http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 10 (5): 1001-1008, 2011
ISSN 1812-5638 / DOI: 10.3923/itj.2011.1001.1008

A Watermark for Authenticating the Integrity of Audio Aggregation Based on Vector Sharing Scheme

Juan Li, Rang-Ding Wang and Jie Zhu
CKC Software Laboratory, Ningbo University, Ningbo, Zhejiang 315211, China

Abstract: A method to authenticate the integrity of audio aggregation is proposed in this study. The vector-sharing scheme is used to fragile watermarking technology because it is very sensitive when recovering the secret. In this algorithm, the key sharing ideology is introduced into audio aggregation watermarking algorithm by separating the watermark in different audio works of the audio aggregation. When detected the original watermark can be recovered without original audio aggregation. The experimental results show that the proposed algorithm has strong vulnerability, good imperceptibility and can locate the audio work (s), which suffered attack in the audio aggregation.

Key words: Vector-sharing scheme, audio aggregation, fragile watermarking quantization index modulation

INTRODUCTION

With the rapid development of Internet technology, the audio information is vulnerable to be attacked or tampered during transmission. This may lead to serious consequences if the tampering involves important elements such as national security, court evidence and so on. Therefore, in recent years, how to protect the authenticity and integrity of audio information content effectively in the network environment has become a hot research spot in the multimedia information security field. Fragile watermarking as an effective means to solve this problem has become more and more important. However, certification of the integrity of the audio works essentially use a single audio as carrier, but audio works in the market mostly circulate in the form of aggregation such as audio album and there is correlation between each audio in the aggregation that means they have the same copyright information. Furthermore, pirates are more willing to work on the entire audio aggregation for commercial interests. Therefore, watermark technology that lets audio aggregation as carrier has a bright future (Xiong and Wang, 2009).

Copyright information can take audio aggregation as carrier like the single audio. There are differences and connections between the watermarking technology of taking audio aggregation as carrier and the traditional watermarking technology of taking single audio as carrier. The traditional technology can be applied to the audio aggregation watermarking technology indirectly, but the traditional audio watermarking technology does not consider the relationship of all the audio works in the audio aggregation that they have the same copyright. If using the traditional watermarking algorithm to protect the copyright or authenticate the integrity of audio aggregation, we must embed the whole watermark in every audio work of the audio aggregation respectively. When detected, we must extract from all the audio works. Therefore, embedding and extraction process should be carried out n times, n is the number of audio works in audio aggregation. Not only increases the algorithm's computational complexity, but also can't achieve the best balance between robustness and imperceptibility. During the study of audio aggregation watermarking technology, many factors must be considered. For example, how to embed a single watermark in the whole audio aggregation; how to extract the watermark from the audio aggregation and the detected audio aggregation would be suffered some different attacks and so on. The audio aggregation-watermarking algorithm is very different to the traditional watermarking algorithm by these factors (Wang and Xiong, 2010).

Zhang and Lv (2009) introduced the key sharing method is into audio watermarking algorithm by separating the watermark in different segments of the audio data so when detected, the original watermark can be gotten back by extracting only part of the watermark information. The algorithm uses the repetition coding technology to improve the robustness, while sacrifices the imperceptibility and this method is still a zero-watermarking technology based on a single audio for the carrier. Xiong and Wang (2010) introduced Shamir scheme into audio aggregation watermarking technology, but the algorithm increases the embedding capacity, has poor imperceptibility. What's more, when detected, the original audio aggregation needed.

Corresponding Author: Rang-Ding Wang, CKC Software Laboratory, Ningbo University, Ningbo, Zhejiang 315211, China

Some sub-keys based on the secret sharing scheme, while some audio works composes an audio aggregation can recover the main key. In view of the similarities between them and the sensitivity of recovering the secret, vector-sharing scheme will be applied to watermarking technology to authenticate the integrity of audio aggregation in this algorithm. The algorithm will generate n shares from the visible binary watermark by using vector-sharing scheme. The n shares will be embedded in the n audio works of audio aggregation respectively. The vulnerability of the algorithm will improve greatly if taking the coefficients of node, which has the lowest energy in wavelet packet domain as embedding position. Using Quantization Index Modulation (QIM) to complete the embedding process and the watermark can be extracted without the original audio aggregation. According to the experimental analysis, the proposed algorithm can authenticate the integrity of audio aggregation.

VECTOR SHARING SCHEME

Vector sharing scheme proposed by the Blakley (1979) and Schneier (1996) described it as follow. Secret will be defined as a point of m-dimensional space, any (m-1)-dimensional hyperplanes equation which contains the point represents a share. Therefore, arbitrary m hyperplanes determine this point exactly. The total number n of shares is the total number of hyperplane equations.

As long as get t hyperplanes, the secret can be recovered. Since any (m-1)-dimensional hyperplane can be expressed by m linear equations, so the vector-sharing scheme can be defined as follow:

Definition: (m, n)-vector sharing scheme which on the ring R is a triple (N, β, A), where N is the set of m-element vector which is represented by the column vector on the ring R^{β}, is the set of n-element vector which is represented by the column vector on the ring $R^{m\leq n}$. The matrix A on the ring R has n rows, m columns that must meet the following requirements:

- The matrix composed by m rows that select from the matrix A randomly is reversible
- An arbitrary sharing vector, which can be decomposed into n shares according to the equation, where every element of B is one share

Theorem: (m, n)-vector sharing scheme which on the ring R (m, n) is -threshold scheme. That means the secret can be recovered if t (m≤t≤n) shares are got.

Proof: Each share generated by the (m, n)-vector-sharing scheme which on the ring R corresponds to a m-linear equation. Coefficients of the linear equation is a row of matrix A. Obtaining t (m≤t≤n) shares means getting t m-linear equations. According to the requirement (1) of the definition, the linear equations is solvable when select m m-linear equations randomly, then obtain the secret (Yao *et al*., 2003).

ALGORITHM THEORY

Digital watermarking distribution based on vector sharing scheme: Suppose the audio aggregation is composed by n audio works, to make the digital watermark only can be recovered on the whole audio aggregation, which means each audio work in audio aggregation contains watermark information. Distributes the visible binary watermark into n shares by vector sharing scheme, then embeds each share in the n audio works in the aggregation. So when detected, the original watermark can be gotten back by extracting only m (m≤n) audio works theoretically. But, the purpose of this study is to authenticate the integrity of the audio aggregation, so take m = n in the algorithm which can not only avoid leaking situation effectively, but also improve the vulnerability of the algorithm greatly (Xiong and Wang, 2010).

Assuming the binary image W (i, j) ($0\leq i\leq L_1$, $0\leq j\leq L_2$) as the watermark of audio aggregation, the watermark distribution based on vector sharing scheme is shown in Fig. 1.

According to the Fig. 1, the specific steps of watermarking distribution are shown as following:

- Dimension Reduction. Because the audio signal is one-dimensional and watermark image W (i, j) two-dimensional. Therefore the watermark image should be reduced into one-dimensional signal V (k) (k = I×L1 + j)
- In practical, the capacity of watermark embedding is large and the watermark is binary sequences in general. To recover the shared secret correctly, the watermark sequence should be divided into segments firstly to ensure the elements of vector X must be within the ring Z_p (Jacobson, 1984).The binary sequence of the segments should convert to decimals, the converted decimal H must be within the [0-(p-1)], assuming $H = 2^q$, so take every n×q bits as a segment, denoted as f = n×q. Therefore V (k)can be divided into $s = \lfloor (L_1\times L_2) | f \rfloor$ segments. Denoted as V (k) = $\{v_1, (y), ..., v_s (y)\}$, 0≤y≤f-1
- Every q bits of v_i will be converted into a decimal number, then we will get sequence h_i (r) composed by these decimal numbers, 0≤r≤n-1. Therefore, obtain $X_i = [h_i (r)]^T = [h_i (0), ..., h_i (n-1)]^T$

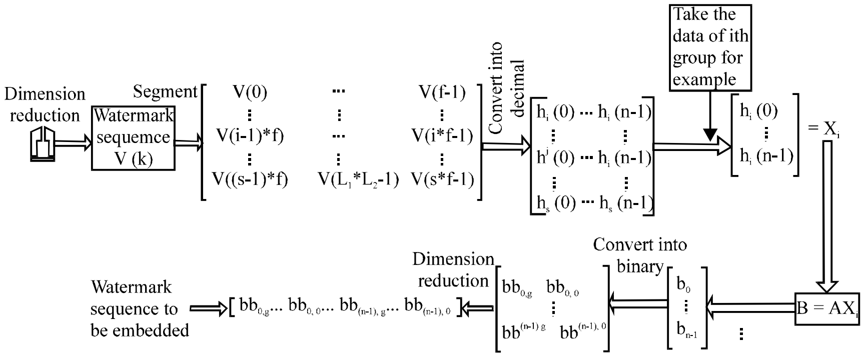


Fig. 1: Digital watermarking distribution based on vector sharing scheme

- $B = [b_0, b_1, ..., b_{n-1}]^T$ can be gotten by the equation $B = Ax_i$, where the matrix A has n rows and m columns $b_0, b_1, ..., b_{n-1}$ are the shares of watermark information
- Convert $b_0, b_1, ..., b_{n-1}$ into their binary form, respectively $b_I = bb_{i-g}...bb_{i,0}$ (I = 0, 1, ...n-1, bb_{i}, $j \in \{0, 1\}$, j = 0 , ..., g), obtain the binary watermark sequence to be embedded bb from it, $bb = \{bb_{0,g}...bb_{0,0}...bb_{i,g}...bb_{i,0}...\}$
- Repeat (3)~(5) steps for all data of each segment in $V(k) = \{v_i (y), ..., v_i (y), ..., v_s) (y)\}$

Select the position of watermark embedding: Wavelet packet analysis method is the promotion of multi-resolution wavelet analysis, which can describe high-frequency part of signal more carefully. It not only greatly expands the space for embedding information, but also can select the optimal basis adaptively. Eight sub-bands, i.e., 8 nodes, will be gotten when the audio signals are put into 3 level wavelet packet decomposition. The position of watermark embedding is selected based on the energy relationship between two sub-bands. Select various styles of audio signals: blues, classical, country, folk, pop, for carrying out a large number of experiments. The experiment shows that each style of audio signal has a same regular pattern: The energy of wavelet packet nodes is lower, it will be more sensitive to various common signal-processing operations. Limited to the length of the paper, take blues style music for example to illustrate the process of selecting embedding position which is shown as following. In Fig. 2a and b (Horizontal axis shows the nodes, vertical axis shows the corresponding energy and shows 8 sub-bands generated by the blues style music is put into 3 level wavelet packet decomposition and the energy distribution of each corresponding sub-bands. It can be seen from the experimental results in the figure, the largest energy is node (3, 0), the minimum energy is node (3, 4). Consider the number of node coefficients is large, we select 100 coefficients of node (3, 0) and node (3, 4) to show in Fig. 3. So in Fig. 3, the horizontal axis represents the 100 coefficients, the vertical axis shows the corresponding energy. Figure 3a and b shows the changes of the coefficients of node (3, 0) and node (3, 4) after they have been attacked such as re-quantization, re-sampling, adding noise, MP3 compression and so on. According to Fig. 3, the change of node (3, 4) coefficient is more obvious than node (3, 0) coefficient after they are attacked for the energy of node (3, 4) coefficient is lower which proves the node coefficients of lower energy are sensitive to common signal processing. Since the purpose of this study is to realize audio aggregation certification using the nature of fragile watermark and combined with the nature of fragile watermark, we selected the node coefficient of the lowest energy from corresponding audio works to embed.

Watermark embedding: A typical quantization index modulation technology, Dither Modulation (DM) (Solanki *et al*., 2005; Shterev and Lagendijk, 2006; Hogan *et al*., 2006) was applied in this study.

Suppose that the watermark information is a binary sequence that contains N bits, which means $m \in \{0, 1\}$. According to DM's embedding function (Eq. 1):

$$s (x; m) = q [x+d (m)]-d (m) \quad (1)$$

The formula for embedding binary watermark can be gotten:

$$S (k) = q_\Delta (x (k) + d [k, m_k])-d, m_k] \quad (2)$$

where, x (k) is k-th data in carrier for embedding watermark information. $m_k \in \{0, 1\}$. Corresponds to watermark information. d [k, m_k] is jitter, $q_\Delta(.)$ is the quantization function with step size Δ which can be define as:

$$q_\Delta (x) = round (x/\Delta) \Delta \quad (3)$$

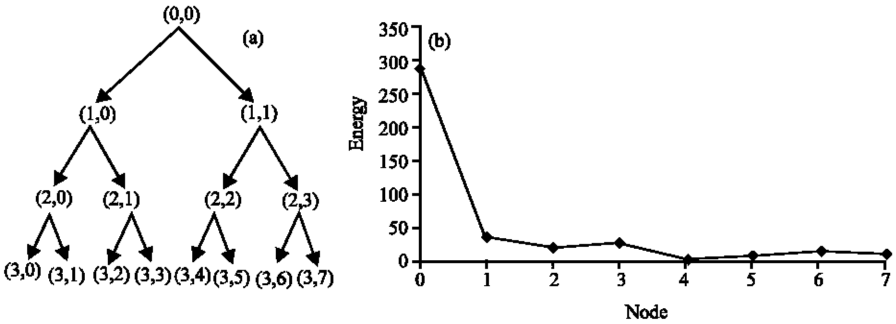


Fig. 2: (a) 3-level wavelet packet decomposition of audio signal and (b) the energy of all nodes

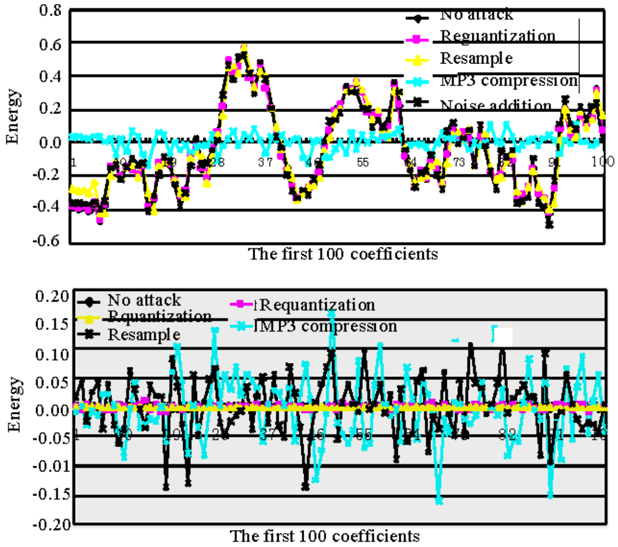


Fig. 3: The changes of node (a) (3, 0) and (b) (3, 4) coefficients after being attacked

where, x (x) is the data which to be quantized, round (.) represents rounded operation.

According to the theory of DM, the embedding process can be divided into following 5 steps:

Step 1: Every audio of the audio aggregation will get corresponding watermark information after distributing binary watermark image into watermark information $w_1, ..., w_n$ based on vector sharing scheme

Step 2: The 3-level wavelet packet decomposition is applied to the audio work x_i (I = 1, ..., n) in audio aggregation, then select the node coefficients $cfs_{i,\ min}$ of minimum energy as embedding position. Segment the coefficients $cfs_{i,\ min}$ into frames according to the length of w_i, one bit will be embedded in one frame and one frame contains L samples

Step 3: Determine the jitter d [k, m_k]. Generally, the value of d [k, 0] can choose freely, then the value of d [k, 1] must determine by the following equation:

$$d[k,1]=\begin{cases} d[k,0]+\Delta/2 & d[k,0]<0 \\ d[k,0]-\Delta/2 & d[k,0]>0 \end{cases} \quad k=1,2,\ldots,N \qquad (4)$$

d [k, 1] and d [k, 1] are used for embedding 0 and 1, respectively.

Step 4: The watermark information will be embed according to the Eq. 2. Firstly, quantize the host signal with the quantization function q_Δ (.), then calculate the output value S (k)

Step 5: Reconstruct the audio segment from all the modified wavelet packet coefficients. Perform the inverse wavelet packet decomposition to get the watermarked audio aggregation $\{x_1, x_2, ..., x_n\}$

Watermark detection: The watermark can be recovered without using the original audio signal as follows:

Watermark extraction: Extraction is based on minimum distance detection method. In the case that encoder embedded one bit in each sample of the host audio signal, extraction can be described as:

$$\hat{m}_k = \underset{i\in\{0,1\}}{\arg\min}\,(\hat{S}(k) - S_i(k))^2 \tag{5}$$

where, $\hat{S}(k)$ is the received signal, the decoder calculates the results of jitter modulation S_0 (k), S_1 (k) by embedding 0 and 1, k = 1, 2, ..., N.

Detector will extract the watermark information by comparing the sum of the Euclidean distances between L samples of S_0 (k), S_1 (k) from received signal for one bit is embedded in every L samples. Judgment is then carried out based on which of them has minimum summation, in following way:

$$\hat{m}_k = \underset{i\in\{0,1\}}{\arg\min} \sum_{n=(k-1)L+1}^{kL} (\hat{S}(n) - S_i(n))^2 \tag{6}$$

According to above equation, extraction process can be divided into following steps:

- Obtain the wavelet packet coefficients $cfs'_{i,\min}$ from each detected audio X'_i using the same approach in watermark embedding process
- Segment coefficients $cfs'_{i,\min}$ into samples in the same method as using in watermark embedding. Then extract the watermark information w'_i according to the Eq. 6

Recover of binary watermark image: Convert the extracted watermark information into decimal system $B' = [b'_0, b'_1, \ldots, b'_{n-1}]$.

- It can be seen from analysis, we can obtain the X'_i by solving the linear equations $B' = AX'_i$, then get V' (k) by converting the X'_i into binary system
- Enhance its dimensions, gain the extracted watermark image W_s

EXPERIMENTAL RESULTS

In this experiment, five types of music including blues, classical, country, folk, pop, are used to compose an original audio aggregation. Two audio works are selected from each type of music, each audio is a 16-bit mono audio work in the WAVE format sampled at 44100 Hz. So an audio aggregation has n = 10 audio works.

In the experiment, ring R is taken as Z_{17}, m = n 10. According to the vector-sharing scheme, we calculate a matrix A, that has 10 rows and 10 columns in Z_{17}:

$$A = \begin{bmatrix} 11 & 3 & 14 & 4 & 6 & 3 & 12 & 11 & 6 & 3 \\ 13 & 4 & 15 & 13 & 12 & 3 & 12 & 14 & 10 & 4 \\ 6 & 12 & 11 & 4 & 5 & 15 & 7 & 14 & 12 & 2 \\ 7 & 12 & 6 & 7 & 1 & 13 & 5 & 1 & 1 & 10 \\ 15 & 14 & 5 & 0 & 15 & 6 & 7 & 11 & 6 & 1 \\ 8 & 9 & 9 & 10 & 14 & 8 & 1 & 2 & 8 & 1 \\ 1 & 13 & 10 & 9 & 11 & 14 & 9 & 12 & 1 & 5 \\ 12 & 11 & 1 & 7 & 16 & 16 & 5 & 11 & 6 & 9 \\ 14 & 13 & 2 & 11 & 4 & 13 & 0 & 15 & 6 & 5 \\ 11 & 6 & 3 & 10 & 11 & 4 & 1 & 10 & 4 & 8 \end{bmatrix}$$

Imperceptibility analysis: Use the Signal to Noise Rate (SNR) to evaluate the perceptual evaluation of the watermark embedded audio quality. The watermark bits to be embedded and the SNR of the method proposed in this paper and in literature (Xiong and Wang, 2010) are shown as follow:

- Suppose that the original watermark contains 40 bit. In order to compare the performance of the two methods of distributing watermark, under the same conditions(the length of audio, the size of watermark, etc.), we calculate the embedding capacity theoretically after using the two methods to distribute the original watermark, which are as shown in Table1.

According to the Table 1, the total bits of watermark both increase after distribution. But the embedding capacity of the algorithm in this paper is obviously much smaller than the method introduced in literature (Xiong and Wang, 2010). That means the audio work will be changed less if using the algorithm in this study under the same conditions. In other words the proposed algorithm in this study affects the perceived quality of the audio lightly.

The SNR of the algorithm in this study and the algorithm introduced by Xiong and Wang (2010) are shown in the Fig. 4 in which horizontal axis shows the audio works in audio aggregation, vertical axis shows the corresponding SNR.

Experimental result show that the value of SNR of the algorithm is larger, it means the imperceptibility of the audio aggregation that is got by the method in this study is better.

Table 1: Comparison of the embedding capacity of the two methods

Methods	Value bit
The original watermark	40
The method in this study	50
The method by Xiong and Wang (2010)	400

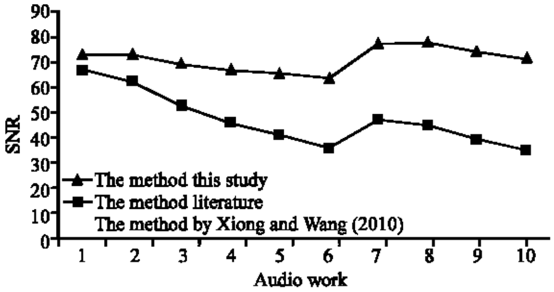


Fig. 4: Comparison of SNR using two different algorithms

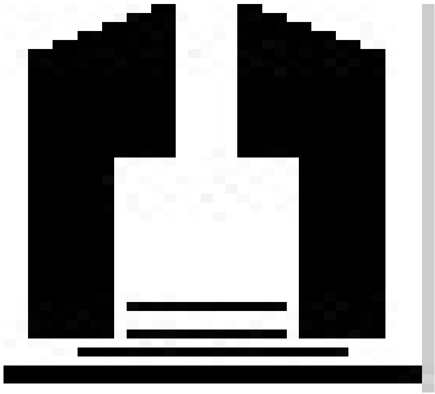


Fig. 5a: The original watermark

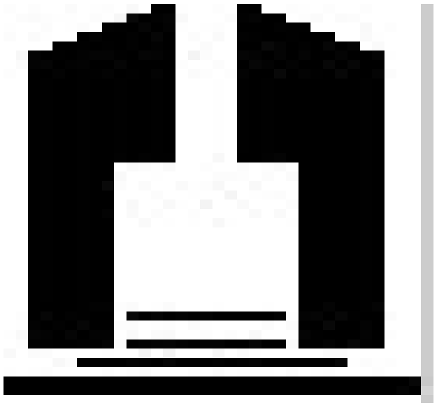


Fig. 5b: The extracted watermark without attacks

Vulnerability analysis: Compute the correlation coefficient (NC) between the original watermark and the extracted watermark and observe the similarity between them to evaluate the vulnerability of algorithm, NC defined as follows:

$$NC(W, W_s) = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} w(i,j)w_s(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} w^2(i,j)}\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2} w_s^2(i,j)}} \qquad (7)$$

where, W is the original watermark and Ws is the extracted watermark and i, j are indices of the binary watermark image. If NC is close to 1, then the similarity between W and Ws is very high. If NC is close to zero, then the similarity between W and Ws is very low.

The original watermark is the binary image of size 34×43 bits, shown in Fig. 5a. Figure 5b is the extracted watermark from the detected audio aggregation which is not suffered from any attacks. The NC=1 which means the watermark can be recovered correctly if the audio aggregation without any attacks.

To test the algorithm can verify the audio work in the aggregation whether to be attacked, the audio aggregation is suffered from traditional attack and joint attack and analyze the vulnerability of the extracted watermark.

Traditional attack, which is tested on each audio of the audio aggregation, such as Low-pass filtering. Adopt a six order Butterworth filter with cut-off frequencies 22.05 kHz; Resample. Consist of subsequent down sampling to 22.05 kHz; Re-quantization. Audio signal is quantified from the 16 bit to 8 bit and then quantified to 16 bit again; Noise addition. White Gaussian Noise is added to the audio signal to give 26 dB SNR; MP3 (MPEG-1 audio layer-3) compression. The audio signals are compressed into MP3 format by MPEG-1 Layer-3 encoder and decoded, compression rate is 128kbps; Cropping. Cut 20% section of digital audio randomly.

Then extract the watermark from the audio aggregation which is to be attacked. When one or more audio works being suffered from traditional attacks, the results as shown in Table 2.

According to Table 2, the extracted watermark changes obviously after one audio being suffered from various attacks. When the number of the attacked audio work is larger, the extracted watermark changes severer which shows that the proposed algorithms are fragile to the above attacks.

Every audio work of the audio aggregation has its watermark information because we have used the vector-sharing scheme to distribute the original watermark. When the audio aggregation being attacked, we can determine which audio work has been attacked in the audio aggregation. Take one case of Table 2 for example, when five audio works in the aggregation suffered from Re-quantization attack, the correlation coefficients of each audio are showed in the Table 3.

If the correlation coefficient (NC) of the audio work is less than 1 that proves it was destroyed. It can be seen from the data in Table 3, the collection coefficients (NC)

Table 2: The extracted watermark after one or more audio being suffered from attacks

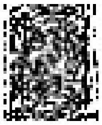
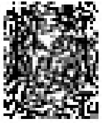
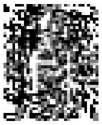
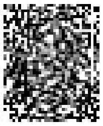
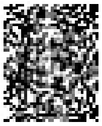
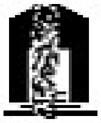
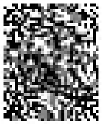
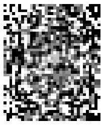
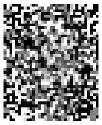
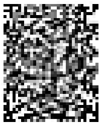
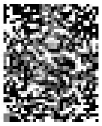
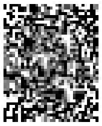
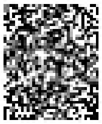
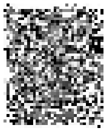
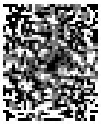
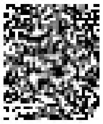
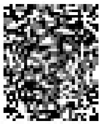
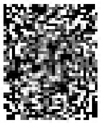
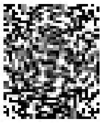
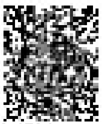
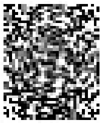
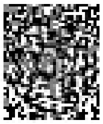
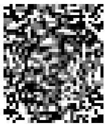
	Re-quantization	Resample	MP3 compression	Noise addition (26dB)	Low-pass filtering	Cropping
Attack 1 audio						
NC	0.5917	0.5705	0.6029	0.5372	0.5505	0.86
Attack 5 audio						
NC	0.4746	0.5188	0.4986	0.4898	0.4973	0.470
Attack 10 audio						
NC	0.474	0.4846	0.4926	0.4926	0.489	0.4576

Table 3: Five audio works in the aggregation suffered from Re-quantization attack

	Audio 1	Audio 2	Audio 3	Audio 4	Audio 5	Audio 6	Audio 7	Audio 8	Audio 9	Audio 10
NC	0.4654	0.4104	1	1	0.4011	1	1	0.3952	1	0.3975

Table 4: The extracted watermark after one or more audio being suffered from substituting audio attacks

	Substitute 1 audio from aggregation	Substitute 2 audio from aggregation	Substitute 3 audio from aggregation	Substitute 4 audio from aggregation	Substitute 5 audio from aggregation
Extracted watermark					
NC	0.4835	0.4704	0.4923	0.4564	0.4659

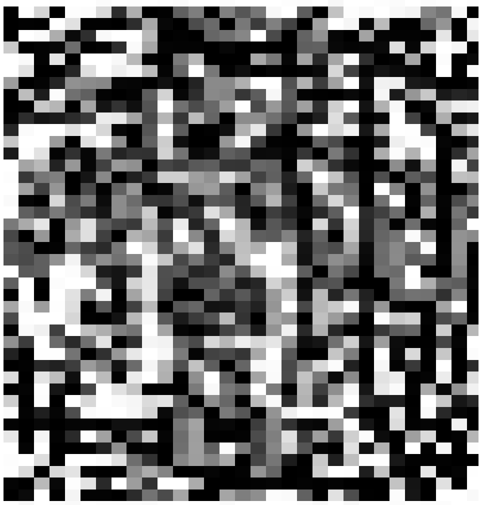


Fig. 6: The extracted watermark after being suffered from above attack

To test the algorithm can verify the integrity of an audio aggregation and consider the specificity of the audio aggregation, the audio aggregation is suffered from deleting audio attack and substituting audio attack and analyze the vulnerability of the extracted watermark.

Deleting audio attack means deleting one or more audio works in the audio aggregation, then extracting the watermark from the audio aggregation which is suffered from the above attack. In this algorithm, the extracted watermark is shown in Fig. 6 when deleting one audio work, where NC = 0.5230.

It can be seen from Fig. 6, we can not correctly extract the watermark when deleting one audio work from the audio aggregation. This also proves that watermark information only can be seen from the entire aggregation because of using the vector sharing scheme to distribute watermark in this study and m is set as n. We only can extract the watermark when the audio aggregation is complete, which can authenticate the integrity of the audio aggregation.

Substituting audio attack means one or more audio works replaced by some non-correlated audio works, then extracting watermark from the replaced audio aggregation. According to the Table 4, when substituting one detected audio, it is very difficult to extract watermark correctly. When the number of the attacked audio work is larger, the extracted watermark changes greater. This shows that the watermark information is closely related to the various audio works in the aggregation because k is set as n when using the vector sharing scheme to distribute watermark in this algorithm.

DISCUSSION

In order to evaluate other digital watermarking methods and the proposed algorithm, several points were shown as follows to discuss for later researchers.

It can be seen from the Table 1, the watermark bits after using the proposed method to distribute the original watermark is much less than the method proposed in literature (Xiong and Wang, 2010) to distribute the same watermark.

By analyzing the Fig. 4, the value of SNR obtained by the proposed method in this paper is larger than the value obtained by the method introduced in literature (Xiong and Wang, 2010). This also proves the above point.

If an audio aggregation has been attacked, the proposed method can not only detect it correctly, but also locate which audio work in the audio aggregation has been attacked.

From the point of attack methods, the method for attacking audio aggregation should be improved.

In this study, when the audio aggregation has been attacked, although the algorithm can determine which audio work (s) of the aggregation, but can not determine what kind of attack and also can not recover the audio work (s). We can perfect these deficiencies in future.

In our method, we only consider the audio works in the WAVE format. So, audio works in compress domain, for example Mp3 audio format, should be considered.

CONCLUSION

From the perspective of the practical application of audio works, a fragile watermarking algorithm to authenticate the integrity of audio aggregation based on vector sharing scheme is presented in the study. The watermark can only be recovered from the complete audio aggregation, we also test the algorithm by a series of experiments. Experimental results show, as long as one audio work of aggregation is attacked, the change can be significantly reflected in the extracted watermark. The algorithm not only has a strong sensitivity to common signal processing, but also can verify the integrity of the audio aggregation.

ACKNOWLEDGMENTS

This study is supported by the National Natural Science Foundation of China (NSFC: 60873220), Zhejiang natural science foundation of China (ZJNSF:Y108022, Y1090285) and the Industry preferred Projects of Ningbo Technology of China (2009B10003). In addition, our programs are supported by High School Special Fields Construction of Computer Science and Technology, Zhejiang Province Excellent Course Project (2007) and Zhejiang Province Key teaching material Construction project (2009).

REFERENCES

Blakley, G.R., 1979. Safeguarding cryptographic keys. Proc. Natl. Comput. Conf. AFIPS., 48: 313-317.

Hogan, M.T., F. Balado, G.C.M. Silvestre and N.J. Hurley, 2006. Secure and robust steganography using side information at the encoder. Inform. Secu. Proc. IEEE, 153: 87-95.

Jacobson, N., 1953. Lectures in Abstract Algebra. Vol. 2, D. Van Nostrand Co. Inc., New York.

Schneier, B., 1996. Applied Cryptography. 2nd Edn., John Wiley and Son, Inc., New York, pp: 12-16,23.

Shterev, I.D. and R.L. Lagendijk, 2006. Amplitude scale estimation for quantization-based watermarking. IEEE Trans. Signal Proc., 54: 4146-4155.

Solanki, K., K. Sullivan, U. Madhow, B.S. Manjunath and S. Chandrasekaran, 2005. Statistical restoration for robust and secure steganography. Int. Conf. Image Proc., 2: 1118-1121.

Wang, R.D. and Y.Q. Xiong, 2010. A novel watermarking algorithm for protecting audio aggregation based on ICA. Proceedings of the 6th International Conference on Digital Content, Multimedia Technology and its Applications, Aug. 16-18, Seoul, pp: 302-308.

Xiong, Y.Q. and R.D. Wang, 2009. A robust audio aggregate zero-watermark algorithm. Proceeding of the 6th International Conference on Information Technology. New Generations ITNG, Las Vegas, Nevada, April 27-29, IEEE, USA., pp: 366-370.

Xiong, Y. and R. Wang, 2010. An authentication algorithm of audio aggregate based on the (k, n/k=n) method. Proceeding of the 2nd International Conference Future Computer and Communication(ICFCC), May 21-24, Wuhan, pp: 69-73.

Yao, H.M., A.F. Sui and S.Z. Niu, 2003. Digital watermarking sharing algorithm based on vector secret sharing scheme. J. Elect. Inform. Technol., 25: 1612-1615.

Zhang, H.M. and H.W. Lv, 2009. Audio watermarking sharing algorithm based on *Blakley scheme*. Comput. Eng. Appl., 45: 111-112.