragile watermarking [10-18]. The direct beneficiary from this reversibility is those applications requiring zero permanent distortions such as medical imaging, military imaging, forensics of documents and art work authentication. On the other hand, the perfect restoring ability realizes watermarking based lossless authentication which accounts for the major part of earlier algorithms [8-11]. In recent years, researches on reversible watermarking center on increasing embedding capacity to meet requirements of large volume data embedding [12-18]. In the meanwhile, its applications reach to non-raster image fields [20-22]. However so far, almost all the reversible watermarking schemes exploit high correlation among neighboring data samples, and therefore face difficulty in the application of relational databases which usually contains only low-correlated, or even in the extreme case, completely random generated data.

Some schemes were proposed [1-6] to watermark relational databases for copyright protection, which are based on the facts that the relational data have enough redundancy and can tolerate some unnoticeable degradation in data precision caused by watermark embedding. The targets of the papers [1-6] are to verify the copyright of the relational data and the ownership of the owner, and the fragile watermarking scheme algorithm proposed in [7] is to detect and localize the tampered area of relational data, which however, inevitably introduces permanent distortion to the cover data.

* Correspondence author

Above relevant works all assume that minor distortions caused to some attribute data can be tolerated to some specified precision grade. However some applications in which relational data are involved cannot tolerate any permanent distortions and data's integrity needs to be authenticated. To meet this requirement, we propose a reversible watermarking technique for lossless authentication of relational databases. Considering the typical case of randomly generated data sequence with even distribution as the host data, the scheme takes advantage of the uneven distribution of the error of two even-distributed variables and gains embedding capacity from reversible histogram expansion [15,17,18]. The rest of the paper is organized as follows: section 2 analyzes the distribution of errors between randomly generated even-distributed data as a simulation of practical numerical attributes in a database; section 3 presents the proposed scheme of reversible watermarking for relational databases; section 4 presents analysis and simulations, and section 5 concludes the paper.

2 Distribution of Error of Two Even-Distributed Variables

Considering the low correlation between neighboring data of a typical database, we assume an extreme case – randomly generated real values – as the host media for reversible watermarking. Since so far most of reversible watermarking algorithms are based on high correlation among neighboring pixels, these algorithms are hard to embed a large capacity of watermark bits in the low-correlated or independent values in a typical database. In this paper, we investigate the distribution of error between two even-distributed variables and consider the possibility of reversibly watermarking these errors and their corresponding original data. Now we analyze the distribution of the error between two even-distributed variables as follows:

Assume X and Y are two independent variables with even distribution over $[a,b]$ ($a,b \in \mathrm{R}$ and $a<b$), and the probability density function of error Z=X-Y is

$$f_Z(z)=\begin{cases}\dfrac{z-a+b}{(b-a)^2}, & a-b\le z<0\\ \dfrac{b-a-z}{(b-a)^2}, & 0\le z<b-a\\ 0, & others\end{cases}. \qquad (1)$$

with the distribution shown in Fig.1.

From figure 1 it is obvious that the errors take on an uneven distribution centering near zero, reminding us of the histogram expansion technique [15] to exploit the uneven distribution for a reversible watermark embedding.

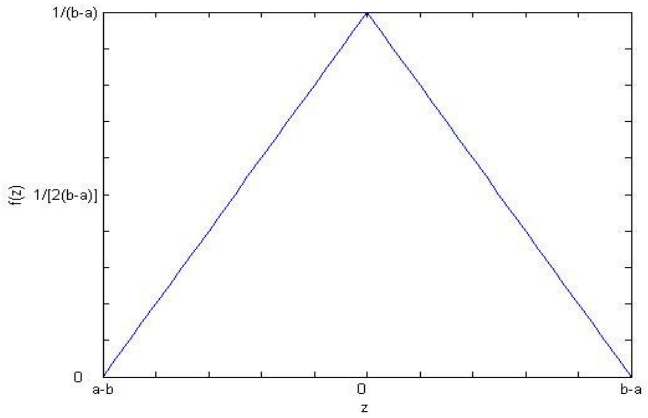

Fig. 1. PDF of error of two even-distributed variables *a* and *b*

3 The Proposed Scheme

Other than the case of histogram expansion used for images in the greyscale range [0,255], the real values have an uneven distribution over a variable range of $[a-b,b-a]$. To simplify the implementation of histogram expansion in this real value case, we extract just part of each original real value (called partial real value in the follows) instead of the whole one, and then retrieve the digits resident in the main value order of each error generated from two neighboring original real values to form the final histogram. Details are presented as follows.

3.1 Partial Error Generation

Let $D_{Ni}D_{(N-1)i}D_{(N-2)i}\ldots D_{Mi}{*}D_{(M-1)i}\ldots D_{2i}D_{1i}$ ($1 \le i \le L$, $N \ge M > 0$, L is the length of original real value sequence, N is the total digit number of a real value, and L,N,M are all positive integers) be an original real value sequence. We can choose D_{ji} as the initial digit to obtain a partial value $D_{ji}D_{(j-1)i}D_{(j-2)i}\ldots D_{Mi}{*}\ D_{(M-1)i}\ldots D_{2i}D_{1i}$ for partial error calculation:

$$d_i = d_{ji}d_{(j-1)i}d_{(j-2)i}\ldots d_{Mi}{*}\ d_{(M-1)i}\ldots d_{2i}d_{1i} = D_{j(i+1)}D_{(j-1)(i+1)}D_{(j-2)(i+1)}\ldots D_{M(i+1)}{*}D_{(M-1)(i+1)}\ldots D_{2(i+1)}D_{1(i+1)} - D_{ji}D_{(j-1)i}D_{(j-2)i}\ldots D_{Mi}{*}D_{(M-1)i}\ldots D_{2i}D_{1i} . \quad (2)$$

where $1 \le j \le N$ and '*' is a decimal point. Note that here practical applications' requirement in precision can be adjusted with j when performing the histogram expansion on all partial errors: the smaller is j, the smaller will be the watermarking distortion and in this way the watermark embedding distortion can be well controlled.

The capacity in the proposed scheme is gained from the partial errors between two neighbouring original partial values. Assume an arbitrary pair of neighbouring original partial values x_i, x_{i+1}(x_i<x_{i+1}), the errors can be calculated as

$$d_i = x_{i+1} - x_i . \quad (3)$$

Now find those errors with nonzero initial digits ($d_{ji} \neq 0$) and extract them to form a histogram. It is easy to see that d_{ji} are resident in the main value order of each error, i.e., errors with nonzero digits in the jth value order account for definitely major part of all errors (around 80% in experiments). In this way the variable range of [a-b,b-a] can be simplified to a fixed integer scale range from 1 to 9 which forms the final histogram bins, i.e., d_{ji} = 1,2,…,9. The histogram expansion technique can be then employed on these nonzero initial digits for reversibly embedding and leave those digits lower than j (from $d_{(j-1)i}$ to d_{1i}) unchanged. Let d_i' be the watermarked version of d_i, the difference between the two is limited to the initial digits d_{ji}, and therefore d_i' can be expressed as

$$d_i' = d_{ji}'d_{(j-1)i}d_{(j-2)i}\ldots d_{Mi}{*}d_{(M-1)i}\ldots d_{2i}d_{1i} . \quad (4)$$

where d_{ji}' is the watermarked version of d_{ji}, and '*' is a decimal point.

Now we consider using the inverse integer Haar wavelet tranform to derive watermarked database values x'_i and x'_{i+1} from the watermark information carrier d_{ji}'. Removing the decimal point from x_{i+1}, x_i and d' by multiplication with 10^{M-1} to obtain integers x^I_i, x^I_{i+1} and d^{I}'. Define the median value of x^I_i and x^I_{i+1}as

$$x^I_m = \lfloor (x^I_i + x^I_{i+1}) / 2 \rfloor . \quad (5)$$

Let d' be the watermarked version of d, the watermarked integers can be obtained by the inverse integer Haar wavelet:

$$x^{I'}_i = x^I_m - \lfloor d^{I}' / 2 \rfloor . \quad (6)$$

$$x^{I'}_{i+1} = x^I_m + \lfloor (d^{I}' + 1) / 2 \rfloor . \quad (7)$$

and after division by 10^{M-1} we can obtain the watermarked database partial values x'_i and x'_{i+1}.

It is obvious the original partial value pair x_i, x_{i+1} and their watermarked version x'_i and x'_{i+1} form a lossless transform by integer Haar wavelet. Based on this lossless transform, the watermark information can be losslessly embedded into the partial values of the cover data.

3.2 Expansion on Partial Error Histogram

The values contained in the database attributes for embedding are assumed to be even-distributed numerical data with specified data precision (controlled by selection of j for the initial digit D_{ji}) and our scheme embeds watermark on the errors' initial digits d_{ji}, whose distribution looks almost same as the uneven distribution in Fig.1. This is because the nonzero ones account for a major part of all d_{ji} and therefore watermarking on nonzero d_{ji} is equivalent to watermarking most of original partial values in the database.

The reversible watermark embedding process is illustrated in Fig.2 and described as follows:

Step 1: Set j of the initial digit D_{ji} according to the precision requirements of practical applications and extract all nonzero errors' initial digits d_{ji} to form a histogram $H(d_{ji})$ with bins from 1 to 9 representing d_{ji} = 1,2,…,9;

Step2: Use the histogram expansion techniques to reversibly watermark the selected nonzero errors' initial digits d_{ji}: find a bin P out of 1~8 with peak absolute amplitude (usually when d_{ji}=1 in this case) and right shift by 1 unit all amplitudes in bin range $\ge P$, i.e., to add 1 to all d_{ji} with absolute value $\ge P$. Now the original bin P has been emptied and watermark bits can be modulated into P and P+1 as illustrated in Fig.2 (detailed description in [15,17,18]). Note that in this case, only the initial digits d_{ji} have been modified and other digits unchanged. The

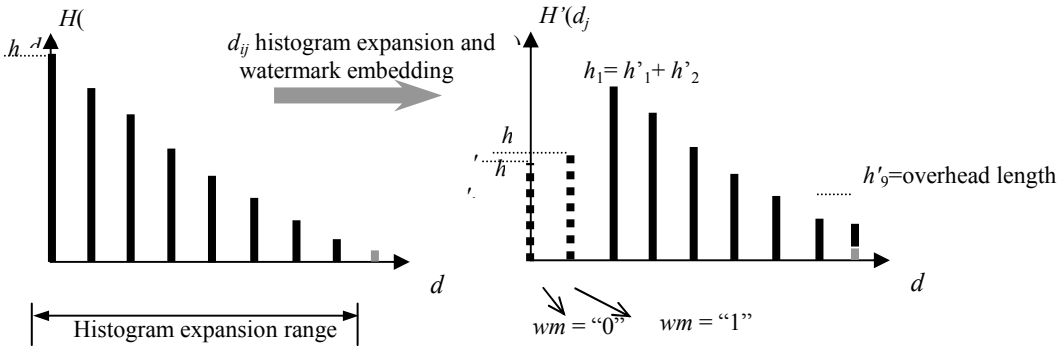

Fig. 2. Histogram expansion based reversible watermarking on the initial digits d_{ji}

total capacity provided by histogram expansion is h_1= h'_1+ h'_2 bits which is the total number of those errors with d_{ji} =1 in the case of Fig.2;

Step 3: Record the overhead information to distinguish the original digits d_{ji} =9 from those newly generated from the original d_{ji} =8. Obviously, it needs a binary sequence with a length of h'_9= h_8+ h_9 in the case of Fig.2 ("0" to tag those original ones and "1" the newly generated ones);

Step 4: Embed the watermark bits together with the overhead bits into the errors by histogram expansion described in Step3. Perform the inverse Haar wavelet transform and obtain the watermarked database attribute. It is easy to see the final capacity of this reversible watermarking scheme is around (h_1– h_8 – h_9) bits.

The watermark extraction is an inverse process of the above embedding process.

3.3 Over- / Underflow Prevention

Note that when an initial digit D_{ji} of the original partial value x_i equals 1 or 9, the inverse integer Haar wavelet over the watermarked errors may cause the resultant partial value x'_i and x'_{i+1} to over-and underflow, i.e., drive x'_i or $x'_{i+1} \geq 10^{j-M+1}$ or $\leq 10^{j-M}$ and thus fail to guarantee the perfect restoration of the watermark any more. In view of the fixed watermarking distortion of one unit on the initial digit d_{ji}, the maximum absolute distortion caused by watermarking is 10^{j-M} and the maximum absolute distortion caused to x'_i and x'_{i+1} is less than $0.5\times10^{j-M}+10^{-M+1}$. Thus we limit the watermarking range of partial value x_i and x_{i+1} to $[0.5\times10^{j-M}+10^{-M+1}, 10^{-}0.5\times10^{j-M}-10^{-M+1}]$ and distinguish the original partial values from the over-and-underflowed ones in $(0, 0.5\times10^{j-M}+10^{-M+1})$ and $(10^{-}0.5\times10^{j-M}-10^{-M+1}, 10)$ using overhead bits. Obviously, with the decrease of j, this overhead with length around $2\times(L^{-}1)\times10^{j-N-1}$bits (where L is the length of the original real value sequence and N is the total number of digits of an original real value) will also decrease to a very small number. Now we can give the final capacity estimation provided by our reversible watermarking scheme:

$$\text{Capacity} = h_1^{-} h_8^{-} h_9^{-} 2\times(L^{-}1)\times10^{j-N-1} . \qquad (8)$$

3.4 Relational Database Authentication

Fig.3 presents the framework for reversible relational database embedding and authentication, where K_1 is a cryptographic key used to sort the original real values by a preset rule and to select the appropriate real values for watermarking, and K_2 is a cryptographic key used to do watermark embedding and extraction. K_1 and K_2 are secret keys owned by the authorized person to authenticate the database. Note that there are two parts of overhead bits: (h_8+h_9) bits of discrimination information for original real values with initial digits of 8 and 9, and $2\times(L^{-}1)\times10^{j-N-1}$ bits of discrimination information for original real values prone to over- and underflow and those watermarked ones. MD5 or SHA functions can be employed to hash the original state of some specified parts or the whole database for authentication.

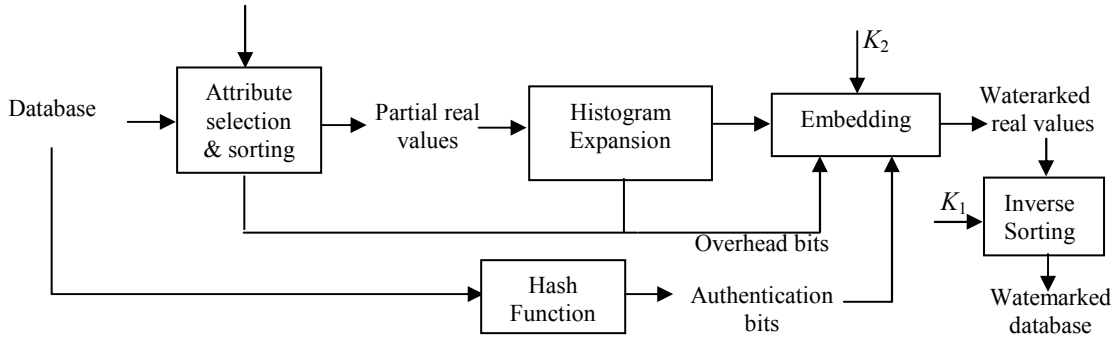

Fig. 3. (a) Histogram expansion based reversible watermarking on the initial digits d_{ji},

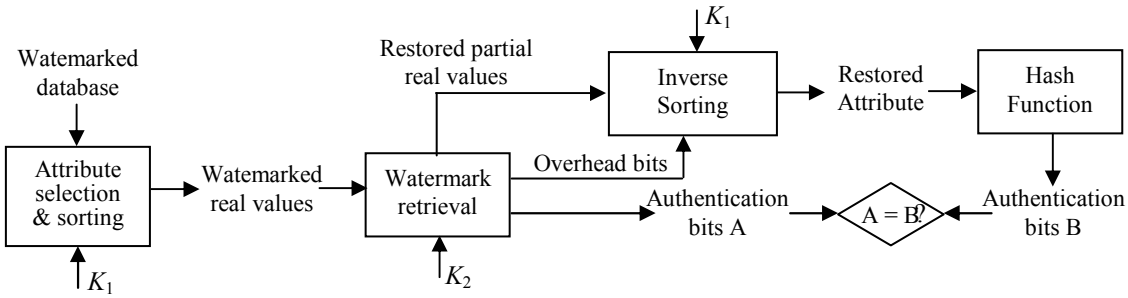

Fig. 3. (b) Watermarking framework: authentication

4 Algorithm Analysis and Simulations

Typically, authentication for database authentication usually needs 128 bits or higher in length, so the numerical data's length in the relational databases should be long enough to provide capacity for overhead bits plus the authentication bits. We generate a relational database containing several 10,001-sized attributes with different data formats, and we embed the authentication information into a attribute of 14-digit numeric data in floating-point format with even distribution over the value range [0,10000), so $L=10000$，N=14，M=11. The data are random generated by the function rand() from Matlab. In our simulations, the j of the errors' initial digit d_{ji} is set to be 13 and therefore the absolute watermarking distortion can be limited to 0.5×10^2. It is obvious that decreasing j can reduce the watermarking distortion to almost zero, but the capacity will not be affected if the data are rigidly even-distributed. Table 1 presents a simulation result of the distribution of error d_i generated from the original real values in the attribute whose watermarking range is limited in (50,9950) so as to avoid over- and underflows. In Table 1, the 9 columns denotes the 9 digits from 1 to 9, the 4 rows denotes 4 value orders on which absolute errors are distributed, and the figures in the main body show the quantity of absolute errors distributed in a certain value order with a certain initial digit. By Eq.(8) we can estimate the final capacity of the tested example shown in Table 1 as 516 bits, which is very close to the actual capacity of 503 bits in our simulation. This capacity should be large enough for authentication of part or even the whole of the database.

Table 1. Absolute errors distribution with original real values' watermarking range of (50,9950).

d_{13i}	1	2	3	4	5	6	7	8	9
10^0	1	2	0	2	1	3	2	1	0
10^1	6	14	13	11	15	6	13	10	8
10^2	103	96	85	110	89	81	98	104	79
10^3	898	719	657	551	416	343	228	138	43

From the scheme description in section 3 and the results in table 1, we can see that if RDB is not tampered, the watermark can be extracted, and the original RDB can be restored perfectly. Once RDB is tampered, the extracted watermark will not match the hash value calculated from the restored RDB, thus authenticating RDB as tampered.

5 Conclusions

The reversible watermarking scheme for relational databases proposed in this paper provides an exact and lossless method to authenticate the relational databases, especially suitable for sensitive data requiring no permanent distortions. The scheme takes advantage of the uneven distribution of errors between neighboring randomly generated values in the same attribute to realize reversibly watermarking, and show ability to limit the watermarking distortion to requirement of practical applications by taking partial real values to calculate errors using initial digit specification. Beside database, this scheme shows great advantage in reversible watermarking for other low-correlated data like encrypted data, images heavily polluted by noises, and noise data itself. Our future work focuses on finer temper localization schemes for relational databases, and more compact descriptions of overhead information.

6 Acknowledgement

This work was supported by the National Natural Science Foundation of China (Project Number: 60372052), the Science Foundation of Guangdong Province (Project Number: 05109511), the Foundation for the Author of National Excellent Doctoral Dissertation of China(Project Number: FANEDD-200238),the Multidiscipline Scientific Research Foundation of Harbin Institute of Technology (Project Number: HIT.MD-2002.11), the Scientific Research Foundation of Harbin Institute of Technology(Project Number: HIT.2003.52), the Foundation for the Excellent Youth of Heilongjiang Province, and the Program for New Century Excellent Talents in University.

References

[1] R.Agrawal, J.Kiernan, "Watermarking Relational Databases," in *Proceedings of 28th VLDB Conference*, Hong Kong, 2002, pp.155-166.

[2] R.Sion, M.Atallah, S.Prabhakarl, "Watermarking Relational Databases," *Technical Report. Indiana*, the Center for Education and Research in Information Assurance and Security of Purdue University, 2002.

[3] Z.H. Zhang, X.M. Jin, J.M. Wang, D.Y. Li, "Watermarking Relational Databases Using Image," in *Proceedings of IEEE Conf. on Machine Learning and Cybernetics*, Shanghai, P.R.China, 2004, pp.1739-1744.

[4] Y. Zhang, X.M. Niu, D.N. Zhao, "A Method of Protecting Relational Databases Copyright with Cloud Watermark," *International Journal of Information Technology*, Vol.1, No.4, 2004, pp.206-210.

[5] Y.Zhang, X.M. Niu, D.Wu, L.Zhao, J.C. Liang, W. J. Xu, "A Method of Verifying Relational Databases Ownership with Image Watermark," *The 6th International Symposium on Test and Measurement*, Dalian, P.R.China, 2005, pp.6316-6319.

[6] Y. Zhang, X. M. Niu, A. Khan, Q. Li, Q. Han, "A Novel Method of Watermarking Relational Databases Using Character String," in *Proceedings of the IASTED International Conference on Artificial Intelligence and Applications 2006*, Innsbruck, Austria, February 2006, pp.120-124

[7] Y.J. Li, H.P. Guo, S. Jajodia, "Tamper Detection and Localization for Categorical Data Using Fragile Watermarks," in *Proceedings of ACM Workshop on Digital Rights Management (DRM)*, October 2004, pp.73-82.

[8] C. W. Honsinger, P. Jones, M. Rabbani, J. C. Stoffel, "Lossless Recovery of an Original Image Containing Embedded Data," *US patent application*, Docket No: 77102/E/D, 1999.

[9] B. Macq, "Lossless Multiresolution Transform for Image Authenticating Watermarking," in *Proceedings of EUSIPCO*

2000, Tampere, Finland, September 2000.

[10] J. Fridrich, J. Goljan, R. Du, "Invertible Authentication," in *Proceedings of SPIE 2001, Security and Watermarking of Multimedia Content*, San Jose, CA, January 2001.

[11] J. Fridrich, M. Goljan, R. Du, "Lossless Data Embedding - New Paradigm in Digital Watermarking," *EURASIP Journal on Applied Signal Processing*, Vol.2, 2002, pp.185–196.

[12] J. Tian, "Wavelet-Based Reversible Watermarking for Authentication," in *Proceedings of SPIE Security and Watermarking of Multimedia Content IV*, Vol.4675, No.74, January 2002.

[13] T. Kalker, F. M. J. Willems, "Capacity Bounds and Constructions for Reversible Data Hiding," In *Proceedings of the 14th International Conference on Digital Signal Processing*, July 2002, No.1, pp.71-76.

[14] M. U. Celik, G. Sharma, A. M. Tekalp, E. Saber, "Reversible Data Hiding," In *Proceedings of International Conference on Image Processing*, Vol.2, September 2002, pp.157-160.

[15] Z.Ni, Y.Q.Shi, N.Ansari, W.Su, "Reversible Data Hiding," in *Proceedings of International Symposium on Circuits and Systems (ISCAS 2003)*, Bangkok, Thailand, May, 2003, Vol.2, pp.912-915.

[16] B.Yang, M.Schmucker, W.Funk, C.Busch, S.Sun, "Integer DCT-Based Reversible Watermarking for Images Using Companding Technique," in *Proceedings of SPIE, Security and Watermarking of Multimedia Content, Electronic Imaging*, San Jose, USA, January 2004, pp.405-415.

[17] B.Yang, M. Schmucker, X. Niu, C. Busch, S.Sun, "Reversible Image Watermarking by Histogram Modification for Integer DCT Coefficients," in *Proceedings of IEEE Multimedia Signal Processing Workshop*, Siena, Italy, September 2004, pp.143-146.

[18] B.Yang, M.Schmucker, X.Niu, C.Busch, S.Sun, "Approaching Optimal Value Expansion for Reversible Watermarking," in *Proceedings of ACM Multimedia and Security Workshop 2005*, New York, U.S.A., August 2005, pp.95-102.

[19] J. Dittmann, S. Katzenbeisser, C. Schallhart, H. Veith, "Provably Secure Authentication of Digital Media Through Invertible Watermarks," *IACR Cryptology ePrint Archive, Report 2004/293*, 2004.

[20] J. Dittmann, O. Benedens, "Invertible Authentication for 3d-Meshes," In *Proceedings of the SPIE*, *Security and Watermarking of Multimedia Contents V*, 2003, Vol.5020, pp.653-664.

[21] M.Voigt, B.Yang, C.Busch, "Reversible Watermarking of 2D-Vector Data," in *Proceedings of the 2004 ACM International Workshop on Multimedia and security*, Magdeburg, Germany, August 2004, pp.160-165.

[22] B.Yang, Z.Lu, S.Sun, "Reversible Watermarking in VQ-Compressed Domain," in *Proceedings of The Fifth IASTED International Conference on Visualization, Imaging, & Image Processing*, September 2005, pp.298-303.