Research Journal of Applied Sciences, Engineering and Technology 4(11): 1545-1549, 2012
ISSN: 2040-7467

Submitted: January 03, 2012 Accepted: March 10, 2012 Published: June 01, 2012

Improving Security of Audio Watermarking in Image using Selector Keys

Amir Reza Fazli, Mohammad Eghbali Asli and Hamid Alinejad-Rokny
Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

Abstract: This study presents a novel watermarking algorithm for improving the security and robustness of hiding audio data in an image. Multi resolution discrete wavelet transform is used for embedding the audio watermark in an image. In this context, security is quantified from an information theoretic point of view by means of the equivocation and information leakage of the secret parameters. The selector keys are used as a criterion to determine the location of appropriate wavelet blocks and wavelet coefficients for embedding the watermark. Also, simulations assess the security levels derived in the theoretical part of the paper. The experimental results demonstrate that using the selector keys enhance the security level of the watermark embedding for a variety of scenarios. The level of the algorithm robustness is shown by considering Normalized Correlation (NC) between the original audio watermark and extracted watermark.

Key words: Entropy, equivocation, information leakage, selector keys, wavelet transform

INTRODUCTION

There is no doubt that the number of digital watermarking studies has been increasing markedly in recent years. This studies lead to advent a lot of new techniques in which a watermark can be embedded in an original signal. The watermark can be applied on wavelet transform (Rehman *et al*., 2009) and cepstrum domain (Bahat *et al*., 2008).

A considerable percentage of the watermark studies have been worked toward the improvement of robustness. The useful effects of using BCH code on robustness is discussed in (Cheng *et al*., 2006). On the other side, no one can deny the importance of security on the watermarking algorithms. The first attempt at providing a mathematical framework for assessing in watermarking security was in (Barni *et al*., 2003). Also, Cayre and Bas (2008) define four security classes, namely, by order of decreasing security: insecurity, key security, subspace security and stego security in (Cayre and Bas, 2006).

This study presents an algorithm for audio watermarking in an image using selector keys based on discrete wavelet transform. Firstly, an original image is decomposed by DWT at 3rd level. The audio watermark could be embedded in the original image wavelet domain in the algorithm.

We use three selector keys with the same size by watermark to enhance the security level of watermarking. The first selector key K1 is used to determine wavelet block for the watermark embedding while two other keys K2 and K3 are applied to choose the suitable coefficients in each selected wavelet block for hiding the audio watermark.

There are a number of most important characteristics that a watermarking technique should exhibit. It is useful to distinguish between these properties. We used the general definition proposed in (Rehman *et al*., 2009):

- **Security:** A watermark should be secret and must be undetectable by an unauthorized user in general. This requirement is regarded as security and watermark is usually achieved by the use of privet secret keys.
- **Robustness:** The digital watermark is still present in the image after attack and can be detected by the watermark detector, especially on the attacks from compression. Possible attacks include linear or nonlinear filtering, resizing and image compression.

The main reason for transferring a secret audio file using a still image is that Human Visual System (HVS) is less sensitive than human auditory system, hence using a still image as a medium instead of an audio file can be effective to achieve maximum measure of imperceptibility. Moreover, there are many attributes of the HVS that are potential candidates for exploitation in a data-hiding system, including our varying sensitivity to contrast as a function of spatial frequency and the masking effect of edges.

Corresponding Author: Amir Reza Fazli, Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran

Three different scenarios for security assessment are considered, according to classification given in (Barni *et al*., 2003):

- **Known Message Attack (KMA):** The attacker is assumed to have access to watermarked signal and message embedded in each of those signals. This scenario constitutes the basis for the study of more involved scenarios and provides the main insight into the security problem.
- **Watermarked-Only Attack (WOA):** the only information available to the attacker is the Watermarked signal, without any knowledge of the embedded messages. As such, WOA models most of the data-hiding scenarios of practical interest.
- **Known Original Attack (KOA):** This scenario occurs when attacker has access to several pairs of watermarked contents and their corresponding original versions.

The techniques used for data hiding vary depending on the type of desirable application of watermarking system. The motivation for this work includes the provision of a practical watermarking algorithm for security applications.

THE THEORETICAL ESTIMATION OF SECURITY

In order to analyse a wavelet based watermarking from an information theoretic point of view, we make a clear definition of Shannon's theory regarding perfect secrecy. An encryption scheme has perfect secrecy iff I (K|O) = 0

This means that in a perfect covering scheme, the observation do not reveal any information about the secret key K. In the case where the secret key is a discrete variable, the entropy H (K) measures the uncertainty of the opponent on the true value of K. When the opponent makes observation O, his uncertainty is evaluated through conditional entropy, which Shannon named equivocation:

$$H(K|O) = H(K) - I(K|O). \quad (1)$$

The information leakage is measured by the mutual information between observation and security key. In the KMA scenario, the opponent only has access to watermarked vector Y and the associate message (Y, M). Therefore, information leakage and equivocation are I (Y; K|W), H (K|W, Y) respectively. In a clear way:

$$I(Y; K|W) = H(Y|W) \quad (2)$$

$$H(K|W, Y) = H(K) - H(Y|W) \quad (3)$$

In the KMA scenario, the opponent observes only watermarked content Y and its original version X, (Y, X), we have:

$$I(Y; K|X) = H(Y|X, W). \quad (4)$$

$$H(K|X, Y) = H(K) - H(Y|W, X). \quad (5)$$

In the WOA scenario, the opponent only has access to watermarked vector Y. The information leakage in the WOA scenario is:

$$I(Y; K) = H(Y) - H(K). \quad (6)$$

Equivocation is denoted by:

$$H(K|Y) = H(K) + H(W) - H(Y). \quad (7)$$

PROPOSED WATERMARKING ALGORITHM

Watermark embedding algorithm: The procedure of embedding watermark is as follows:

Step 1: Decompose the original image *x* into three levels with ten sub- bands using three-level discrete wavelet transform.

C = {LL3, HL3, LH3, HH3, LL2… HH1}

Step 2: The entropy of each sub-band at resolution level three is calculated. The two sub-bands with most measure of entropy are selected for embedding the audio watermark. Usually, two sub-bands LH3 and HL3 will have the most measure of entropy.

Entropy is a statistical measure or randomness:

$$H = -\text{sum}(P * \log(P)) \quad (8)$$

where P indicates the histogram counts for a gray image (Cayre and Bas, 2006).

Step 3: Three random selector keys with the same size by audio watermark are created. The selector key K1 is a binary key and two other keys K2 and K3 are integer keys. Each bit of selector key K1 indicates the wavelet block which is used for embedding its corresponding frame of audio watermark. After the determination of qualified wavelet block for embedding each one of audio watermark frames, the selector keys K2 and K3 are used to identify the location of coefficients which are going to be used for data embedding

Step 4: The coefficients in the qualified blocks are modified with the frames of audio watermark:

$$v'(i, j) = v(i, j) + a * w(l) \quad (9)$$

where v' *marks* the transformed coefficients after embedding audio watermark w in the wavelet coefficients v. Also, a is a scaling parameter for watermark embedding.

Step 5: The Inverse Discrete Wavelet Transformation (IDWT) is applied to modified wavelet coefficients in order to produce the watermarked image.

Watermark extraction algorithm: The embedding of an audio watermark increases the details in the qualified wavelet blocks. Hence, their entropy remains high and they will be identified as the most entropy wavelet blocks at the decoder.

The following are the steps in the extraction of the watermark:

Step 1: We first decompose a watermarked image Y and the original image x with discrete wavelet transform into three levels of ten sub-bands:

$$y = DWT(x)$$

$$y' = DWT(x')$$

Step 2: The entropy of each sub-band at resolution level three is calculated. The two sub-bands with most measure of entropy are selected for extracting the audio watermark.

Step 3: The selector keys are applied to determine the qualified wavelet blocks and the coefficients which are host for the frames of an audio watermark. We subtract the same index of coefficients of qualified wavelet blocks in y' by the coefficients of qualified wavelet blocks in y. Then we scale down the watermark:

$$W'(l) = (y'(i, j) - y(i, j))/a \quad (10)$$

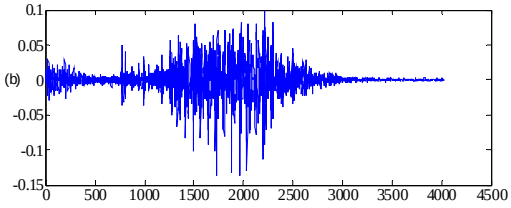
Step 4: After arranging the index of watermarks, we have the extracted watermark W'.

SIMULATION EXPERIMENT

Simulations have been directed to assess the performance of the proposed algorithm. The audio watermark signal sampling rate is 16 bits and single channel.

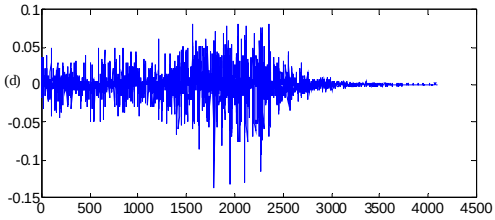
We applied the proposed watermarking algorithm on real images. Then, we used the theoretical analysis presented in the section II to evaluate the measure of security for different scenarios. Also, we measure the similarity of original audio watermarks and extracted watermarks by the standard Normal Correlation (NC) as a criterion to assess the robustness of algorithm.

(a)



(b)

(c)



(d)

Fig. 1: Example of an embedding and extracting watermark. (a) Original image (b) Audio watermark (c) Watermarked image (d) Watermark extract

Figure 2 indicates the measure of equivocation for all of the scenarios without using selector keys relate to size of audio watermark. Also, in Fig. 3 the measure of equivocation for different scenarios is shown. The main difficulty in hiding an audio watermark in a wavelet block

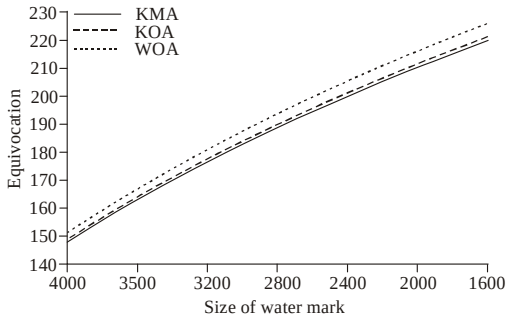


Fig. 2: Measure of equivocation for different scenarios without using selector keys

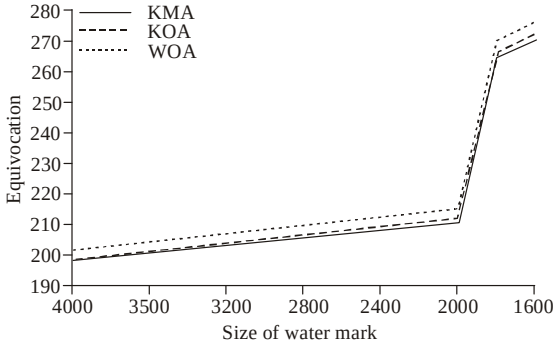


Fig. 3: Measure of equivocation for different scenarios with using selector keys

of an image is that the capacity of these blocks is extremely limited. The maximum numbers of coefficients in a decomposed wavelet block in three levels for an image whose size was 128*128 pixels is 4096. This limitation will cause a remarkable decrease in the measure of equivocation as the number of audio frames increases. This reduce in the quantity of security is shown in Fig. 2. In order to make an improvement in security level, we used the three selector keys instead of one security key which was used in the previous algorithm. Using the selector keys lead to a significant increase in the measure of equivocation which is observable in Fig. 3.

In Fig. 4, we depict the plot of normalized correlation for both algorithms as a function of number of audio frames. We can see the quantity of NC (Normalized Correlation) decreases as the size of audio frames increases in both of these plots but the slope of decrease in NC in the algorithm with using selector keys is very slow whereas NC in the other algorithm reduces abruptly.

It means that using selector keys avoids robustness abating and causes security improvement while keeping NC in an appropriate range for watermarking applications.

For example, if we need to extract an audio able watermark, the measure of NC must be greater than 0.9. Therefore, we can not use the audio watermarks with the

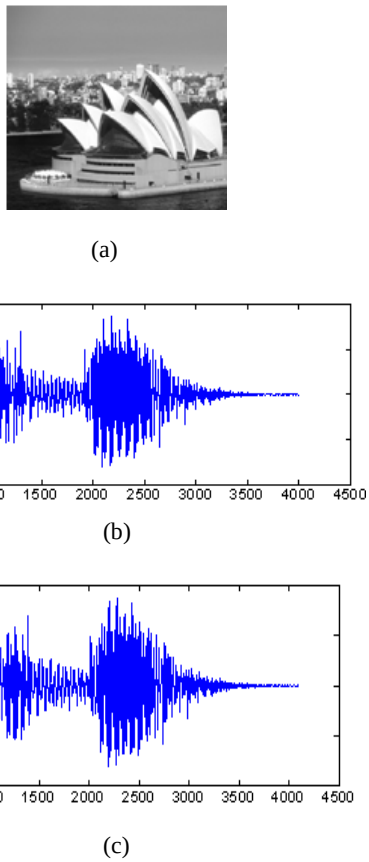


Fig. 4: Example of an embedding and extracting watermark. (a) Watermarked image (b) Audio watermark (c) watermark extract

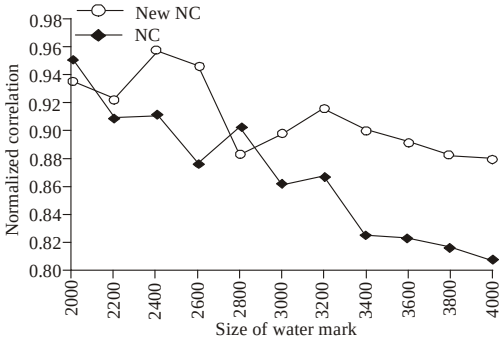


Fig. 5: Normalized correlations between the original watermark and extracted watermark

big sizes. In the area which is located between 3000 to 4000 frames in Fig. 5, the proposed watermarking algorithm, which uses selector keys, has an upper measure of equivocation and better security. The important remark in Fig. 5 happens for the number of frames smaller than 2000 where the measure of equivocation for all scenarios increases suddenly and drew on the ideal measure.

Table 1: PSNR and information leakage for WOA scenario in two watermarking algorithms

Watermark	Size of watermark	N C without selector keys	N C NC with keys	P S N R without selector keys(db)	P S N R with selector keys (db)	Information Leakage without selector (bit/Sym)	Information Leakage with selector (bit/Sym)
Lena(512*512)	2500	0.8953	0.9494	46.1245	40.7664	0.5034	0.5082
Lena(512*512)	3000	0.8613	0.8976	40.7890	44.1723	1.9649	1.5637
Lena(512*512)	3600	0.8222	0.8935	35.8214	36.5333	3.5118	1.8418
Lena(512*512)	4000	0.8070	0.8802	33.6817	32.1187	3.0933	2.2575
Sunday (512*512)	2500	0.9099	0.9034	41.9802	39.7981	0.8614	0.8511
Sunday (512*512)	3600	0.8173	0.9122	33.6543	34.6531	2.7558	1.0068
Sunday (512*512)	4000	0.7998	0.8644	31.8974	33.7968	5.3526	2.4915

Furthermore, the visual imperceptibility of watermarking is measured by the Peak Signal to Noise Ratio (PSNR) of the host image and the watermarked image. Table 1 indicates the PSNR and information leakage for the WOA scenario in both watermarking algorithms. It is clear that the measure of PSNR is almost same for both algorithms. Therefore, we conclude that hiding the audio watermark does not lead to a serious degrade in perceptual quality of watermarked image.

Moreover, algorithm with selector keys has smaller values of information leakage than other algorithm. Also, the difference between the information leakages in two algorithms has grown by increasing in the number of audio frames.

Hence, using the selector keys will be more effective in the bigger number of audio frames.

CONCLUSION

Since some weaknesses exist in human visual system, an image is a suitable medium for hiding an audio file. This paper presents a novel audio watermarking algorithm in an image which improves the level of security. The main characteristic of this algorithm is using three selector keys for increasing the measure of equivocation for opponent. In experimental results, we show that our scheme achieves a high measure of security against the opponent attacks. Moreover, the proposed watermarking algorithm is more robust to either DWT based techniques. Finally, using the selector keys increases the capacity of watermarking algorithm.

REFERENCES

Bahat, V., I. Sengupta and A. Das, 2008. Audio watermarking based on bch coding using CT and DWT. Int. Conf. Inform. Technol., 34(10): 49-51.

Barni, M., F. Bartolini and T. Furon, 2003. A general frame work for robust watermarking security. IEEE Trans. Signal Proces., 83(10): 2069-2083.

Cayre, F. and P. Bas, 2008. Kerckhoffs based embedding security class for WOA data hiding. IEEE T. Inf. Foren. Sec., 3(1): 1-15.

Cheng, L.S., S. Feng and D. Lin, 2006. BCH code-based robust audio watermarking. J. Inf. Sci. Eng., 22(23): 535-543.

Rehman, F.U., R. Khan and F. Ahmed, 2009. Entropy based audio watermarking in image using wavelet transform. Int. Colloq. Comput. Control, 6: 478-481.